

---

# Perle IOLAN SCR1618 RDAC

Updated: May 15, 2020  
Revision: A1.05.15.2020  
Document Part: 5500465-10

---

## Preface

### Audience

This guide is for the individual responsible for the installation of the Perle IOLAN SCR1618 RDAC. Familiarity with networking, concepts, and terminology relating to Ethernet and LAN (local area networks) is required.

### Purpose

This guide provides the information needed to configure and manage the Perle IOLAN SCR1618 RDAC. 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.

Copyright©

2020 Perle Systems Limited.

60 Renfrew Drive

Markham, Ontario

L3R 0E1, Canada

All rights reserved. No part of this document may be reproduced or used in any form without written permission from Perle Systems Limited.

### Publishing History

Date	Revision	Update Details
May 2020	A1.05.15.2020	Initial release of this guide.

# Table of Contents

---

<b>Preface</b> .....	<b>2</b>
<b>Overview</b> .....	<b>4</b>
General Features .....	4
Serial Ports .....	4
Ethernet Ports .....	4
Firewall and Security .....	5
<b>Initial Setup</b> .....	<b>6</b>
Hardware Installation .....	6
LAN Connection .....	6
Power Source Connection .....	6
Setup mode .....	7
<b>Managing the IOLAN</b> .....	<b>7</b>
Using the WebManager .....	7
Navigating with the WebManager .....	7
Search Navigation .....	7
Using the CLI (Command Line Interface) .....	8
Admin Console Port .....	8
Connecting to the Admin Console Port .....	8
Configuration Files .....	9
<b>System</b> .....	<b>10</b>
General .....	10
Logging .....	13
Email .....	18
<b>Interfaces</b> .....	<b>20</b>
Ethernet .....	20
Serial .....	20
VLAN .....	20
Bridge .....	20
PPPoE .....	20
Tunnels .....	20
Serial RS232 .....	36
<b>DNS</b> .....	<b>38</b>
DNS Forwarding .....	38
DNS Listeners .....	39
DNS Domain Forwarding .....	39
Dynamic DNS .....	39
<b>IP Host Tables</b> .....	<b>41</b>
<b>WAN</b> .....	<b>41</b>
<b>ARP Management</b> .....	<b>46</b>
<b>Routing</b> .....	<b>48</b>
Default Gateway .....	48
Static Routing .....	48
Port Forwarding .....	50
NAT/ALG .....	51

---

---

Access Control Lists.....	52
Prefix List.....	54
Route Maps.....	55
AS-Paths.....	59
Policy Routing.....	60
Route Tables.....	62
RIP.....	63
OSPF.....	67
BGP.....	76
<b>Services.....</b>	<b>87</b>
Serial Port Services.....	87
Serial Port.....	88
Console Management.....	88
Trueport.....	91
TCP Sockets.....	94
UDP Sockets.....	98
Terminal.....	102
Printer.....	107
Serial Tunneling.....	108
Virtual Modem.....	110
Modbus Gateway.....	115
Remote Access (PPP).....	120
Remote Access (SLIP).....	129
Dial Options.....	132
Session Strings.....	132
Packet Forwarding.....	133
SSL/TLS.....	138
Port Buffering.....	153
Trueport Baud Rate.....	155
Advanced Serial Options.....	156
<b>DHCP Server.....</b>	<b>157</b>
<b>DHCP Relay.....</b>	<b>161</b>
<b>Zero Touch Provisioning.....</b>	<b>163</b>
Configuration over DHCP.....	163
<b>SNMP.....</b>	<b>166</b>
Connecting to the IOLAN Using SNMP.....	166
Using the SNMP MIB.....	166
<b>NTP Server.....</b>	<b>170</b>
<b>Alarm Manager.....</b>	<b>174</b>
<b>Telnet/SSH.....</b>	<b>176</b>
<b>Security.....</b>	<b>179</b>
User Accounts.....	179
AAA (Authentication, Authorization and Accounting).....	184
Configuring AAA Method.....	185

---

---

Radius .....	186
Login.....	188
TACACS+.....	190
Firewall .....	192
IPSEC.....	196
OpenVPN .....	202
802.1X .....	206
<b>Monitor and Statistics .....</b>	<b>212</b>
System/General.....	212
View Logs.....	213
Interface Status .....	214
Alarms .....	215
<b>Administration.....</b>	<b>216</b>
Software Management .....	216
<b>Boot Configuration File .....</b>	<b>217</b>
Keys and Certificates .....	218
Managing Flash Files .....	224
Reboot/Reset .....	224
Reset to Factory Defaults.....	224
Shutdown .....	224
<b>Trueport .....</b>	<b>226</b>
<b>Modbus Remapping Feature .....</b>	<b>227</b>
<b>Valid SSL/TLS Ciphers .....</b>	<b>228</b>
<b>Diagnostics .....</b>	<b>230</b>
Ping .....	230
Traceroute .....	230
<b>Radius External Parameters .....</b>	<b>232</b>
Supported Radius Parameters .....	232
Accounting Message .....	234
Mapped RADIUS Parameters to IOLAN Parameters.....	236
Perle RADIUS Dictionary Example .....	237
<b>Data Logging Feature .....</b>	<b>243</b>
Trueport Profile.....	243
TCP Socket Profile .....	243

---

---

## Overview

### *About the IOLAN SCR*

Perle's IOLAN SCR all in one Serial Console Server and Ethernet router was specifically design for data center full integration deployments. The IOLAN SCR adds full IPv4/IPv6 routing capabilities with support for RIP, OSPF and BGP protocols and increased security with an integrated firewall supporting zone firewall and two factor authentication. The IOLAN has a powerful multi-core CPU for routing and switching. Serial port access provides secure remote access to Unix Servers, Linux Servers, Windows Servers, and any device on the network with a console port. The IOLAN SCR allows network operations center (NOC) personnel to perform secure remote data center management and out-of-band management of IT assets from anywhere in the world.

### *General Features*

- 10/100/1000 Ethernet and SFP routing and switching support with Redundant Path Technology
- Advanced AAA security and encryption
- RS232 admin port for increased security
- Web GUI and CLI Management
- Primary/Backup host functionality enables automatic connections to alternate hosts should the primary TCP connection go down
- Routing Protocols including RIP, OSPF, BGP
- Firewall
- WAN Traffic Load Balancing
- Dynamic DNS – Easy console management access from anywhere on the Internet
- Java-free browser access to remote serial console ports via Telnet and SSH
- Next Generation IPv6 routing support
- Optional Dual AC Power for Fault-tolerant uptime

### *Serial Ports*

- Connect directly using Telnet/ SSH either by port and IP address (aliasing)
- Connect via HTTP and HTTPS
- Multi-session capabilities allows multiple users to access ports simultaneous
- Multi-host access enables multiple hosts/servers to share serial ports

### *Ethernet Ports*

- Bridging, switching, routing
- IPv4/IPv6, static routing, RIP/RIPNg, NAT, OSPF, BGP-4
- Dynamic DNS, DNS Proxy/Spoofing, DHCP / DHCPV6, Opt82, NTP, SNTP, Reverse SSH, SSL, RIPV2, TFTP,SFTP, Telnet, LDP, RCP, WINS, SNMP, RFC2217 IPsec, OpenVPN, Failover, Load Sharing
- Static routing with Primary/Backup route

---

## *Firewall and Security*

- ACL (list, range and time)
- Filter based IP, port and protocol
- Secure HTTP/HTTPS/FTP/Telnet
- Port forwarding
- BGP Communities
- Zone Firewall
- 2 Factor authentication
- SSHv2
- Radius, TACACS+ Authentication, Authorization and Accounting
- Local User database
- SNMPv3

---

## 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 your IOLAN SCR1618 RDAC Hardware Installation Guide.

### *LAN Connection*

From the factory the IOLAN 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 IOLAN is acting as a DHCP server to provide IP addresses to any connected devices. It is recommended that a single PC is connected to one of the Ethernet ports for doing the initial setup.

**Warning:** Do not connect any of the IOLAN's Ethernet ports to an existing network, since the DHCP service on the IOLAN 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.

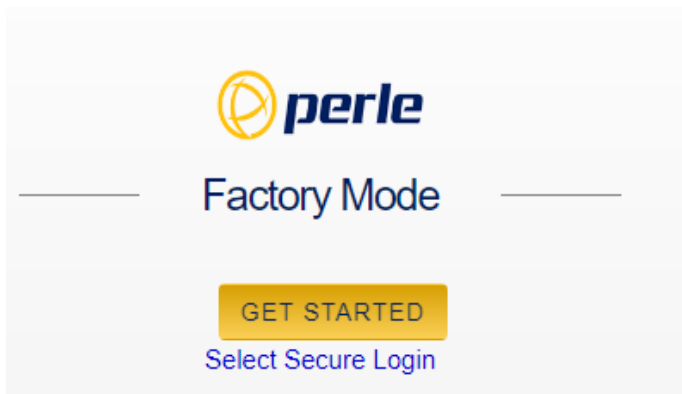
### *Power Source Connection*

Connect dual power to power sources. Once power is connected, the IOLAN will cycle through several sequences. The LED 1, PWR 1 and 2 will show solid green when the IOLAN is fully booted and ready to configure.

See the IOLAN SCR1618 RDAC for more information on power guidelines.

### **Performing initial configuration using the WebManager**

1. Connect Power to power sources.
2. Set your PC to obtain an IP address automatically using DHCP.
3. Plug your PC into any of the IOLAN's Ethernet ports (located on the back of the unit).
4. Use a standard web browser and enter <http://192.168.0.1> to access your IOLAN.
5. On the setup screen, select, Getting Started.





### Setup mode

This mode is available when the IOLAN is in “Factory Default” mode. Once the IOLAN is configured, it is no longer in this mode. You can return to this mode anytime by resetting the IOLAN to factory defaults. In setup mode, you simply need to fill in the required fields, apply changes to save and exit. The configuration changes will be immediately applied to the IOLAN.

**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 *Setup Mode*.

### Sign into the IOLAN

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

### Sign into the IOLAN using Console Mode

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

## Managing the IOLAN

### Using the WebManager

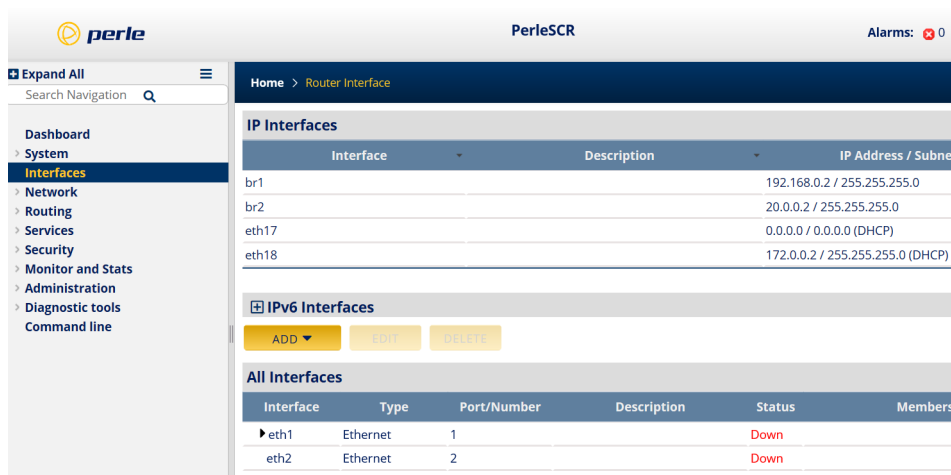
The Perle WebManager is an embedded Web based application that provides an easy to use browser interface for configuring and managing your IOLAN. The WebManager is accessible through any standard desktop web browser either through a secure or non-secure connection.

### Navigating with 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.



---

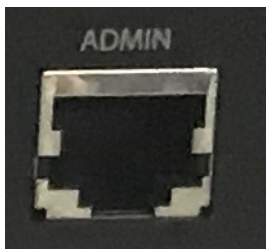
## *Using the CLI (Command Line Interface)*

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 IOLAN console or IP based sessions like SSH or Telnet.

**Note:** If using CLI to perform the initial configuration of the IOLAN you must connect to the IOLAN via the console port.

## *Admin Console Port*

The IOLAN has one serial (RS232) console port (8 pin connector with DTE pinouts) on the front for use with PC's equipped with a serial com port or using a USB to serial converter. The IOLAN can be fully configured and managed from the console port. The console port provides direct access to the Command Line Interface (CLI).



## *Connecting to the Admin Console Port*

To connect to the RJ45 console port:

1. Connect the power, then set the power switches on the back of the IOLAN to the On position.
2. Allow the IOLAN to complete the boot up sequence.
3. Connect an RJ45 cable directly from the IOLAN to the COM port on your PC (a serial port adapter will be needed). A serial to USB converter may also be used.
4. On the PC, select Choose Start-> Control Panel-> Hardware and Sound or equivalent on the Windows Operating System you are using. The exact procedure may vary depending on the version of Windows you are using.
5. Click the Hardware tab and choose Device Manager, Expand the Ports (COM & LPT) section. This will expand the drop down to show the number of com ports on your system. Connect the cable to one of these ports (probably COM1 or COM2, in the case of a USB serial to USB converter look for associated installed driver and com port number).
6. Start a terminal emulation program (such as Putty or SecureCRT) on the COM port where you have connected the cable to the PC.
7. Configure this COM port within the terminal emulation program with the following parameters:
  - 9600 baud
  - 8 data bits
  - 1 stop bit
  - No parity

- 
- None (flow control)
8. Press the Enter key on the keyboard and the login prompt will display.
  9. The login is admin and password is perle1.

## *Configuration Files*

### **Running-config**

The IOLAN operates from a version of the configuration that is loaded into memory and is referred to as “running-config”. When making changes to the configuration using the WebManager, it applies all changes to both “running-config” and “startup-config” when the Save button is selected. These changes take effect immediately and will be persistent (maintained after a restart of the IOLAN).

However when using the CLI to configure your IOLAN, configuration changes are made immediately to the running config but not to your startup-config, therefore, you must copy the running-config to the startup-config before you reload your IOLAN or your configuration changes will be lost.

### **Startup-config**

The “startup-up” configuration resides in flash memory and used every time the IOLAN is reloaded. When making changes to the startup configuration using the WebManager, it applies all changes to both “running-config” and “startup-config” at the same time. All changes made in WebManager take effect immediately and will be persistent (maintained after a restart of the IOLAN).

For detailed information on the CLI, please refer to the IOLAN SCR CLI Guide available for download from the Perle web site at <https://www.perle.com>.

## System

Under System navigation, you will be able to set general parameters for your IOLAN. These features include:

- General
- Logging
- Email

### *General*

This section allows you to setup general IOLAN information such as identification, date and time, IPv6 parameters, Management access rules, command line access, console port parameters, Webmanager access, and lastly enable SNMP.

<i>Identification</i>	
<b>System name</b>	<b>Provide your IOLAN with a name.</b>
<b>Domain Name</b>	<b>Provide your IOLAN with a Domain Name.</b>
<b>Location</b>	<b>Provide a location description.</b>
<b>Contact</b>	<b>Provide a contact name.</b>
<i>Date and Time</i>	
<b>Set clock from PC</b>	<b>Set the IOLAN's clock using your PC clock time.</b>
<b>Change Date and Time</b>	<b>Manually change the IOLAN's time.</b>
<b>Change Time Zone</b>	<b>Manually change the IOLAN's time zone.</b>

### **IPv6**

By default the IOLAN has IPV6 and IPv4 enabled. Enabling or Disabling IPv6 will require a system reboot. The IOLAN has a factory default link local IPv6 address based upon its MAC Address.

#### **For example:**

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

The IOLAN 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.

<i>IPv6</i>	
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 IOLAN is controlled. Protocol based access control is used to restrict access by interface. The IOLAN will, by default, allow management access for LAN type interfaces (e.g. Ethernet). From within each interface configuration screen you can instruct the IOLAN to treat that interface as a WAN or as a LAN management connection.

<i>Management Access</i>	
Access Restriction	Enable or disable access restrictions.
Allow from LAN	<p>Allow management access from LAN type interfaces over these protocols.</p> <ul style="list-style-type: none"> <li>• <i>HTTP</i> – Allow non-secure Web sessions</li> <li>• <i>HTTPS</i> – Allow secure Web sessions</li> <li>• <i>SSH</i> – Allow SSH sessions</li> <li>• <i>TELNET</i> – Allow Telnet sessions</li> <li>• <i>SNMP</i> – Allow SNMP sessions</li> </ul> <p>Default for LAN interfaces is allow.</p>
Allow from WAN	<p>Allow management access from WAN type interfaces over these protocols.</p> <ul style="list-style-type: none"> <li>• <i>HTTP</i> – Allow non-secure Web sessions</li> <li>• <i>HTTPS</i> – Allow secure Web sessions</li> <li>• <i>SSH</i> – Allow SSH sessions</li> <li>• <i>TELNET</i> – Allow Telnet sessions</li> <li>• <i>SNMP</i> – Allow SNMP sessions</li> </ul> <p>Default for WAN interfaces is not allow.</p>

<i>Console Port</i>	
Access Command Line	<p>Access Command Line Mode using:</p> <ul style="list-style-type: none"> <li>• <i>Telnet</i> – Telnet session</li> <li>• <i>SSH</i> – SSH Session</li> <li>• <i>Console</i> – Physical console port</li> </ul>

<b>Speed</b>	<p>Select the speed for the console port. <i>Telnet</i> – Telnet session</p> <ul style="list-style-type: none"> <li>• 9600</li> <li>• 19200</li> <li>• 38400</li> <li>• 57600</li> <li>• 115200</li> </ul>
<b>Parity</b>	<p>Select the parity for the console port.</p> <ul style="list-style-type: none"> <li>• None</li> <li>• Even</li> <li>• Odd</li> </ul>
<b>Data bits</b>	<p>Select the data bits for the console port.</p> <ul style="list-style-type: none"> <li>• 8</li> <li>• 7</li> </ul>
<b>Stop bits</b>	<p>Select the stop bits for the console port.</p> <ul style="list-style-type: none"> <li>• 1</li> <li>• 2</li> </ul>

### 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 IOLAN. If a certificate is not uploaded, the IOLAN 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.

<b><i>WebManager</i></b>	
<b>Webmanager</b>	<p>Specify protocols to be supported by the WebManager.</p> <ul style="list-style-type: none"> <li>• HTTP - Allow non-secure Web sessions</li> <li>• HTTPS - Allow secure Web sessions <ul style="list-style-type: none"> <li>• Port – Port to use for HTTPS sessions</li> </ul> </li> </ul> <p>Default port is 443 Values are 1024 – 65535</p>

	<ul style="list-style-type: none"> <li>• <i>Idle Timeout</i> – Amount of time to wait before disconnecting an idle Web session Default port is 1440 Values are 1 – 1440</li> </ul>
--	--

<b><i>SNMP</i></b>	
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

***Logging***

The IOLAN 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 IOLAN's non-volatile flash memory
- to an external Syslog server
- telnet sessions
- or the serial console port

Logging is enabled by default.

<b><i>Logging</i></b>	
Enable logging	Enable or disable the logging feature.
<b>General</b>	
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	<ul style="list-style-type: none"> <li>• Emergency</li> <li>• Alert</li> <li>• Critical</li> <li>• Error</li> <li>• Warning</li> <li>• Notification</li> <li>• Informational</li> <li>• Debugging</li> </ul>

Timestamp	
Include timestamp in log messages	Enable timestamps in log messages. Select timestamp type and include information.
Timestamp type	<ul style="list-style-type: none"> <li>• Uptime or Date/time</li> <li>• Include milliseconds</li> <li>• Include year</li> <li>• Include time zone</li> <li>• Use local time or UTC time</li> </ul>
Syslog	
Enable logging to Syslog hosts	Enable/disable the sending of messages to one or more IPv4 or IPv6 Syslog servers.
Level	<ul style="list-style-type: none"> <li>• Emergency</li> <li>• Alert</li> <li>• Critical</li> <li>• Error</li> <li>• Warning</li> <li>• Notification</li> <li>• Informational</li> <li>• Debugging</li> </ul>
Syslog source interface	Specify the source interface for sending messages to syslog from the drop-down list.



---

<b>Syslog facility</b>	<ul style="list-style-type: none"><li>• Local7</li><li>• Kernel</li><li>• User</li><li>• Mail</li><li>• Daemon</li><li>• Authorization</li><li>• Syslog</li><li>• LPR</li><li>• News</li><li>• UUCP</li><li>• System 9</li><li>• System 10</li><li>• System 11</li><li>• System 12</li><li>• System 13</li><li>• System 14</li><li>• Local7</li><li>• Kernel</li><li>• User</li><li>• Mail</li><li>• Daemon</li><li>• Authorization</li><li>• Syslog</li><li>• LPR</li><li>• News</li><li>• UUCP</li><li>• System 9</li><li>• System 10</li><li>• System 11</li><li>• System 12</li><li>• System 13</li><li>• System 14</li><li>• Cron</li><li>• Local 0</li><li>• Local 1</li><li>• Local 2</li><li>• Local 3</li><li>• Local 4</li></ul>
------------------------	--

	<ul style="list-style-type: none"> <li>• Local 5</li> <li>• Local 6</li> <li>• Local 7</li> </ul>
<b>Origin ID Source</b>	<ul style="list-style-type: none"> <li>• None</li> <li>• IP</li> <li>• IPv6</li> <li>• Hostname</li> <li>• Custom</li> </ul>
<b>Custom Origin ID</b>	You can append the hostname, an IP address, or a text string to Syslog messages that are sent to remote Syslog servers.
<b>Append delimiter to syslog messages over TCP</b>	Add line feed delimiter to syslog messages.
<b>Syslog (Add, Edit, Delete)</b>	
<b>Hostname/IP address</b>	Hostname or IPv4/IPv6 address.
<b>Transport</b>	Choose a transport method. <ul style="list-style-type: none"> <li>• UDP</li> <li>• TCP</li> </ul>
<b>Port</b>	Port number for the syslog message. Default is 514
<b>Console</b>	
<b>Enable logging on the console port</b>	This command turns console logging on and specifies the level of logging to be directed to the console. The default setting is enabled.
<b>Level</b>	<ul style="list-style-type: none"> <li>• Emergency</li> <li>• Alert</li> <li>• Critical</li> <li>• Error</li> <li>• Warning</li> <li>• Notification</li> <li>• Informational</li> <li>• Debugging</li> </ul>

Telnet/SSH	
Enable logging on Telnet/SSH sessions	This command copies monitor logging messages to the current virtual, (vty, SSH or telnet session).
Level	<ul style="list-style-type: none"> <li>• Emergency</li> <li>• Alert</li> <li>• Critical</li> <li>• Error</li> <li>• Warning</li> <li>• Notification</li> <li>• Informational</li> <li>• Debugging</li> </ul>
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	<ul style="list-style-type: none"> <li>• Emergency</li> <li>• Alert</li> <li>• Critical</li> <li>• Error</li> <li>• Warning</li> <li>• Notification</li> <li>• Informational</li> <li>• Debugging</li> </ul>
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 IOLAN 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.)

<b>Level</b>	<ul style="list-style-type: none"> <li>• Emergency</li> <li>• Alert</li> <li>• Critical</li> <li>• Error</li> <li>• Warning</li> <li>• Notification</li> <li>• Informational</li> <li>• Debugging</li> </ul>
<b>Filename</b>	Enter the name for the log file.
<b>Minimum Size</b>	Enter the minimum size of the log file. Values: 1024 – 2147483647 Default: 2048
<b>Maximum Size</b>	Enter the minimum size of the log file. Values are 4096 – 2147483647 Default is 4096

## *Email*

### *Overview*

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

<i>Email</i>	
<b>Enable</b>	Enabling Email notifications.
<b>Encryption</b>	Emails are to be encrypted using: <ul style="list-style-type: none"> <li>• none</li> <li>• SSL</li> <li>• TLS</li> </ul>
<b>From</b>	Specify the Email address that the Email will appear to be From.
<b>SMTP Server Host</b>	IP Address of the SMTP host that will be used to send the Email.
<b>SMTP Server Port</b>	Port number on the SMTP host required for the connection.

<b>Username / Password</b>	<b>Username and password required to authenticate with the SMTP server.</b>
<b>Validate Email Certificate</b>	<b>Validate the certificate provided by the SMTP server.</b>
<b><i>Email Recipients (Add, Edit or Delete)</i></b>	
<b>Email Address</b>	<b>Email address of the recipient.</b>
<b>Email Subject Line</b>	<b>Subject line that will be contained in the Email.</b>
<b>Notifications Sent</b>	<b>List of events that this recipient will receive.</b> <ul style="list-style-type: none"><li>• <b>alarms</b></li><li>• <b>authentications</b></li><li>• <b>bgp</b></li><li>• <b>entity</b></li><li>• <b>envmon</b></li><li>• <b>ipsec</b></li></ul>
	<ul style="list-style-type: none"><li>• <b>openvpn</b></li><li>• <b>ospf</b></li><li>• <b>snmp</b></li></ul>

---

## Interfaces

### *Introduction*

Fundamentally the IOLAN works with interfaces. Any routing rules, firewalls, Natting all relate back to interfaces. The IOLAN supports a number of different types of interfaces and each may have its 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 IOLAN. These interfaces can connect to devices, switches, or other routers. They can be used as a gateway to a LAN or to provide WAN functionality to routers. The IOLAN also supports 16 serial ports.

An Ethernet interface can be:

- Included into a bridge
- Used as a LAN or a WAN

### *Serial*

The serial interfaces are one of the basic elements of the IOLAN. Devices can connect directly to the serial ports using Telnet/SSH either by port or IP address or using HTTP or HTTPS.

### *VLAN*

Each Ethernet interface can support sub-interfaces and can support 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 them 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. By default the IOLAN comes configured with all of the Ethernet ports configured into one bridge. In order to use any of these interfaces on its own, it must first be removed from the bridge.

### *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 IOLAN supports three types of tunnels:

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

- **OpenVPN** – uses VPN techniques to secure point-to-point and site-to-site connections. The OpenVPN protocol is responsible for handling client-server communications. Basically, it helps establish a secure “tunnel” between the VPN client and the VPN server. OpenVPN handles encryption and authentication. It also, 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.

<i>Ethernet Interface</i>	
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.
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 IOLAN 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	
DHCP	Your IP address will be assigned from a DHCP server.
Static	Provide a IP address and network mask for this interface.
DHCP Client	
Hostname	This can be any string. By default, this is the IOLAN name.

<p><b>Class ID</b></p>	<ul style="list-style-type: none"> <li>• Auto</li> <li>• Specify</li> </ul> <p>Specify a Hex string or ASCII text. This same hex string or text would be configured on the server side and associated with an address to give the client. This can be configured to be the MAC address of an interface name, an ASCII text or hex string.</p> <p>option – 60 - Vendor class identifier                  &lt;oem-name&gt;:&lt;model&gt;:&lt;serial#&gt; in ASCII</p> <p>IOLAN example: Perle:IOLAN SCR1618 RDAC :99-011319T001A4</p>
<p><b>Client ID</b></p>	<p>This can be configured to be the MAC address of an interface name, an ASCII text or hex string.</p> <p>option – 61 - Client class identifier                  &lt;oem-name&gt;:&lt;model&gt;:&lt;serial#&gt; in ASCII</p> <p>IOLAN example: Perle:IOLAN SCR1618 RDAC :99-011319T001A4</p> <p>option – 61 - Client identifier                  &lt;mac-addr&gt;-&lt;ifname&gt; in ASCII</p> <p>IOLAN example: 0040.0298.9939-eth1</p>
<p><b>Enable DHCP Server</b></p>	<p><i>DHCP Server</i></p>
<p><b>Enable IPv6</b></p>	
<p><b>Enable IPv6</b></p>	<p>Select how to obtain the IPv6 address:</p> <ul style="list-style-type: none"> <li>• Auto configuration</li> <li>• DHCP</li> <li>• Static                         <ul style="list-style-type: none"> <li>• Address</li> <li>• Prefix</li> <li>• eui-64</li> </ul> </li> </ul>
<p><b>IPv6 Neighbor Discovery</b></p>	<p>IOLAN Preference</p> <ul style="list-style-type: none"> <li>• High</li> <li>• Medium</li> <li>• Low</li> </ul> <p>Default is Medium</p>
<p><b>Manage config flags</b></p>	<p>Enable or disable config flags.                  Default is disabled</p>



<b>Manage other config flags</b>	<b>Enable or disable other config flags. Default is disabled</b>
<b>DAD attempts</b>	<b>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</b>
<b>Reachable time</b>	<b>Value of the reachable time field of the IPv6 router advertisement messages. Range is 1 – 3600000 Default is 0</b>
<b>Retransmission time</b>	<b>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</b>
<b>IPv6 Routing Prefix Advertisement</b>	
<b>Add Prefix</b>	
<b>Address</b>	<b>Specify an IPv6 address.</b>
<b>Prefix Length</b>	<b>Specify the prefix length. Range is 0 – 128</b>
<b>Valid Lifetime (secs)</b>	<b>Range is 1 – 4294967294 or infinite Default is 2592000</b>
<b>Preferred lifetime (secs)</b>	<b>Range is 1 – 4294967294 or infinite Default is 604800</b>
<b>Do not use prefix for online determination</b>	<b>Enable or disable prefix for online determination. Default is off</b>
<b>Do not use prefix for autoconfiguration</b>	<b>Enable or disable prefix for autoconfiguration. Default is off</b>
<b>IPv6 Routing Advertisement Control</b>	

<b>Suppress IPv6 Router Advertisement</b>	Enable or disable IPv6 router advertisements. Default is off
<b>Hop Limit</b>	Indicates the maximum number of links over which the IPv6 packet can travel before being discarded. Range is 1-255 Default is 64
<b>RA Interval (secs)</b>	Maximum interval between IPv6 RA transmissions. Range is 1 – 1800 Defaults is 600
<b>Minimum Interval (secs)</b>	Minimum interval between IPv6 RA transmissions. Range is 1 – 1350 Default is 198
<b>RA Lifetime (secs)</b>	The lifetime associated with the default router in seconds. A value of 0 indicates that the router is not a default router and will not appear on the default router list. The router lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options. Range is 1 – 9000 Default is 1800
<b>Add DNS</b>	
<b>Address</b>	Add IPv6 address of DNS server.
<b>Role</b>	<ul style="list-style-type: none"> <li>• WAN</li> <li>• LAN</li> <li>• TRUSTED</li> </ul> Default is LAN
<b>MTU size</b>	Provide an Maximum Transmission Unit (MTU) size. Default is 1600

<b><i>VLAN Interface</i></b>	
<b>Enable</b>	Enabled or disabled interface. Default is enabled
<b>Ethernet</b>	Select the Ethernet interface. Range 1-18

<b>VLAN ID:</b>	Select the Ethernet interface to be associate with the VLAN ID.
<b>Description</b>	Provide a description for this interface.
<b>Enable IPv4 address</b>	
<b>DHCP</b>	Your IP address will be assigned from a DHCP server.
<b>Static</b>	Provide a IP address and network mask for this interface.
<b>DHCP Client</b>	
<b>Hostname</b>	This can be any string. By default, this is the switch name.
<b>Class ID</b>	Hex string or ASCII text. This same hex string or text would be configured on the server side and associated with an address to give the client. This can be configured to be the MAC address of an interface name, an ASCII text or hex string. option – 61 - Client identifier <mac-addr>-<ifname> in ASCII IOLAN example: 0040.0298.9939-eth1
<b>Client ID</b>	This can be configured to be the MAC address of an interface name, an ASCII text or hex string. option – 60 - Vendor class identifier <oem-name>:<model>:<serial#> in ASCII IOLAN example: Perle:IOLAN SCR1618 RDAC :99-011319T001A4
<b>Enable DHCP Server</b>	<i>DHCP Server</i>
<b>Enable IPv6</b>	Select how to obtain the IPv6 address: <ul style="list-style-type: none"> <li>• Auto configuration</li> <li>• DHCP</li> <li>• Static                         <ul style="list-style-type: none"> <li>• Address</li> <li>• Prefix</li> <li>• eui-64</li> </ul> </li> </ul>

<b>IPv6 Neighbor Discovery</b>	<b>IOLAN Preference</b> <ul style="list-style-type: none"> <li>• High</li> <li>• Medium</li> <li>• Low</li> </ul>
<b>Manage config flags</b>	Enable or disable config flags. Default is disabled
<b>Manage other config flags</b>	Enable or disable other config flags. Default is disabled
<b>DAD attempts</b>	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
<b>Reachable time</b>	Value of the reachable time field of the IPv6 router advertisement messages. Range 1 – 3600000 Default is 0
<b>Retransmission time</b>	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
<b>IPv6 Routing Prefix Advertisement</b>	
<b>Add Prefix</b>	
<b>Address</b>	Specify an IPv6 address.
<b>Prefix Length</b>	Specify the prefix length. Range is 0 – 128
<b>Valid Lifetime (secs)</b>	Range is 1 - 4294967294 or infinite Default is 2591800
<b>Preferred Lifetime (secs)</b>	Range is 1 - 4294967294 or infinite Default is 604800

<b>Do not use prefix for online determination</b>	<b>Enable or disable prefix for online determination. Default is off</b>
<b>Do not use prefix for autoconfiguration</b>	<b>Enable or disable prefix for autoconfiguration. Default is off</b>
<b>IPv6 Routing Advertisement Control</b>	
<b>Suppress IPv6 Router Advertisement</b>	<b>Enable or disable IPv6 Router advertisements. Default is off</b>
<b>Hop Limit</b>	<b>Indicates the maximum number of links over which the IPv6 packet can travel before being discarded. Range is 1-255 Default is 64</b>
<b>RA Interval (secs)</b>	<b>Maximum interval between IPv6 RA transmissions. Range is 1 - 1800 Defaults is 600</b>
<b>Minimum Interval (secs)</b>	<b>Minimum interval between IPv6 RA transmissions. Range is 1 - 1350 Default is 198</b>
<b>RA Lifetime (secs)</b>	<b>The lifetime associated with the default router in seconds. A value of 0 indicates that the router is not a default router and will not appear on the default router list. The router lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options. Range is 1 – 9000 Default is 1800</b>
<b>Add DNS</b>	
<b>Address</b>	<b>Add IPv6 address of DNS server.</b>
<b>Role</b>	<b>Used for controlling admin access. Default is LAN Options:</b> <ul style="list-style-type: none"> <li>• LAN</li> <li>• WAN</li> <li>• TRUSTED</li> </ul>

<b>MTU Size</b>	Optional: provide an MTU size. Default is 1500 Range is 64 – 9000
<b><i>Bridge Interface</i></b>	
<b>Enable/Disable Interface</b>	The interface will be enabled or disabled. Default – enabled.
<b>Bridge ID</b>	Provide a number for bridge id Range is 1 – 9999
<b>Description</b>	Provide a description for this interface.
<b>Select Interfaces</b>	Select the interfaces that you want to associate with this bridge. Ethernet 1-16
<b>Enable IPv4 address</b>	
<b>Enable DHCP</b>	Your IP address will be assigned from a DHCP server.
<b>Enable Static</b>	Provide an IP address and network mask for this interface.
<b>DHCP Client</b>	
<b>Hostname</b>	This can be any string. By default, this is the switch name.
<b>Class ID</b>	Hex string or ASCII text. This same hex string or text would be configured on the server side and associated with an address to give the client. This can be configured to be the MAC address of an interface name, an ASCII text or hex string. option – 61 - Client identifier <mac-addr>-<ifname> in ASCII IOLAN example: 0040.0298.9939-eth1

<p><b>Client ID</b></p>	<p>This can be configured to be the MAC address of an interface name, an ASCII text or hex string.  <b>option – 60 - Vendor class identifier</b>                  &lt;oem-name&gt;:&lt;model&gt;:&lt;serial#&gt; in ASCII                  IOLAN example: Perle:IOLAN SCR1618 RDAC :99-011319T001A4</p>
<p><b>Enable DHCP Server</b></p>	<p><i>DHCP Server</i></p>
<p><b>Enable IPv6</b></p>	<p>Select how to obtain the IPv6 address:</p> <ul style="list-style-type: none"> <li>• Auto configuration</li> <li>• DHCP</li> <li>• Static                         <ul style="list-style-type: none"> <li>• Address</li> <li>• Prefix</li> <li>• eui-64</li> </ul> </li> </ul>
<p><b>IPv6 Neighbor Discovery</b></p>	<p>IOLAN Preference</p> <ul style="list-style-type: none"> <li>• High</li> <li>• Medium</li> <li>• Low</li> </ul> <p>Default is Medium</p>
<p><b>Manage config flags</b></p>	<p>Enable or disable config flags.                  Default is disabled</p>
<p><b>Manage other config flags</b></p>	<p>Enable or disable other config flags.                  Default is disabled</p>
<p><b>DAD attempts</b></p>	<p>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</p>
<p><b>Reachable time</b></p>	<p>Value of the reachable time field of the IPv6 router advertisement messages.                  Range 1 – 3600000                  Default is 0</p>

<b>Retransmission time</b>	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
<b>IPv6 Routing Prefix Advertisement</b>	
<b>Add Prefix</b>	
<b>Address</b>	Specify an IPv6 address.
<b>Prefix Length</b>	Specify the prefix length. Range is 0 – 128
<b>Valid Lifetime (secs)</b>	Range is 1 – 4294967294 or infinite Default is 2591800
<b>Preferred Lifetime (secs)</b>	Range is 1 – 4294967294 or infinite Default is 604800
<b>Do not use prefix for online determination</b>	Enable or disable prefix for online determination. Default is off
<b>Do not use prefix for autoconfiguration</b>	Enable or disable prefix for autoconfiguration. Default is off
<b>IPv6 Routing Advertisement Control</b>	
<b>Suppress IPv6 Router Advertisement</b>	Enable or disable IPv6 Router advertisements. Default is off
<b>Hop Limit</b>	Indicates the maximum number of links over which the IPv6 packet can travel before being discarded. Range is 1-255 Default is 64
<b>RA Interval (secs)</b>	Maximum interval between IPv6 RA transmissions. Range is 1 – 1800 Defaults is 600
<b>Minimum Interval (secs)</b>	Minimum interval between IPv6 RA transmissions. Range is 1 – 1350 Default is 198



<b>RA Lifetime (secs)</b>	The lifetime associated with the default router in seconds. A value of 0 indicates that the router is not a default router and will not appear on the default router list. The router lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options. Range is 1 – 9000 Default is 1800
<b>Add DNS</b>	
<b>Address</b>	Add IPv6 address of DNS server.
<b>Role</b>	Used for controlling admin access. Default is LAN Options: <ul style="list-style-type: none"> <li>• LAN</li> <li>• WAN</li> <li>• TRUSTED</li> </ul>
<b>MTU Size</b>	Optional: provide an MTU size. Default is 1500 Range is 64 – 9000

<b><i>PPPoE Interface</i></b>	
<b>Enable/Disable Interface</b>	Enabled or disabled interface. Default is enabled
<b>PPPoE ID</b>	The ID for this PPPoE connection.
<b>Interface</b>	Select an available Ethernet interface. Ethernet 1-18
<b>Description</b>	Provide a description for this interface.
<b>Encapsulation</b>	Set to PPP.
<b>User Name</b>	Enter a username for this connection.
<b>Password</b>	Enter a password for this connection.

Idle Timeout	Drop the connection after idle timer expires. Values 1-4294967
Access Concentrator	Specify the name for the access concentrator.
Enable IPv4 address	
DHCP	Your IP address will be assigned from a DHCP server.
tic	Provide a IP address and network mask for this interface.
DHCP Client	
Hostname	This can be any string. By default, this is the IOLAN's name.
Class ID	Hex string or ASCII text. This same hex string or text would be configured on the server side and associated with an address to give the client. This can be configured to be the MAC address of an interface name, an ASCII text or hex string. option – 61 - Client identifier <mac-addr>-<ifname> in ASCII IOLAN example: 0040.0298.9939-eth1
Client ID	This can be configured to be the MAC address of an interface name, an ASCII text or hex string. option – 60 - Vendor class identifier <oem-name>:<model>:<serial#> in ASCII IOLAN example: Perle:IOLAN SCR1618 RDAC :99-011319T001A4
Enable DHCP Server	<i>DHCP Server</i>

<b><i>Tunnel Interface</i></b>	
Tunnel Type	<ul style="list-style-type: none"> <li>• GRE</li> <li>• OpenVPN</li> <li>• 6in4</li> </ul> Default is GRE
Enable/Disable Interface	Enabled or disabled interface. Default is enabled

<b>OpenVPN Mode</b>	Select tun or tap.
<b>Tunnel ID</b>	Provide a tunnel ID.
<b>Description</b>	Provide a description for this interface.
<b>Source IP Address</b>	Provide the source IP address. <ul style="list-style-type: none"> <li>• IP Based</li> <li>• Interface based                 <ul style="list-style-type: none"> <li>• Eth 1-18</li> <li>•</li> </ul> </li> </ul>
<b>Destination IP Address</b>	Provide the destination IP address.
<b>Type of Service</b>	Specify the type of service.
<b>Time to live</b>	Specify the time to live.
<b>Set Multicast operation over tunnel</b>	Set multicast operation over tunnel.
<b>Enable IPv4 address</b>	
<b>DHCP</b>	Your IP address will be assigned from a DHCP server.
<b>Static</b>	Provide a IP address and network mask for this interface.
<b>Enable IPv6</b>	Static <ul style="list-style-type: none"> <li>• Address</li> <li>• Prefix</li> <li>• eui-64</li> </ul>
<b>IPv6 Neighbor Discovery</b>	IOLAN Preference <ul style="list-style-type: none"> <li>• High</li> <li>• Medium</li> <li>• Low</li> </ul> Default is Medium
<b>Manage config flags</b>	Enable or disable config flags. Default is disabled
<b>Manage other config flags</b>	Enable or disable config flags. Default is disabled

<b>DAD attempts</b>	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
<b>Reachable time</b>	Value of the reachable time field of the IPv6 router advertisement messages. Range 1 – 3600000 Default is 0
<b>Retransmission time</b>	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
<b>IPv6 Routing Prefix Advertisement</b>	
<b>Add Prefix</b>	
<b>Address</b>	Specify an IPv6 address.
<b>Prefix Length</b>	Specify the prefix length. Range is 0 – 128
<b>Valid Lifetime (secs)</b>	Range is 1 – 4294967294 or infinite Default is 2591800
<b>Preferred Lifetime (secs)</b>	Range is 1 – 4294967294 or infinite Default is 604800
<b>Do not use prefix for online determination</b>	Enable or disable prefix for online determination. Default is off
<b>Do not use prefix for autoconfiguration</b>	Enable or disable prefix for autoconfiguration. Default is off
<b>IPv6 Routing Advertisement Control</b>	
<b>Suppress IPv6 Router Advertisement</b>	Enable or disable IPv6 Router advertisements. Default is off

<b>Hop Limit</b>	Indicates the maximum number of links over which the IPv6 packet can travel before being discarded. Range is 1-255 Default is 64
<b>RA Interval (secs)</b>	Maximum interval between IPv6 RA transmissions. Range is 1 – 1800 Defaults is 600
<b>Minimum Interval (secs)</b>	Minimum interval between IPv6 RA transmissions. Range is 1 – 1350 Default is 198
<b>RA Lifetime (secs)</b>	The lifetime associated with the default router in seconds. A value of 0 indicates that the router is not a default router and will not appear on the default router list. The router lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options. Range is 1 – 9000 Default is 1800
<b>Role</b>	Used for controlling admin access <ul style="list-style-type: none"> <li>• LAN</li> <li>• WAN</li> <li>• TRUSTED</li> </ul> Default is TRUSTED
<b>MTU Size</b>	Optional: provide an MTU size. Default is 1500 Range is 64-9000
<b><i>Serial RS232</i></b>	
<b>The Usage Mode</b>	<ul style="list-style-type: none"> <li>• Disable</li> <li>• Serial-Line</li> </ul>
<b>Serial Port Settings</b>	

<p><b>Speed</b></p>	<p><b>Configure speed:</b></p> <ul style="list-style-type: none"> <li>• 300</li> <li>• 600</li> <li>• 1200</li> <li>• 1800</li> <li>• 2400</li> <li>• 4800</li> <li>• 9600</li> <li>• 19200</li> <li>• 28800</li> <li>• 38400</li> <li>• 57600</li> <li>• 115200</li> <li>• 230400</li> </ul>
---------------------	---

<p><b>Parity</b></p>	<p><b>Configure parity:</b></p> <ul style="list-style-type: none"> <li>• None</li> <li>• Even</li> <li>• Odd</li> <li>• Mark</li> <li>• Space</li> </ul>
<p><b>Data bits</b></p>	<p><b>Configure databits:</b></p> <ul style="list-style-type: none"> <li>• 5</li> <li>• 6</li> <li>• 7</li> <li>• 8</li> </ul>
<p><b>Stop bits</b></p>	<p><b>Configure stop bits:</b></p> <ul style="list-style-type: none"> <li>• 1</li> <li>• 2</li> </ul>
<p><b>Enable CTS Toggle</b></p>	<p><b>Configure the Toggle CTS Feature if your application needs for CTS to be raised during character transmission.</b></p>

<b>Initial Delay</b>	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.
<b>Final Delay</b>	Configure the time (in ms) between the time of character transmission and when CTS is dropped.
<b>Flow control</b>	
<b>Enable Inbound Flow Control</b>	Determines if input flow control is to be used. Default: Enabled
<b>Enable Outbound Flow Control</b>	Determines if output flow control is to be used. Default: Enabled
<b>Enable DTR-DSR monitor</b>	The serial will not go active until DTR-DSR are both active.
<b>Discard Characters Received with errors</b>	When enabled, the IOLAN will discard characters received with a parity or framing error. Default is disabled
<b>Enable Echo Suppression</b>	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

## 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 IOLAN.

The local Host Table in your IOLAN 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 IOLAN.

***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**

<b><i>DNS</i></b>	
<b>Enable DNS</b>	Enabled or disabled DNS. Default is enabled
<b>IPv4 Address (Add, Delete)</b>	Enter an IPv4 address for your DNS server. Select the + symbol to add more.
<b>IPv6 DNS Servers (Add, Delete)</b>	Enter an IPv6 address for your DNS server. Select the + symbol to add more.
<b><i>DNS Forwarding</i></b>	
<b>Cache Size</b>	By setting the cache size, this will allow the IOLAN to store frequently used resolved DNS queries, thereby allowing clients to resolve DNS queries locally rather than remotely from a global DNS server. DNS server 0-10000 Default is 10000
<b>Seconds to Cache NVDOMAIN entries</b>	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
<b>Ignore IP Host Tables</b>	Do not check the IP host table for host resolution.
<b>Use DNS Servers received from DHCP servers for the following interfaces</b>	Select the interfaces that meet this criteria.



<b><i>DNS Listeners</i></b>	
<b>IPv4 address</b>	Enter an IPv4 address to listen for DNS requests.
<b><i>DNS Domain Forwarding</i></b>	
<b>Domain</b>	This server will receive domain requests.
<b>IPv4 Address</b>	Forward domain request to this server.
<b><i>Dynamic DNS</i></b>	
<b>Host Groups (Add, Edit or Delete)</b>	Specify a Group name.
<b>Add Hostname entries</b>	Add hosts that will be added to this group.
<b>Add DDNS to interface</b>	
<b>Interface</b>	Select from the drop-down list, the interface to add DDNS functionality.
<b>Web Check to obtain external IP</b>	Enter the URL that you want to obtain an IP address from. This will allow the IOLAN to be seen on the internet as a public address.
<b>Service used for Dynamic DNS</b>	
<b>Service</b>	Set to dyndns.
<b>Login</b>	Specify a username to use for logging into the Dyndns Host server.
<b>Password</b>	Specify a password to use for logging into the dyndns host server.
<b>Registered DNS service</b>	Specify whether you will be providing a host name or a host group name.
<b>Host name or Host group name</b>	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 IOLAN. 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 IOLAN 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 IOLAN.

### 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.

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

## WAN

### Overview

Your IOLAN 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.

<i>Health Profiles</i>	
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

<b>Tests (Add, Edit, Delete)</b>	
<b>Test priority</b>	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).
<b>Target</b>	Enter a target IPv4 address or hostname.
<b>Type</b>	Select the type of test to run. <ul style="list-style-type: none"> <li>• ping</li> <li>• traceroute</li> </ul>
<b>Response</b>	Select the response timeout between pings.
<b>Test Limit</b>	Enter a numerical value from 1 – 254
<b><i>Interface IP Health</i></b>	
<b>Interface</b>	Select the interface that you want to add a health profile to.
<b>Profile</b>	Select the pre-defined profile from the drop-down list.
<b>NextHop</b>	<ul style="list-style-type: none"> <li>• IP</li> <li>• DHCP</li> </ul>
<b>IP Address</b>	The IP address of the next hop.
<b><i>High Availability</i></b>	
<b>Mode</b>	<ul style="list-style-type: none"> <li>• Disable</li> <li>• Failover</li> <li>• Load Sharing</li> </ul>

<b>Failover</b>	<p>Failover is defined as a mode where 2 or more WAN interfaces are configured, but only 1 interface is active at a time. Once IP HEALTH has detected that a WAN interface no longer has internet connectivity, it will "failover" to the next active (via IP HEALTH status) WAN interface.</p> <p>Note: IP HEALTH profile(s) (ie. Ping or traceroute tests) and IP-HEALTH on EACH of the WAN interfaces, must be configured when using WAN HIGH-AVAILABILITY. The IP HEALTH feature is used to determine whether a WAN interface has internet connectivity (one or more of the ping or traceroute tests MUST pass)</p> <p>You need to define:</p> <ul style="list-style-type: none"><li>• one or more source interfaces. You will select the source/originating traffic that will be included in the dynamic WAN high-availability failover feature. An interface CANNOT be configured as both a source interface and WAN interface.</li><li>• one or more WAN interface. When you select a WAN interface, you are adding that interface to a pool of available WAN interfaces. When an active WAN interface becomes inactive (via IP Health) all routed traffic from the defined source interfaces are automatically routed to the next active WAN interface. While defining a single WAN interface is valid, it makes no sense to do so. The priority value of each WAN interface will dictate the failover order. The failover feature will make an ACTIVE WAN interface with the HIGHEST priority, the designated WAN interface. If a higher priority WAN interface recovers from being inactive, the failover feature will make it the designated WAN interface. Observed, cut over times are in the order of 10-20 seconds (due to IP HEALTH on an interface). Specify the source interface to fall over to. If you configure two interfaces with the same priority, the interface will failover to the other interface if required, but will never failover back to the original interface.</li></ul>
-----------------	---

WAN Interface	
Interface	Specify WAN interface.
Priority	Specify the priority for load-sharing. Values are 1-255
Load Sharing	<p>Load Sharing is defined as a mode where you define how routed traffic can be sent over one or more defined active WAN interfaces. Unlike failover, mode where ALL routed traffic is cut over to the next highest priority active WAN interface, this mode defines how specific or all traffic is to be shared/divided over multiple active WAN interfaces. This is accomplished by defining one or more load-sharing rules.</p> <p>Each load-sharing rule allows the user to define:</p> <ul style="list-style-type: none"> <li>• a SINGLE source interface</li> <li>• MULTIPLE WAN interfaces (each with a weighting value that determines percentage output relative to all WAN interfaces).</li> </ul> <p>Example of weighting value on each WAN interface:  Wan interface 1's weighting = 10, results in <math>10 / (10+20+40) = 1/7</math> output of this rule</p> <p>Wan interface 2's weighting = 20, results in <math>20 / (10+20+40) = 2/7</math> output of this rule</p> <p>Wan interface 3's weighting = 40, results in <math>40 / (10+20+40) = 4/7</math> output of this rule</p> <p>optional source packet matching rules based on protocol, source/destination IP, port, etc.</p> <p>Note: Load sharing requires at least one valid rule to enable it.</p>
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

<b>Enable inbound connection tracking</b>	Track inbound connections.
<b>Rules</b>	
<b>Rule Number</b>	Supply a rule number.
<b>Description</b>	Description of this rule.
<b>Enable excluding of matching rules load sharing</b>	Check for rule matching.
<b>Enable per-packet load-sharing</b>	Load-sharing based at packet level.
<b>WAN</b>	
<b>Interface</b>	Specify a WAN interface.
<b>Weight</b>	<p>Specify a weight.            Example of weighting value on each WAN interface:            Wan interface 1's weighting = 10, results in <math>10 / (10+20+40) = 1/7</math> output of this rule</p> <p>Wan interface 2's weighting = 20, results in <math>20 / (10+20+40) = 2/7</math> output of this rule</p> <p>Wan interface 3's weighting = 40, results in <math>40 / (10+20+40) = 4/7</math> output of this rule</p> <p>optional source packet matching rules based on protocol, source/destination IP, port, etc.</p> <p>Note: Load sharing requires at least one valid rule to enable it.</p>
<b>Enable Matching Protocol</b>	Select protocol to match.
<b>Limit</b>	
<b>Burst</b>	Number of packets that match the criteria allowed out the WAN interface based on the rate calculation window.

<b>Rate calculation window</b>	<ul style="list-style-type: none"> <li>• hour</li> <li>• minute</li> <li>• second</li> </ul>
<b>Rate</b>	<b>Number of packets that match the criteria allowed out the WAN interface based on number of packets.</b>
<b>Threshold behavior for limit</b>	<ul style="list-style-type: none"> <li>• above</li> <li>• below</li> </ul>

## 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 IOLAN will prevent the software from "arping" for a host-name 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 IOLAN will prevent the software from "arping" for a hostname or IP address.

<i>Static ARP</i>	
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.
<i>ARP Timeout</i>	
ARP Timeout	If an ARP entry is not used for a specific amount of time the entry is removed from the caching table.
Disable ARP filter	If enabled the IOLAN 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 <ul style="list-style-type: none"> <li>• 0 (default): reply for any local target IP address, configured on any interface</li> <li>• 1 reply only if the target IP address is local address configured on the incoming interface</li> </ul>
Enable Proxy ARP	Enable Proxy ARP if you need your IOLAN to respond to local networks with its MAC address. Default is Disabled





## Routing

<i>Default Gateway</i>	
	Enter the default gateway for your IOLAN.

### *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 the IOLAN 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 IOLAN supports these networking routing techniques.

**RIP** – See [RIP](#) for more information

**BGP** – See [BGP](#) for more information

**OSPF** – See [OSPF](#) for more information

<i>Static Routing</i>	
Static Routing (Add, Edit, Delete)	
Destination Prefix	The prefix for the destination network.

<b>Destination Prefix Mask</b>	<b>The prefix mask for the destination network.</b>
<b>Route</b>	
<b>Route via:</b>	<p><b>The interface the traffic is to leave by:</b></p> <ul style="list-style-type: none"> <li>• <b>Gateway</b> – The IP address of the forwarding router</li> <li>• <b>Interface</b> –The interface to use for this route</li> <li>• <b>Null</b> – Select null to discard IP packets (used to prevent routing loops from occurring in your network)</li> </ul>
<b>Default Gateway for Interface obtained by DHCP</b>	<b>Enable if you want this interface to obtain default gateway though DHCP.</b>
<b>Administrative Distance</b>	<p>(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</p> <p>Default is 1 Range is 1-255 (with 1 being the most reliable) 255 is route not used or unknown</p>
<b>IPv6</b>	
<b>Enable IPv6 Unicast Routing</b>	<b>Enable unicast routing if your IOLAN needs to be able to route IPV6 traffic AND to participate in IPv6 IGP (Interior Gateway Protocols)</b>
<b>IPv6 Static Routing (Add, Edit, Delete)</b>	
<b>Destination Prefix</b>	<b>The prefix for the destination network.</b>
<b>Destination Prefix Mask</b>	<b>The prefix mask for the destination network.</b>
<b>Route</b>	

<p><b>Route via:</b></p>	<p><b>The interface the traffic is to leave by:</b></p> <ul style="list-style-type: none"> <li>• <b>Gateway</b> – The IP address of the forwarding router</li> <li>• <b>Interface</b> –The interface to use for this route</li> <li>• <b>Null</b> – Select null to discard IP packets (used to prevent routing loops from occurring in your network)</li> </ul>
<p><b>Administrative Distance</b></p>	<p><b>(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</b></p> <p><b>Default is 1</b>  <b>Range is 1-255 (with 1 being the most reliable)</b>  <b>255 is route not used or unknown</b></p>

### *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 IOLAN supports 99 port forwarding rules.

<p><i>Port Forwarding</i></p>	
<p><b>Protocol</b></p>	<p><b>Set the protocol to be used for this rule.</b></p> <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> </ul>
<p><b>Inbound Interface</b></p>	<p><b>Select the inbound interface.</b></p> <ul style="list-style-type: none"> <li>• Br (bridge)</li> <li>• Eth 9-16, 25-32</li> </ul>
<p><b>Inbound port</b></p>	<p><b>Specify the port number for the incoming data.</b>  <b>Range is 1-65535</b></p>
<p><b>Destination address</b></p>	<p><b>Specify the IPv4 address of the end device receiving the data.</b></p>

<b>Destination port</b>	<b>Specify the port number for the end device receiving the data. Range is 1-65535</b>
-------------------------	--

### *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 the IOLAN (NAT outside) and another interface on the IOLAN (NAT inside).

<b><i>NAT</i></b>	
<b>NAT Rules (Add, Edit, Delete)</b>	
<b>ACL List</b>	<b>Set the ACL from the drop-down list to be used with the specified interface.</b>
<b>Global Address</b>	
<b>Interface or Pool</b>	<ul style="list-style-type: none"> <li>• Select the interface from the drop-down list</li> <li>• Select the pool from the drop-down list</li> </ul>
<b>Do not turn on firewall to drop invalid connections</b>	<b>By default connections will not be dropped by the firewall.</b>
<b>Add Pool</b>	
<b>Pool name</b>	<b>Enter the name for this pool.</b>
<b>Start IP Address</b>	<b>Enter the start address of this pool.</b>
<b>End Address</b>	<b>Enter the end address of this pool.</b>
<b>Netmask</b>	<b>Enter netmask for this pool.</b>
<b>Add Nat66 Rules</b>	

<b>Inside Prefix</b>	Enter the inside prefix for name for this rule.
<b>Inside Prefix Length</b>	Specify a prefix length.
<b>Outside Prefix</b>	<ul style="list-style-type: none"> <li>• Prefix</li> <li>• Any</li> </ul>
<b>Outside Interface</b>	Select the outside interface to be used for this rule.
<b>Outside Prefix Length</b>	Specify the prefix length.
<b>Do not turn on firewall to drop invalid connections</b>	By default connections will not be dropped by the firewall
<b>Netmask</b>	Enter netmask for this pool.
<b><i>ALG</i></b>	
<b>Enable certain protocols to transverse Nat and Firewalls</b>	
<b>Select the protocols to enable</b>	<p>By default all protocols are enabled, to disable uncheck the checkbox</p> <ul style="list-style-type: none"> <li>• ftp</li> <li>• gre</li> <li>• h323</li> <li>• nfs</li> <li>• pptp</li> <li>• sip</li> <li>• sqlnet</li> <li>• tftp</li> </ul>

### ***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 IOLAN.
- Ability to control which areas a client access.

**Terminology**

**Standard access-list**

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

**Extended access lists**

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

**Feature details / Application notes**

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

<i>ACL</i>	
<b>ACL Type</b>	Specify the type of ACL. <ul style="list-style-type: none"> <li>• Standard</li> <li>• Extended</li> </ul>
<b>ACL number</b>	Enter an ACL number for this entry. <ul style="list-style-type: none"> <li>• Standard range is 1-99</li> <li>• Extended range is 1300-1999</li> </ul>
<b>Sequence number</b>	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.
<b>Action</b>	Permit or denies the IP packet from the specified source (host/address) <ul style="list-style-type: none"> <li>• Permit</li> <li>• Deny</li> </ul>
<b>Source Type</b>	Specify the source type for matching <ul style="list-style-type: none"> <li>• Any</li> <li>• Host</li> <li>• Wildcard</li> </ul>
<b>Source hostname/address</b>	IPv4 address or hostname

IPv6 Access Control Lists	
ACL Number	Enter an ACL number for this entry. <ul style="list-style-type: none"> <li>• Standard range is 1-99</li> <li>• Extended range is 1300-1999</li> </ul>
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) <ul style="list-style-type: none"> <li>• Permit</li> <li>• Deny</li> </ul>
Source Type	Specify the source type for matching <ul style="list-style-type: none"> <li>• Any</li> <li>• Prefix</li> </ul>
IPv6 Prefix	Specify an IPv6 prefix
Prefix Length	Specify a prefix length
Exact Match	Match exactly on the prefix

### *Prefix List*

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

#### **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.



<i>Prefix-List</i>	
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	<ul style="list-style-type: none"> <li>• Permit – Allows routes or IP packets that match the prefix list</li> <li>• Deny – Rejects routes or IP packets that match the prefix list.</li> </ul>
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 IOLAN 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 IOLAN 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 IOLAN makes changes to the routing information only when all of the default match-\* rules happen to match the attributes of the route.

<i>Route Maps</i>	
<b>Route Maps (Add, Edit, Delete)</b>	
<b>Name</b>	Specify a name for this route map rule.
<b>Rule Number</b>	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.
<b>Description</b>	Enter a description for this rule.
<b>Set Operation</b>	Set the operation mode on whether this rule is an Permit (accept) rule or a Deny (reject rule) <ul style="list-style-type: none"> <li>• Permit</li> <li>• Deny</li> </ul>
<b>Match Values from Routing Table</b> Add Traffic Match	
<b>Select Matching Criteria</b>	<ul style="list-style-type: none"> <li>• AS Path</li> <li>• BGP Community List</li> <li>• BGP/VPN Extended Community List</li> <li>• Interface</li> <li>• IP Address Route</li> <li>• Next-hop Address of route</li> <li>• match-iproutesource</li> <li>• match-ipv6address</li> <li>• match-ipv6nexthop</li> <li>• Metric of Route</li> <li>• BGP Origin Code</li> <li>• Peer Address</li> <li>• Tag of Route</li> </ul>
<b>Set Values in Destination Routing Protocol</b> Set Attribute	

<p><b>Set Attribute</b> <b>Select Set Criteria</b></p>	<ul style="list-style-type: none"> <li>• BGP Aggregator</li> <li>• Transform BGP AS-Path</li> <li>• BGP Atomic Aggregate</li> <li>• Delete BGP community list</li> <li>• BGP Community</li> <li>• BGP Extended Community</li> <li>• IP (next hop)</li> <li>• IPv6 (next hop)</li> <li>• BGP Local Preference</li> <li>• Metric</li> <li>• Metric Type</li> <li>• BGP Origin Code</li> <li>• BGP Originator ID</li> <li>• Source Address for Route</li> <li>• BGP Weight</li> </ul>
<p><b>Jump to another Route-map after match+set</b></p>	
<p><b>Route Map</b></p>	<p>Specify the route map to jump to after match.</p>
<p><b>Continue to a different entry within the route-map</b></p>	<p>Select a rule from the drop-down list.</p>
<p><b>Rule List</b></p>	<p>Select a rule from the drop-down list.</p>
<p><b>Exit policy on matches</b></p>	<p>What action to take when rule matches.</p> <ul style="list-style-type: none"> <li>• none</li> <li>• Next</li> <li>• Goto</li> </ul>
<p><b>Community List (Add, Edit, Delete)</b></p>	<p>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.</p>
<p><b>Community List Type</b></p>	<p>Specify the type of list;</p> <ul style="list-style-type: none"> <li>• Standard</li> <li>• Expanded</li> </ul>

<p><b>Community List Sequence number</b></p>	<p>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</p>
<p><b>Community List Rules</b></p>	
<p><b>Sequence number</b></p>	<p>Specify a sequence number. Entries will be read from lowest to highest. It is best practice to leave gaps between rule numbers such as 10, 20, 30, so that further entries can be inserted between rule numbers. Range is 1-65535.</p>
<p><b>Action</b></p>	<p>What action will be taken with this route.</p> <ul style="list-style-type: none"> <li>• Permit</li> <li>• Deny</li> </ul>
<p><b>Community</b></p>	<p>Select how the BGP routes will be advertised to the community</p> <ul style="list-style-type: none"> <li>• internet – advertise this route to the Internet community; by default, all prefixes are members of the Internet community</li> <li>• local-AS– routes are advertised to only peers that are part of the local autonomous system</li> <li>• no-advertise - do not advertise this to any other routers</li> <li>• no-export - do not advertise to external neighbors, but is ok to advertise to internal neighbors.</li> </ul>
<p><b>Ext-Community List (Add, Edit, Delete)</b></p>	<p>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.</p>

<p><b>Community List Type</b></p>	<p>Specify the type of list;</p> <ul style="list-style-type: none"> <li>• Standard</li> <li>• Expanded</li> </ul>
<p><b>Community List Sequence number</b></p>	<p>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</p>
<p><b>Action</b></p>	<p>What action will be taken with this route.</p> <ul style="list-style-type: none"> <li>• Permit</li> <li>• Deny</li> </ul>
<p><b>Type</b></p>	<p>Select how the BGP routes will be advertised to the community</p> <p><b>Route Target</b></p> <ul style="list-style-type: none"> <li>• VPN Extended Community (ASN.nn)</li> </ul> <p><b>Site of Origin</b></p> <ul style="list-style-type: none"> <li>• VPN Extended Community (ASN.nn)</li> </ul> <p>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.</p>

***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 the IOLAN sees its own AS number in the AS path, it will not accept the prefix.

<p><b><i>AS-Paths</i></b></p>	
<p><b>Name</b></p>	<p>Specify a AS-path name.</p>

<b>Sequence number</b>	<b>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</b>
<b>Action</b>	<b>What action to take when rule matches.</b> <ul style="list-style-type: none"> <li>• Permit</li> <li>• Deny</li> </ul>
<b>Regular Expression</b>	<b>Enter a text string.</b>

### ***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.

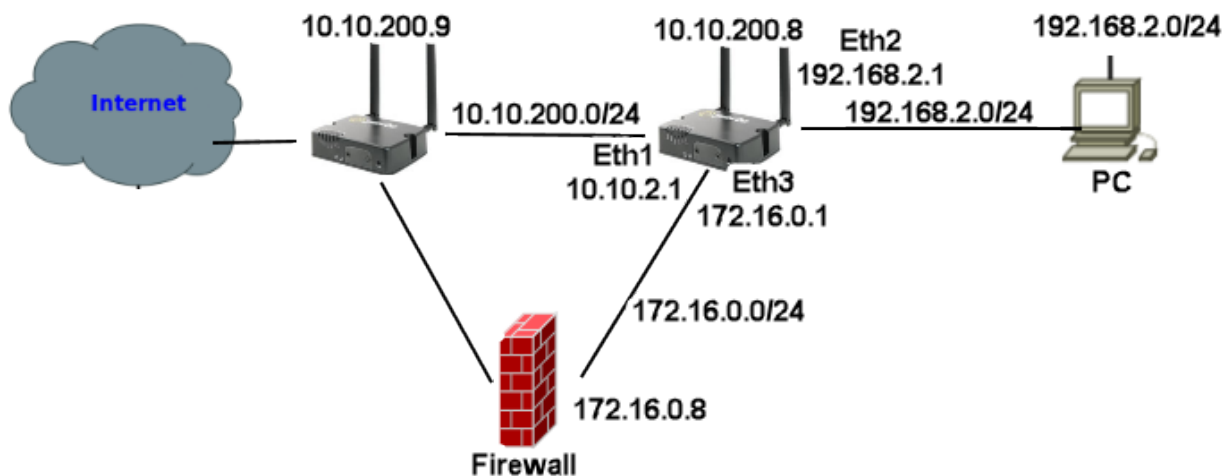
#### **Overview**

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.

<b><i>Policy Routing</i></b>	
<b>Enable</b>	<b>Enabled or disabled Policy routing. Default is disabled</b>
<b>Rule Number</b>	<b>Specify a rule number. Range is 1-9999</b>
<b>Description</b>	<b>Enter a description for this rule.</b>
<b>Log packeting matching this rule</b>	<b>Log the packets that match this rule.</b>
<b>Traffic Match</b>	

<p><b>Select Matching Criteria</b></p>	<ul style="list-style-type: none"> <li>• Source IPv4-address</li> <li>• Source MAC address</li> <li>• Destination IPv4-address</li> <li>• Protocol</li> <li>• Fragment</li> <li>• IPsec</li> <li>• Recent</li> <li>• State</li> </ul>
<p><b>Policy Action</b></p>	<ul style="list-style-type: none"> <li>• Drop Matched Packets</li> <li>• Route</li> </ul>
<p><b>Assign to routing table (default static)</b></p>	<p>Matching packets should be assigned to this default routing table.</p>
<p><b>Schedule</b></p>	<ul style="list-style-type: none"> <li>• Use UTC</li> <li>• Enable Schedule</li> </ul> <p>Select Schedule Type</p> <ul style="list-style-type: none"> <li>• Date</li> <li>• Weekdays</li> <li>• Days of Month</li> </ul>

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



1. Create a static route as ip route 0.0.0.0 0.0.0.0 10.10.200.9  
 Create a route table entry (2) as 0.0.0.0 0.0.0.0 172.16.0.8  
 Create a route policy named http-firewall, under this create a rule (2)
2. Create a traffic match for criteria matching protocol tcp and destination port 80 >

3. Under interfaces assign an IP address of 192.168.2.1 255.255.255.0 to interface Ethernet 2.
4. Under Routing/Routing Policy/Interface/ Assign Policy Route http-firewall to Ethernet interface 2.

### ***Route Tables***

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

#### **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.

<b><i>Route Tables</i></b>	
<b>Route Tables (Add, Edit, Delete)</b>	
<b>Destination Prefix</b>	<b>Specify a destination prefix.</b>
<b>Destination Network Mask</b>	<b>Specify a destination prefix mask.</b>
<b>Route</b>	
<b>Route via:</b>	<ul style="list-style-type: none"> <li>• <b>Forwarding Address</b></li> <li>• <b>Interface</b></li> <li>• <b>Null</b></li> </ul>
<b>Interface</b>	<b>Select the interface</b>
<b>Router Address</b>	<b>Specify the address of the forwarding router.</b>
<b>Default Gateway for Interface obtained by DHCP</b>	<b>Select this option if you want to use the default gateway obtained by DHCP. Default is off</b>



<b>Administrative Distance</b>	Enter an Administrative Distance. (AD) is a value that your IOLAN will 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 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
<b>IPv6 Route Tables (Add, Edit, Delete)</b>	
<b>Destination Prefix</b>	Specify a destination prefix.
<b>Destination Network Mask</b>	Specify a destination prefix mask.
<b>Route</b>	
<b>Route via:</b>	<ul style="list-style-type: none"> <li>• Forwarding Address</li> <li>• Interface</li> <li>• Null</li> </ul>
<b>Interface</b>	Select the interface
<b>Router Address</b>	Specify the address of the forwarding router.
<b>Administrative Distance</b>	Enter an Administrative Distance. (AD) is a value that your IOLAN will 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 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 your IOLAN. A network is unreachable at 16 hops according to the RIP hop limit.

<i><b>RIP</b></i>	
<b>Enable RIP</b>	Enable or disabled RIP. Default is disabled
<b>Distance</b>	Enter an Administrative Distance. (AD) is a value that your IOLAN will 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 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
<b>Metric</b>	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
<b>Originate Default-information</b>	Using originate default-information will advertise a default route, if there is one in the routing table. Default is no
<b>Timers</b>	
<b>Update</b>	Rate (in seconds) at which routing updates are sent. Default is 30 seconds Range is 1 to 2147483
<b>Invalid</b>	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

<b>Flush</b>	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
<b>Passive Interfaces, Networks and Neighbors</b>	
<b>Passive Interface (Add, Delete)</b>	Select an interface from the drop-down list
<b>Network</b>	Specify the Network's IPv4 address and netmask. <ul style="list-style-type: none"> <li>• IPv4 Address</li> <li>• IPv4 Mask</li> </ul>
<b>Neighbors</b>	Specify the Neighbor address <ul style="list-style-type: none"> <li>• IPv4 Address</li> </ul>
<b>Distributed and Redistributed Lists</b>	
<b>Filter</b>	Filter the packets based on: <ul style="list-style-type: none"> <li>• ACL</li> <li>• Prefix</li> </ul> Default is ACL
<b>ACL List Prefix List</b>	Select ACL list from the drop-down list. Select a Prefix List from the drop-down box
<b>Direction</b>	Select the direction to apply the ACL list to; <ul style="list-style-type: none"> <li>• In</li> <li>• Out</li> </ul>
<b>Specify Interface</b>	Select an interface to apply the ACL list to. Only defined interfaces will be shown.
<b>Add Redistributed List</b>	
<b>Type</b>	Type of routing protocol to redistribute to another routing protocol. It includes advertising your static routes and default routes also. <ul style="list-style-type: none"> <li>• BGP</li> <li>• Connected</li> <li>• Kernel</li> <li>• OSPF</li> <li>• Static</li> </ul>

<b>Metric</b>	<p><b>Metric (hop count)</b> is the number of routers through which data must pass from source network to reach the destination.</p> <p>Range is 1-16 Default is 1</p>
<b>Interface RIP (Edit)</b>	
<b>Interface</b>	Select the interface to add authentication.
<b>Mode</b>	<p>To specify the type of authentication used in the Routing Information Protocol (RIP) Version 2 packets</p> <ul style="list-style-type: none"> <li>• null</li> <li>• text</li> <li>• md5</li> </ul>
<b>Enable Split Horizon</b>	<p>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.</p> <p>Default is enabled</p>
<b>Enable Poison reverse for split-horizon</b>	<p>Enabling poison reverse for split-horizon sets the IOLAN to actively advertise routes as unreachable from the interface over which they were learned by – setting the IOLAN’s metric to infinite (16 for RIP). The effect of such an announcement is to immediately remove most looping routes before they can propagate through the network.</p> <p>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.</p> <p>Default is disabled.</p>
<b>Key Chain (Add, Edit, Delete)</b>	Specify the set of keys that can be used on an interface for RIP authentication.
<b>Name</b>	Add a key chain name.
<b>Add Key</b>	<p>Specify the Key ID and Password.</p> <ul style="list-style-type: none"> <li>• ID for this key. Range is 1-2147483647</li> <li>• Password password will be encrypted</li> </ul>

---

## ***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. OSPF was designed to replace the RIP protocol as it optimizes the updating up of the routing table. OSPF should be enabled on your IOLAN.

#### **BGP** (Broader Gateway Protocol)

BGP is an independent routing protocol that is used exclusively for the internet. If using your IOLAN to connect to the internet, BGP should be enabled.

### **Feature details / Application notes**

**Areas** are a logical collection of routers that carry the same Area ID or number inside of an OSPF network, the OSPF network itself can contain multiple areas, the first and main Area is called the backbone area “Area 0”, all other areas must connect to Area 0.

#### **Area Type**

**Normal area** By default, when you use a multiple area design, your created area’s will be considered “normal” area’s. This just means that these area’s support the flooding of all standard LSA types (1,2,3,4,5). Your backbone is considered a “normal” area. The main problem with “normal” area’s are they must carry all redistributed routes, including the redistributed routes instability. So to limit the amount of routing information into area’s, besides summarization, different “stubby” 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 OSPF 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/multi-cast capability, such as frame-relay, ATM, SMDS, & X.25.

<i><b>OSPF</b></i>	
<b>Enable OSPF/OSPFv3</b>	<b>Enable or disabled OSPF/OSPFv3</b> <b>Default is disabled</b>
<b>Router ID</b>	<b>Router-id for this OSPF process.</b>

<b>Enable Auto cost</b>	Enable Auto-cost and specify a reference bandwidth that will be used to dynamically calculate OSPF interface cost. Default is no
<b>Reference Bandwidth</b>	Default reference bandwidth is 100 Mbps.
<b>Enable RFC 1583 compatibility</b>	Enable for RFC 1583 compatibility.
<b>Enable Opaque Capability</b>	Enable for Opaque capability
<b>Distance</b>	
<b>Administrative</b>	Enter an Administrative Distance. (AD) is a value that your IOLAN will 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 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
<b>OSPF External</b>	Routes injected by redistribution. Range is 1 – 255 Default is 110
<b>OSFP inter-area routes</b>	Routes from another area are inter-area. Range is 1 – 255 Default is 110
<b>OSFP intra-area routes</b>	Routes within an area are intra-area. Range is 1-255 Default is 110
<b>Specify Default Metric</b>	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
<b>Original Default-Information</b>	Default is off
<b>Max-Metric</b>	

<b>Administrative</b>	Advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations.
<b>On Shutdown</b>	Advertise stub-router prior to full shutdown of OSPF. Range is 5 - 86400 Default is 600
<b>On Startup</b>	Configures the IOLAN to advertise a maximum metric at startup. Range is 5 - 86400 Default is 600
<b>Refresh Timer</b>	The IOLAN 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
<b>Throttle Timers</b>	<ul style="list-style-type: none"> <li>• Delay between receiving a change to SPF calculation in milliseconds. Range is 1-600000</li> <li>• Delay between first and second SPF calculation. Range is 1-600000</li> <li>• Maximum wait time in milliseconds for SFP calculations. Range is 1-600000 Default is off</li> </ul>
<b>OSPF Areas (Add, Edit, Delete)</b>	
<b>Select Area ID format</b>	Specify a unique number or IP address to identify this area <ul style="list-style-type: none"> <li>• Number ID (use 0 to specify a backbone area)</li> <li>• IP address (use 0.0.0.0 to specify a backbone area)</li> </ul>



<p><b>Area Type</b></p>	<ul style="list-style-type: none"> <li>• 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</li> <li>• stub – can contain type 1, 2, and 3 LSAs. A default route is substituted for external routes</li> <li>• 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</li> </ul>
<p><b>Export List (OSFPv3)</b></p>	<p>Select the export list.</p>
<p><b>Import List (OSPFv3)</b></p>	<p>Select the import list.</p>
<p><b>Add Range (OSPFv3)</b></p>	
<p><b>Range</b></p>	<p>Add IPv6 range. (X:X:X:X::X)</p>
<p><b>Prefix length</b></p>	<p>Add Prefix length.</p>
<p><b>Default Authentication</b></p>	<p>Select the method for authentication.</p> <ul style="list-style-type: none"> <li>• None</li> <li>• Text</li> <li>• Message Digest</li> </ul> <p>Default is no authentication</p>
<p><b>Default cost</b></p>	<p>Cost for the default summary route used for a stub or NSSA. Range is from 0 to 16777215</p>
<p><b>Shortcut</b></p>	<p>This parameter allows to "shortcut" routes (non-backbone) for inter-area routes.</p> <ul style="list-style-type: none"> <li>• enable – the area will be used for shortcutting every time the route that goes through it is cheaper</li> <li>• disable – this area is never used by ABR for routes shortcutting.</li> <li>• 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</li> </ul>

<b>Virtual Link (Add, Edit, Delete)</b>	
<b>IP address</b>	IPv4 address of this virtual link
<b>Hello Packet Interval</b>	(Optional) Specifies the time (in seconds) between the hello packets that your IOLAN 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.
<b>Dead Router Detection Time</b>	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
<b>LSA retransmit Interval</b>	Specify the time between link-state advertisement (LSA) retransmissions for adjacencies that belong to the virtual link. Default is 5
<b>LSA transmission Delay</b>	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.
<b>Authentication</b>	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. <ul style="list-style-type: none"> <li>• None – no password</li> <li>• Text – text</li> <li>• Message-digest –(Optional) Identifies the key ID and key (password) used between this router and neighboring routers for MD5 authentication.</li> </ul> The Default is none.
<b>Area Range (Add, Edit, Delete)</b>	
<b>Prefix</b>	Specify a prefix specified as IP address.

<b>Mask</b>	Specify a subnet mask
<b>Mode</b>	<ul style="list-style-type: none"> <li>• sets the address range status to advertise and generates a Type 3 summary LSA</li> <li>• sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed and the component networks remain hidden from other networks.</li> <li>• substitute (network prefix to be announced instead of range)</li> </ul> Default is advertise
<b>User Specified Cost</b>	Specify the metric for this area range. Range is 0-16777215
<b>Substitute Prefix</b>	Specify the substitute prefix when mode set to substitute.
<b>Substitute Mask</b>	Specify the substitute mask when mode set to substitute.
<b>Distributed and Redistributed Lists</b>	
<b>Distributed List (Add, Edit, Delete)</b>	
<b>ACL List</b>	Select ACL (Access Control List) from drop-down list.
<b>Direction</b>	<p>Out – the distributed list out option works only on the routes being redistributed by the ASBR into the OSPF. It can only be applied to external type 2 and external type 1 routes but not to intra-area and inter area routes.</p> <p>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.</p>
<b>Type</b>	Select the type of route <ul style="list-style-type: none"> <li>• BGP</li> <li>• Connected (directly attached subnet or host)</li> <li>• Kernel</li> <li>• OSPF</li> <li>• Static</li> </ul>

Redistributed List (Add, Edit, Delete)	
Type	<p>Select the type of route</p> <ul style="list-style-type: none"> <li>• BGP</li> <li>• Connected (directly attached subnet or host)</li> <li>• Kernel</li> <li>• OSPF</li> <li>• Static</li> </ul>
Metric	Specify the metric for this redistribution list
Metric Type	<p>Set metric type to;</p> <p>1 – OSPF External Type 1</p> <p>2 – OSPF External Type 2</p>
Interface – OSPF	
Network Type	<ul style="list-style-type: none"> <li>• broadcast – a designated router and backup designated router are elected which uses OSPF multicasting capabilities. (most common type)</li> <li>• non-broadcast – use this type of network on networks that have no broadcast/multicast capability, such as frame-relay, ATM, SMDS, &amp; X.25. The key point is that these layer 2 protocols are unable to send broadcasts/multicasts.</li> <li>• point-to-multipoint – allows you to configure selected routers with neighbor / cost commands, identifying a specific cost for the connection to the specified peer</li> <li>• 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.</li> </ul>

<b>Disable MTU mismatch detection</b>	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.
<b>Router Priority</b>	A router with a high priority will always win the DR/BDR election process Priority Range is 0-255 Default is 1
<b>Interface cost</b>	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 $100 \text{ Mbps} / 10 \text{ Mbps} = 10$
<b>Dead interval</b>	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
<b>Hello interval</b>	Specify the time between HELLO packets. Range is 1 – 65535 Default is 10 seconds
<b>Retransmit interval</b>	Set the time between retransmitting lost link state advertisements. Range is 1 – 65535 Default is 5 seconds
<b>Transmit delay</b>	Transmit-delay is 1 – 65535 Range is 1 – 65535 Default is 5 seconds
<b>Authentication</b>	

<b>Mode</b>	<p>Enable authentication in OSPF in order to exchange routing update information in a secure manner.</p> <ul style="list-style-type: none"> <li>• md5 – the most secure OSPF authentication mode. You must configure an entire area with the same type of authentication</li> <li>• text – plain text (a password) will be used for authentication</li> <li>• null – no authentication will be used</li> </ul>
-------------	--

## ***BGP***

### **Overview**

BGP is an independent routing protocol that is used exclusively for the internet. If using your IOLAN 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.

<b><i>BGP</i></b>	
<b>BGP (Add, Edit, Delete)</b>	
<b>ASN</b>	<p>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.</p> <p>Your service provider will assign you the first three digit for ASN, the last two digits should be unique. Values are 1-4294967295</p>
<b>Administrative Distance</b>	
<b>Remote Addresses (Add)</b>	

<p><b>Distance (Administrative)</b></p>	<p>Enter an Administrative Distance. (AD) is a value that your IOLAN will 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 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</p>
<p><b>IP Source</b></p>	<p>You must specify the IP addresses of the peers in order to establish a BGP session. Specify the network.</p>
<p><b>IP Mask</b></p>	<p>Specify a network mask for this network.</p>
<p><b>BGP Distance</b></p>	
<p><b>Distance for external routes to AS</b></p>	<p>Specify the administrative distance for external routes. Values are 1-255 Default is 20</p>
<p><b>Distance for internal routes to AS</b></p>	<p>Specify the administrative distance for internal routes. Values are 1-255 Default is 200</p>
<p><b>Distance for local routes</b></p>	<p>Specify the administrative distance for local routes. Values are 1-255 Default is 200</p>
<p><b>Timers</b></p>	
<p><b>Keep Alive</b></p>	<p>Specify a keepalive time. Range is 0-65535 Default is 60 seconds</p>
<p><b>Hold Time</b></p>	<p>Specify a hold time. Default is 180 seconds</p>

<b>Redistribution List (Add)</b>	<p>Select the type of route for redistribution.</p> <ul style="list-style-type: none"> <li>• BGP</li> <li>• Connected (directly attached subnet or host)</li> <li>• Kernel</li> <li>• OSPF</li> <li>• Static</li> </ul>
<b>Router Map</b>	<p>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.</p>
<b>Metric</b>	<p>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</p>
<b>IPv4 Family</b>	<p>Enter address family mode. Select IPv4 or IPv6.</p>
<b>Maximum Path</b>	<p>Specify the maximum paths to forward packets over. Default is 1</p>
<b>IBGP Maximum Path</b>	<p>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</p>
<b>BGP Settings</b>	
<b>BGP Router ID</b>	<p>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</p>
<b>Compare MED from different neighbors</b>	<p>Allow comparing MED from different sources. Default is off</p>
<b>Best Path (AS-path)</b>	



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

<b>Dampening</b>	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.
<b>Half-life</b>	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
<b>Value to Start re-using a route</b>	A dampen route will begin to be advertised to neighbors when it recovers to this value. Values 1-20000 Default is 750
<b>Value to start suppressing a route</b>	Specify a value, when reached will no longer advertise this route to any neighbors. Values are 1-20000 Default is 2000
<b>Max duration to suppress a stable route</b>	The maximum suppress-limit is used to ensure the prefix doesn’t get dampened indefinitely. Values are 1-255 Default is 60
<b>Activate IPv4-unicast</b>	Activate ipv4-unicast for a peer by default. Default is off
<b>Default Local Preference</b>	Specify a local preference level. The higher is more preferred. Values are 0-4294967295 Default is 100
<b>Pick the best-MED path among paths advertised from the neighboring AS</b>	Determine the best MED-path from paths advertised from the neighboring AS. Default is off

<b>Enforce the first AS for EBGp routes</b>	<b>Enforce that the first (left-most) autonomous system number (ASN) in AS-path is the previous neighbor's ASN. Default is off</b>
<b>Immediately reset session if a link to a directly connected external, peer goes down</b>	<b>Immediately reset the session information associated with BGP external peers if the link used to reach them goes down. Default is on</b>
<b>Graceful Restart capability parameters</b>	<b>The GR feature provides a routing device with the capability to inform its neighbors when it is performing a restart. Default is off</b>
<b>Set the max time to hold onto restarting peer's stale paths</b>	<b>Set the time to hold stale paths of restarting neighbors Value is 1 to 3600 seconds. Default is 360 seconds</b>
<b>Log neighbor up/down and reset reason</b>	<b>Log reason for neighbor up/down/reset state. Default is off</b>
<b>Check BGP network route exists in IGP</b>	<b>Check if the BGP network route exists in IGP. Default is on</b>
<b>Background scanner interval</b>	<b>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</b>
<b>Aggregate Address</b>	<b>BGP Route Aggregation reduces the number of BGP entries that have to be stored and exchanged with other BGP peers.</b>
<b>IPv4 Address</b>	<b>Specify a IPv4 aggregation address. This address can be used to summarize a set of networks into a single prefix</b>
<b>IPv4 Mask</b>	<b>Specify the netmask for the aggregate address.</b>
<b>Generate AS set path information</b>	<b>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.</b>
<b>Filter more specific routes from update</b>	<b>Filter longer-prefixes inside of the aggregate address before sending BGP updates.</b>

<b>Neighbor (Add)</b>	
<b>IPv4 neighbor address</b>	IPv4 address of a neighbor peer.
<b>BGP neighbor</b>	Configure a BGP neighbor also called peer.
<b>Enable neighbor</b>	Enable this BGP neighbor. Default is enabled
<b>Description of the neighbor</b>	Provide a description of this neighbor.
<b>Advertisement interval</b>	Specify a minimum time between sending BGP routing updates. Values are 0 - 600 seconds Default is 30 seconds
<b>Accept as-path with my AS occurrence</b>	Accept AS-path with my own AS present in it. Values are 1-10 Default is 3
<b>Override match AS-number when sending updates</b>	Override matching AS-numbers when sending updates.
<b>All BGP attributes are propagated unchanged to this neighbor</b>	Send BGP attributes unchanged. Default is enabled
<b>Specify BGP attribute is propagated unchanged to this neighbor</b>	<ul style="list-style-type: none"> <li>• AS-path</li> <li>• MED</li> <li>• Next-hop</li> </ul>
<b>Advertise capability to the peer</b>	<ul style="list-style-type: none"> <li>• Dynamic</li> <li>• ORF receive</li> <li>• ORF transmit</li> <li>• ORF both</li> </ul> Default is OFR Transmit
<b>Originate default route to this neighbor</b>	Send default route to this neighbor.
<b>One-hop away EBGP peer using loopback address</b>	Enables a directly connected eBGP neighbor to peer using a loopback address without adjusting the default TTL of 1.

<b>Do not perform capability negotiation</b>	Set this option on if you need to control advertisement of BGP capabilities to peers. Default is off
<b>Allow EBGP neighbors not on directly connected networks</b>	Allows you to establish eBGP peer relationships between routers that aren't directly connected to one another. Default is off.
<b>Filter outgoing updates</b>	Filter outgoing packet updates from neighbors. You must create the access list before it can be selected here. Default is off
<b>Filter incoming routes</b>	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.
<b>Filter outgoing routes</b>	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.
<b>Specify local as number</b>	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.
<b>Allow a maximum number of prefixes accepted from this peer</b>	Specify the number of prefixes that have been received from a peer has exceeded the maximum prefix limit.
<b>Disable the next hop calculation for this neighbor</b>	This command will change next hop attribute for received updates to its own IP address. Default is off
<b>Override capability negotiation result</b>	Use configured capabilities regardless of what capabilities have been negotiated.
<b>Don't send open messages to this neighbor</b>	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

<b>Set a password</b>	MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made.
<b>Neighbor's BGP port (TCP)</b>	Specify the TCP port that BGP peers will use to exchange BGP information. Default is 179
<b>Filter incoming routes</b>	Allow incoming routes to be filtered. Default is off
<b>Filter outgoing routes</b>	Allow outgoing routes to be filtered. Default is off
<b>Remove private AS number from outbound updates</b>	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
<b>Apply map incoming routes</b>	Apply route map to incoming routes.
<b>Apply map outgoing routes</b>	Apply route map to outgoing routes.
<b>Configure a neighbor as Route Reflector client</b>	Configure the BGP peer to be a route reflector responsible for passing iBGP learned routes to iBGP neighbors.
<b>Configure a neighbor as Route Server client</b>	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.
<b>Send Community attribute to this neighbor</b>	<ul style="list-style-type: none"> <li>• Extended</li> <li>• Standard</li> <li>• Both</li> </ul> Default is both
<b>Allow inbound soft reconfiguration for this neighbor</b>	Enables you to generate inbound updates from a neighbor, change and activate BGP policies without clearing the BGP session.

<p><b>Strict capability negotiation for this neighbor</b></p>	<p>By default, your IOLAN 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.</p>
<p><b>Keepalive interval</b></p>	<p>How often the IOLAN sends out keepalive messages to neighbor routers to maintain those sessions. Values are 1-65535 Default is 60</p>
<p><b>Hold Time</b></p>	<p>How long the IOLAN 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</p>
<p><b>Connect Timer</b></p>	<p>How long in seconds the IOLAN will try to reach this neighbor before declaring it offline. Values are 1-65535 Default is 120</p>
<p><b>Specify the maximum number of hops to the BGP peer</b></p>	<p>Enable, then specify the number of hops for not directly connected EBGP neighbors. Values are 1 – 254</p>
<p><b>Route-map to selectively unsuppressed suppressed routes</b></p>	<p>Use this command if a BGP neighbor requires some of the granular routes within the route-map summary. Default is off</p>
<p><b>Set source of routing updates</b></p>	<p>Select the source for routing updates.</p> <ul style="list-style-type: none"> <li>• IP based</li> <li>• Interface based</li> </ul>
<p><b>IP address</b></p>	<p>Specify an IP address for IP based source routing updates.</p>
<p><b>Set default weight for routes from this neighbor</b></p>	<p>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</p>
<p><b>Network (Add)</b></p>	
<p><b>IPv4 Address</b></p>	<p>Specify a IPv4 address for this network.</p>

<b>Mask</b>	<b>Specific the network mask</b>
<b>Specify a BGP backdoor route</b>	<b>Specify a route map to be used in order for an interior gateway routing protocol (IGP) to take precedence over an eBGP route.</b>
<b>Route Map</b>	<b>Use this route map as a backdoor.</b>
<b>IPv6 Address Family</b>	
<b>Aggregate Address</b>	
<b>IPv6 Address</b>	<b>Specify the IPv6 address.</b>
<b>IPv6 Mask</b>	<b>Specify the IPv6 mask.</b>
<b>Filter more specific routes from update</b>	<b>Filter longer-prefixes inside of the aggregate address before sending BGP updates.</b>
<b>Networks (Add)</b>	
<b>IPv6 address</b>	<b>Add a IPv6 peer network.</b>
<b>Prefix Length</b>	<b>Specify a prefix length for this network</b>
<b>Route Map</b>	<b>A route map consists of a series of statements that check to see if a route matches the policy, to permit or deny the route A route map must be predefined.</b>
<b>Redistribute List (Add)</b>	
<b>Type</b>	
<b>Router Map</b>	<b>A route map consists of a series of statements that check to see if a route matches the policy, to permit or deny the route A route map must be predefined.</b>
<b>Metric</b>	<b>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.</b>



---

## Services

### *Serial Port Services*

#### Overview

Each IOLAN serial port can be connected to a serial device. From the side navigation panel/Services/ Serial Ports Services 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** – This Console Management profile configures a serial port to provide network access to a console or administrative port. This profile sets up a serial port to support a TCP socket that listens for a Telnet or SSH connection from the network.
- **Trueport** – This Trueport profile configures a serial port to connect network servers or workstations running the TruePort software to a serial device as a virtual COM port. This profile is ideal for connecting multiple serial ports to a network system or server.
- **TCP Sockets** –This 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** – This UDP Sockets profile configures a serial port to allow communication to/from the network and serial devices connected to the IOLAN using the UDP protocol.
- **Terminal** – This Terminal profile configures a serial port to allow network access from a terminal connected to the IOLAN's serial port. This profile is used to access predefined hosts on the network from the terminal.
- **Printer** – This Printer profile configures a serial port to support a serial printer that can be accessed by the network.
- **Serial Tunneling** – This Serial Tunneling profile configures a serial port to establish a virtual link over the network to a serial port on another Perle IOLAN. Both IOLAN 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** – This Virtual Modem profile configures a serial port to simulate a modem. When the serial device connected to the IOLAN initiates a modem connection, the IOLAN start up a TCP connection to the other IOLAN configured with a virtual Modem serial port or to a host running a TCP application.
- **Modbus** – This Modbus Gateway profile configures a serial port to act as a Modbus Master Gateway or a Modbus Slave Gateway.
- **Remote Access (PPP)** – This Remote Access (PPP) profile configures a serial port to allow a remote user to establish a PPP connection to the IOLAN's serial

port. This is typically used with a modem for dial-in or dial-out access to the network.

- **Remote Access (Slip)** – This Remote Access (SLIP) Profile configures a serial port to allow a remote user to establish a SLIP connection to the IOLAN 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](#)

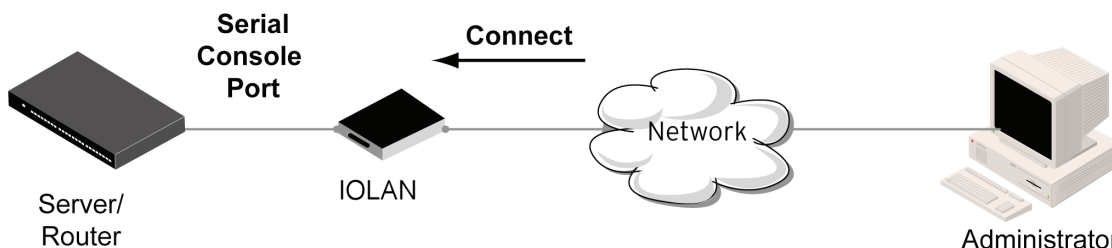
<i>Serial Port</i>	
<b>Name</b>	Specify a name for this serial port.
<b>Enable</b>	Enable this serial port.
<b>Service</b>	Select a service type.

**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 IOLAN attached to the IOLAN’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



*Console Management*

Settings	
Protocol	<p>Specify the connection method that users will use to communicate with a serial device connected to the IOLAN through the network.</p> <ul style="list-style-type: none"> <li>• SSH</li> <li>• Telnet</li> </ul> <p>Default is Telnet</p>
Listen For Connections on TCP Port	<p>The port number that the IOLAN will listen on for incoming TCP connections.</p> <p>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.</p> <p>Default: 10001, depending on the serial port number</p>
Enable IP Aliasing IP Address	<p>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 IOLAN's IP address and port number.</p> <p>Default is Disabled</p>
Advanced	
Authenticate User	<p>Enables/disables login/password authentication for users connecting from the network.</p> <p>Default is Disabled</p>
Enable Keepalive	<p>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 <i>Advanced Serial Options</i> 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.</p>

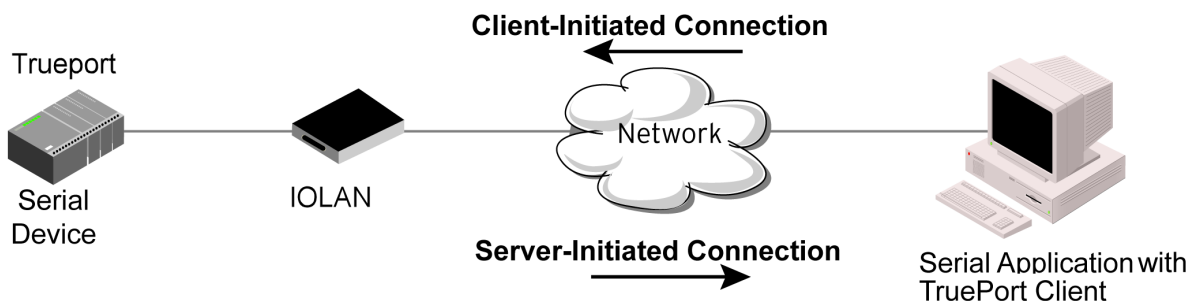
<p><b>Enable Message of the Day (MOTD)</b></p>	<p>Enables/disables the display of the message of the day. Default is Disabled</p>
<p><b>Session Timeout</b></p>	<p>Use this timer to forcibly close the session/ connection when the Session Timeout expires. Default is 0 seconds so the port will never timeout Range is 0-4294967 seconds (about 49 days)</p>
<p><b>Idle Timeout</b></p>	<p>Use this timer to close a connection because of inactivity. When the idle Timeout is reached, the IOLAN will end the connection. Range is 0-4294967 seconds (about 49 days) Default is 0 seconds so the port will never timeout</p>
<p><b>Dial Options</b></p>	<p>Configures Dial in and Dial Out parameters. See <i>Dial Options</i></p>
<p><b>Session Strings</b></p>	<p>Configures Send at Start, End and Delay after parameters for session control. See <i>Session Strings</i></p>
<p><b>Break Handing</b></p>	<p>Specifies how a break is interpreted.</p> <ul style="list-style-type: none"> <li>• None –The IOLAN ignores the break key completely and it is not passed through to the host</li> <li>• Local – The IOLAN deals with the break locally. If the user is in a session, the break key has the same effect as a hot key</li> <li>• Remote – When the break key is pressed, the IOLAN translates this into a telnet break signal which it sends to the host machine</li> <li>• 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)</li> </ul>
<p><b>Packet Forwarding</b></p>	<p>Packet forwarding can be used to control/define how and when serial port data packets are sent from the IOLAN to the network. See <i>Packet Forwarding</i></p>

### 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 IOLAN to establish a connection. In server mode, the client PC sends a connection request to the IOLAN.

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 IOLAN 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.



<b>Trueport</b>	
<b>Settings</b>	
<b>Connection</b>	<p>Connection determines how the TruePort connection is initiated and then sets up the appropriate connection parameters.</p> <ul style="list-style-type: none"> <li>• <b>Server Initiated</b> – The IOLAN will initiate the connection to the client.</li> <li>• <b>Client Initiated</b> – The client will initiate the connection to the IOLAN.</li> </ul> <p>Default is Client initiated</p>
<b>Server Initiated</b>	
<b>Host</b>	The configured host that the IOLAN will connect to (must be running TruePort).

<p><b>TCP Port</b></p>	<p>The TCP port that the IOLAN will use to communicate through to the Trueport client.                  Default – 10001 for serial port 1, then increments by one for each serial port</p>
<p><b>Connect to Multiple Hosts</b></p>	<p>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</p>
<p><b>Send Name on Connect</b></p>	<p>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</p>
<p><b>Client Initiated</b></p>	
<p><b>TCP Port</b></p>	<p>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</p>
<p><b>Client Allow Multiple Connections (Trueport Lite mode)</b></p>	<p>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.</p>
<p><b>Advanced</b></p>	<p>Configures those parameters that are applicable to specific environments. See <i>Advanced Serial Options</i></p>

<p><b>Raise Signals when not under Trueport control</b></p>	<p>This option has the following impact based on the state of the TruePort connection:</p> <ul style="list-style-type: none"> <li>• TruePort Lite Mode –When enabled, the EIA-232 signals remain active before, during, and after the TruePort connection is established. When disabled, the EIA-232 signals remain inactive during and after the Trueport connection is established.</li> <li>• 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.</li> </ul> <p>Default is enabled</p>
<p><b>Enable Message of the Day (MOTD)</b></p>	<p>Enables/disables the display of the message of the day. Default is Disabled</p>
<p><b>Enable TCP Keepalive</b></p>	<p>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.</p> <p>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.</p> <p>Default: Disabled</p>
<p><b>Enable Data Logging (Trueport Lite Mode)</b></p>	<p>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.</p> <p>Default</p> <p>Note: a kill line or a reboot of the IOLAN causes all buffered data to be lost</p> <p>Some profile features are not compatible with the data logging feature. See <a href="#">Data Logging Feature</a></p>

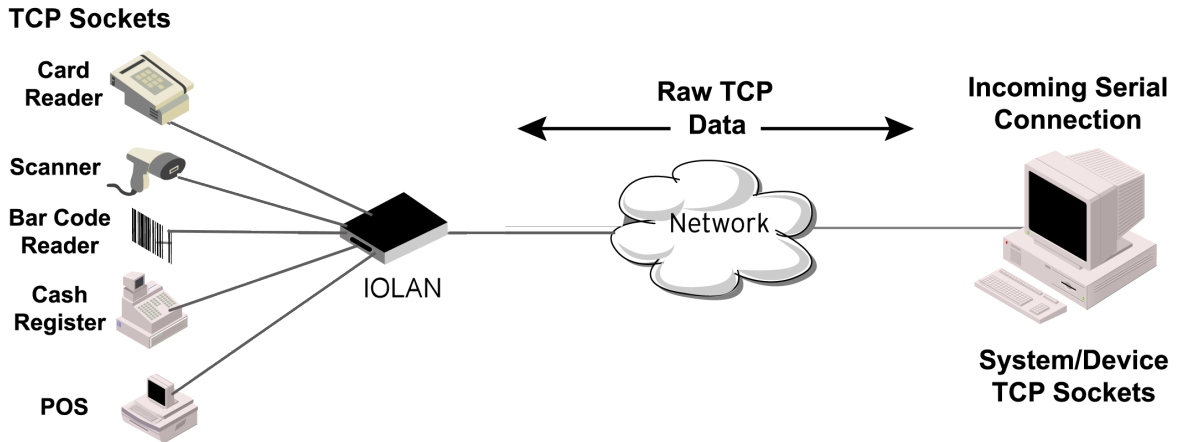
<p><b>Session Timeout</b></p>	<p>Use this timer to forcibly close the session/connection when the Session Timeout expires.                  Default is 0 seconds so the port will never timeout                  Range is 0-4294967 seconds (about 49 days)</p>
<p><b>Idle Timeout</b></p>	<p>Use this timer to close a connection because of inactivity. When the idle Timeout, the IOLAN will end the connection.                  Range is 0-4294967 seconds (about 49 days)                  Default is 0 seconds so the port will never timeout</p>
<p><b>Dial Options</b></p>	<p>Configures Dial in and Dial Out parameters. See <a href="#">Dial Options</a></p>
<p><b>Session Strings</b></p>	<p>Configures Send at Start, End and Delay after parameters for session control. See <a href="#">Session Strings</a></p>
<p><b>Packet Forwarding</b></p>	<p>Packet forwarding can be used to control/define how and when serial port data packets are sent from the IOLAN to the network.                  See <a href="#">Packet Forwarding</a></p>
<p><b>SSL/TLS</b></p>	<p>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</p> <ul style="list-style-type: none"> <li>• You can set up the IOLAN to act as an SSL/TLS client or server.</li> <li>• There is an extensive selection of SSL/TLS ciphers that you can configure for your SSL/TLS connection</li> </ul> <p>See <a href="#">SSL/TLS</a></p>

### ***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 IOLAN



<i>TCP Sockets</i>	
Settings	<ul style="list-style-type: none"> <li>• Listen for connection – the IOLAN is listening for a connection from the server</li> <li>• Connect to – the IOLAN is initiating a connection to the server</li> <li>• Bidirectional Connection – both sides can initiate or respond to the connection</li> </ul>
TCP Port	When enabled, the IOLAN 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 IOLAN's IP address and port number. Default is disabled

IP address	Users can access serial devices connected to the IOLAN 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 <a href="#">Advanced Serial Options</a>
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 IOLAN causes all buffered data to be lost Some profile features are not compatible with the data logging feature. See <a href="#">Data Logging Feature</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)

<p><b>Idle Timeout</b></p>	<p>Use this timer to close a connection because of inactivity. When the idle Timeout, the IOLAN will end the connection.                  Range is 0-4294967 seconds (about 49 days)                  Default is 0 seconds so the port will never timeout</p>
<p><b>Dial Options</b></p>	<p>Configures Dial in and Dial Out parameters. See <a href="#">Dial Options</a></p>
<p><b>Session Strings</b></p>	<p>Configures Send at Start, End and Delay after parameters for session control. See <a href="#">Session Strings</a></p>
<p><b>Packet Forwarding</b></p>	<p>Packet forwarding can be used to control/define how and when serial port data packets are sent from the IOLAN to the network.                  See <a href="#">Packet Forwarding</a></p>
<p><b>SSL/TLS</b></p>	<p>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</p> <ul style="list-style-type: none"> <li>• You can set up the IOLAN to act as an SSL/TLS client or server.</li> <li>• There is an extensive selection of SSL/TLS ciphers that you can configure for your SSL/TLS connection</li> </ul> <p>See <a href="#">SSL/TLS</a></p>

---

## *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 IOLAN will accept UDP packets from any source address.

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

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

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

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

- **Start IP Address** – This is the IP address of the host from which the UDP data will originate. If the data will originate from a number of hosts, this becomes the starting IP address of a range.
- **End IP Address** – If you wish to receive data only from the single host defined by "Start IP address", leave this entry as is (0.0.0.0). If you wish to accept data from a number of hosts, this address will represent the upper end of a range starting from "Start IP address". Only data originating from this range will be forwarded to the serial port.
- **UDP port** – This is the UDP 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;

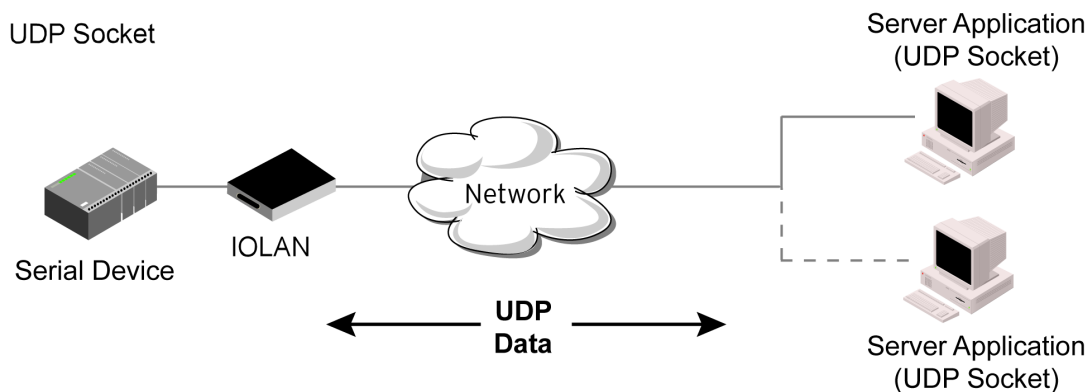
- **Start IP Address** – This is the IP address of the host to which the serial data will be sent using UDP datagrams. It is also the IP address of the host from which UDP data coming from the LAN will be accepted from. If the data is to be sent to or received from more than one host, this becomes the 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 IOLAN 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.



<i>UDP Sockets</i>	
Listen for Connections on UDP Port	The IOLAN will listen for UDP packets on the specified port. Default is 1000+ port-number. (for example, 10001 for serial port 1)

<p><b>Direction</b></p>	<p>The direction in which information is received or relayed:</p> <ul style="list-style-type: none"> <li>• Disabled – UDP service not enabled.</li> <li>• 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.</li> <li>• 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.</li> <li>• Both – Allows for data to flow from the serial device to the LAN and from the LAN to the serial device.</li> </ul>
<p><b>Start IP address</b></p>	<p>The first host IP address in the range of IP addresses (for IPv4 and IPv6) that the IOLAN will listen for messages from and/or send messages to. Field Format is IPv4 or IPv6 address</p>
<p><b>End IP address</b></p>	<p>The last host IP address in the range of IP addresses (for IPv4, not supported for IPv6) that the IOLAN will listen for messages from and/or send messages to. Field Format is IPv4 or IPv6 address</p>
<p><b>UDP Port</b></p>	<p>Determines how the IOLAN’s UDP port that will send/receive UDP messages is defined:</p> <ul style="list-style-type: none"> <li>• Auto Learn – The IOLAN 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.</li> </ul> <p>UDP Port determines how the IOLAN’s UDP port will send/receive UDP messages.</p> <ul style="list-style-type: none"> <li>• Auto Learn –The IOLAN 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.</li> <li>• Port – The port that the IOLAN will use to relay messages to servers/hosts. This option works with any Direction except disabled. The IOLAN will listen for UDP packets on the port configured by the Listen for connection on UDP port parameter. Default is Auto Learn</li> </ul>

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

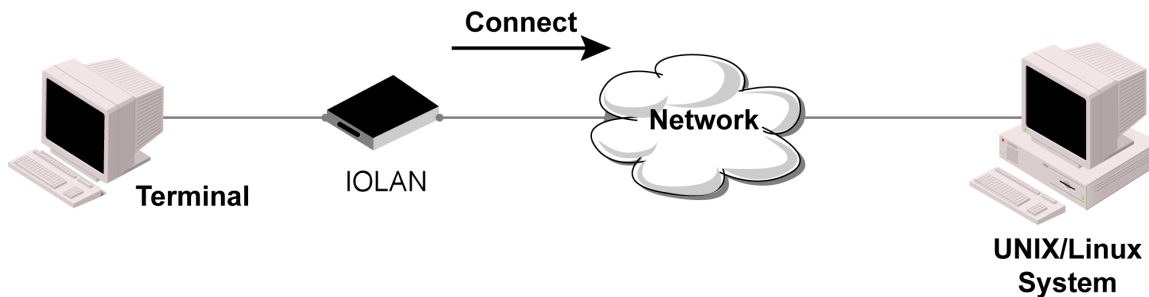
### *Terminal*

The Terminal profile allows network access from a terminal connected to the IOLAN'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 IOLAN first and then a connection to a host can be established.
- who are connecting through the serial port directly to a host.

#### **Terminal**



<i>Terminal</i>	
Settings	
<b>Terminal Type</b>	Type of terminal attached to this serial port. <ul style="list-style-type: none"> <li>• Dumb</li> <li>• WYSE60</li> <li>• VT100</li> </ul>



	<ul style="list-style-type: none"> <li>• TVT100</li> <li>• ANSI</li> <li>• YVI925</li> <li>• IBM3151TE</li> <li>• VT320</li> <li>• HP700</li> <li>• term 1</li> <li>• term 2</li> <li>• term 3</li> </ul> <p>Default is Dumb</p>
<p><b>Mode</b></p>	<p>When users access the IOLAN’s serial ports, they must be authenticated, using either the local user database or an external authentication server. After a user has been successfully authenticated, the IOLAN will connect to the specified host using the specified protocol according to:</p> <ul style="list-style-type: none"> <li>• the User Service parameter for locally configured users</li> <li>• the Default User Service parameter for users who are externally authenticated</li> <li>• TACACS+/RADIUS for externally authenticated users where the target host is passed to the IOLAN</li> </ul> <p>Default: Enabled See User Service settings</p> <ul style="list-style-type: none"> <li>• See <i>Login</i></li> <li>• See <i>Telnet</i></li> <li>• See <i>RLogin</i></li> <li>• See <i>SSL/TLS</i></li> <li>• See <i>Remote Access (SLIP)</i></li> <li>• See <i>Remote Access (PPP)</i></li> <li>• See <i>SSL/TLS</i></li> </ul>
<p><b>Connect to Remote System</b></p>	
<p><b>Host</b></p>	<p>Select the remote host you want to connect to.</p>
<p><b>Port</b></p>	<p>The TCP Port that the IOLAN will use to connect to the host. Default: Telnet-23, SSH-22, Rlogin-513</p>

<p><b>Initiate Connection</b></p>	<ul style="list-style-type: none"> <li>• <b>Automatically</b> – 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 IOLAN will initiate the session immediately after being powered up.</li> <li>• <b>Any Data Received</b> – Initiates a connection to the specified host when any data is received on the serial port.</li> <li>• <b>Specify a character</b> – 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)</li> </ul> <p>Default: Disabled</p>
<p><b>Protocol</b></p>	<p>Specify the protocol that will be used to connect to the specified host.  Options – Telnet, SSH, Rlogin  Default –Telnet  See <i>Telnet</i>  See <i>RLogin</i>  See <i>SSH</i></p>
<p><b>Terminal Type</b></p>	<p>Type of terminal attached to this serial port.</p> <ul style="list-style-type: none"> <li>• Dumb</li> <li>• WYSE60</li> <li>• VT100</li> <li>• ANSI</li> <li>• TVI925</li> <li>• IBM3151TE</li> <li>• VT320 (specifically supporting VT320-7)</li> <li>• (HP700 (specifically supporting HP700/44)</li> <li>• Term 1</li> <li>• Term 2</li> <li>• Term 3</li> </ul> <p>Default is Dumb</p>

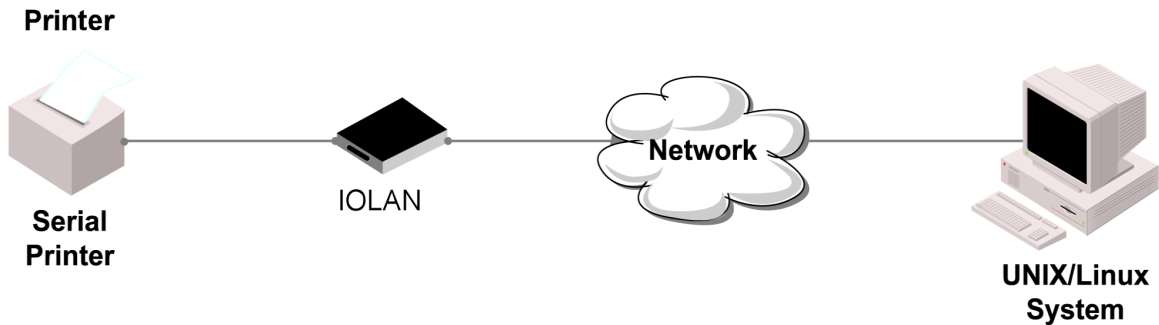
<p><b>Enable Local Echo</b></p>	<p>Toggles between local echo of entered characters and suppressing local echo. Local echo is used for normal processing, while suppressing the echo is convenient for entering text that should not be displayed on the screen, such as passwords. This parameter can be used only when Enable Line Mode is enabled. Default is Disabled</p>
<p><b>Enable Line Mode</b></p>	<p>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</p>
<p><b>Map CR to CR/LF</b></p>	<p>When enabled, maps carriage returns (CR) to carriage return line feed (CRLF). Default is Disabled</p>
<p><b>Control Characters</b></p>	
<p><b>Interrupt</b></p>	<p>Defines the interrupt character. Typing the interrupt character interrupts the current process. This value is in hexadecimal. Default is 3 (ASCII value ^C)</p>
<p><b>Quit</b></p>	<p>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)</p>
<p><b>EOF</b></p>	<p>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)</p>
<p><b>Erase</b></p>	<p>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)</p>
<p><b>Echo</b></p>	<p>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)</p>

<p><b>Escape</b></p>	<p>Defines the escape character. Returns you to the command line mode. This value is in hexadecimal. Default is 1d (ASCII value <b>GS</b>)</p>
<p><b>Advanced</b></p>	
<p><b>Enable Message of the Day (MOTD)</b></p>	<p>Enables/disables the display of the message of the day. Default is Disabled</p>
<p><b>Reset Terminal on Disconnect</b></p>	<p>When enabled, resets the terminal definition connected to the serial port when a user logs out. Default is Disabled</p>
<p><b>Allow Port Locking</b></p>	<p>When enabled, you can lock your terminal with a password using the Hot Key Prefix (default Ctrl-a) ^a l (lowercase L). The IOLAN prompts you for a password and a confirmation. Default is Disabled</p>
<p><b>Hot Key Prefix</b></p>	<p>The prefix that a user types to lock a serial port. Data Range:</p> <ul style="list-style-type: none"> <li>• ^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.</li> </ul> <p>Default is Hexadecimal 01 (Ctrl-a, ^a)</p>
<p><b>Session Timeout</b></p>	<p>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)</p>
<p><b>Idle Timeout</b></p>	<p>Use this timer to close a connection because of inactivity. When the Idle Timer times out, the IOLAN will end the connection. Range is 0-4294967 seconds (about 49 days) Default is 0 seconds so the port will never timeout</p>

<p><b>Packet Forwarding</b></p>	<p>Packet forwarding can be used to control/define how and when serial port data packets are sent from the IOLAN to the network. See <a href="#">Packet Forwarding</a></p>
<p><b>SSL/TLS</b></p>	<p>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</p> <ul style="list-style-type: none"> <li>• You can set up the IOLAN to act as an SSL/TLS client or server.</li> <li>• There is an extensive selection of SSL/TLS ciphers that you can configure for your SSL/TLS connection</li> </ul> <p>See <a href="#">SSL/TLS</a></p>

**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.

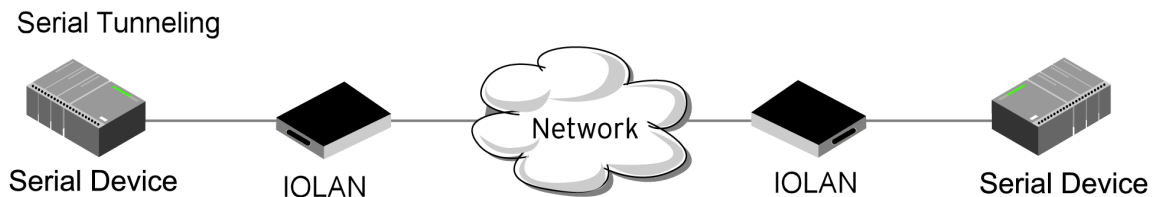


<b>Printer</b>	
<p><b>Map CR to CR/LF</b></p>	<p>The default end-of-line terminator as CR/LF (ASCII carriage-return line-feed) when enabled. Default: Disabled</p>
<p><b>Session Strings</b></p>	<p>Configures Send at Start, End and Delay after parameters for session control. See <a href="#">Session Strings</a></p>

<b>Packet Forwarding</b>	<p>Packet forwarding can be used to control/define how and when serial port data packets are sent from the IOLAN to the network.</p> <p>See <a href="#">Packet Forwarding</a></p>
--------------------------	---

### ***Serial Tunneling***

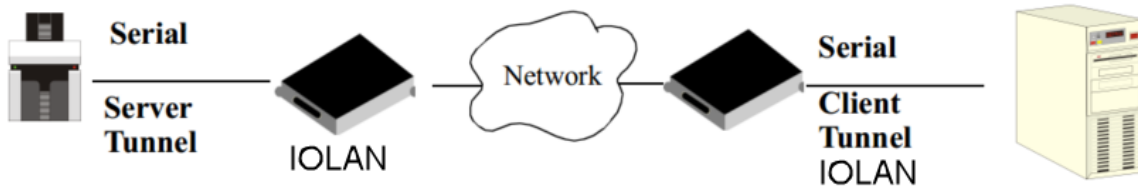
The Serial Tunneling profile allows two IOLANs to be connected back-to-back over the network to establish a virtual link between two serial ports based on RFC 2217. The serial device that initiates the connection is the Tunnel Client and the destination is the Tunnel Server, although once the serial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



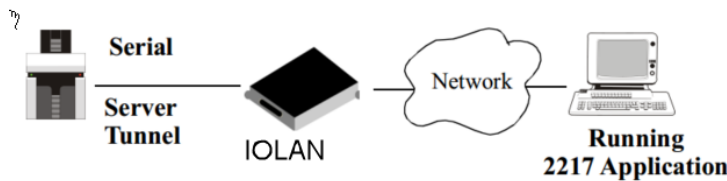
<b><i>Serial Tunneling</i></b>	
<b>Settings</b>	
<b>Act as a</b>	<ul style="list-style-type: none"> <li>• <b>Tunnel Server</b> – The IOLAN will listen for an incoming connection request on the specified Internet Address on the specified port. Default: Enabled</li> <li>• <b>Tunnel Client</b> – The IOLAN will initiate the connection the Tunnel Server. Default: Disabled</li> </ul>
<b>Listen for connection on TCP Port</b>	<p>The TCP port that the IOLAN will listen for incoming connection on. Default – 10000+serial port number; so serial port 1 is 10001.</p>

<p><b>Enable TCP Keepalive</b></p>	<p>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.</p> <p>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.</p> <p>Default: Disabled</p>
<p style="text-align: center;"><b>Advanced</b></p>	
<p><b>Break Length</b></p>	<p>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.</p> <p>Default is 1000ms (1 second)</p>
<p><b>Delay After Break</b></p>	<p>This parameter defines the delay between the termination of a a break condition and the time data will be sent out the serial port.</p> <p>Default is 0ms (no delay)</p>
<p><b>Packet Forwarding</b></p>	<p>Packet forwarding can be used to control/define how and when serial port data packets are sent from the IOLAN to the network.</p> <p>See <a href="#">Packet Forwarding</a></p>
<p><b>SSL/TLS</b></p>	<p>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</p> <ul style="list-style-type: none"> <li>• You can set up the IOLAN to act as an SSL/TLS client or server.</li> <li>• There is an extensive selection of SSL/TLS ciphers that you can configure for your SSL/TLS connection</li> </ul> <p>See <a href="#">SSL/TLS</a></p>

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 IOLANs 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.

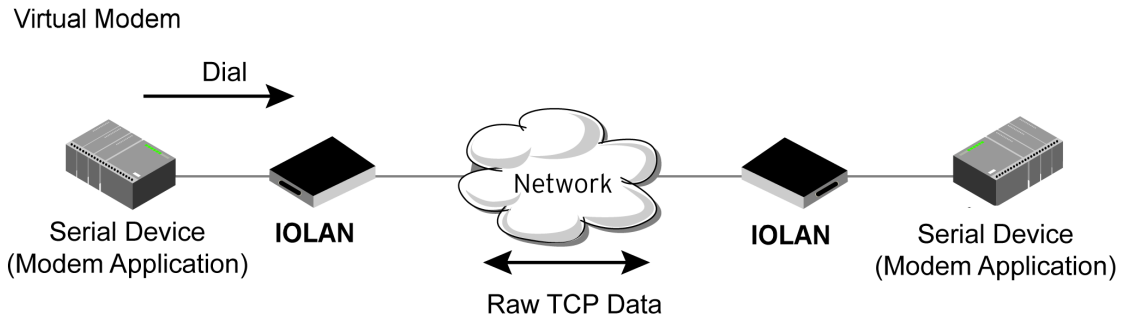
### *Virtual Modem*

Virtual Modem (Vmodem) is a feature of the IOLAN 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 IOLAN 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 IOLAN will then translate the dial request into a TCP connection and data will 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).



<i>Virtual Modem</i>	
<b>Settings</b>	
<b>Listen on TCP Port</b>	The IOLAN TCP port that the IOLAN will listen on. Default: 10000 + serial port number (for example, serial port 1 defaults to 10001)
<b>Connection</b>	<ul style="list-style-type: none"> <li>• <b>Connect Automatically</b> – When enabled, automatically establishes the virtual modem connection when the serial port becomes active. Default: Enabled</li> <li>• <b>Manually</b> – 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 IOLAN using the mapping table. Default: Disabled</li> </ul>
	<p>When your modem application provides a phone number in an AT command string, you can map that phone number to the destination host.</p> <p>Add a phone number</p> <ul style="list-style-type: none"> <li>• Phone number</li> <li>• Host</li> <li>• TCP Port</li> </ul>

<p><b>Host</b></p>	<p>The preconfigured target host name.</p>
<p><b>TCP Port</b></p>	<p>The port number the target host is listening on for messages. Default: 0 (zero)</p>
<p><b>Send Connection Status as</b></p>	<p>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</p> <ul style="list-style-type: none"> <li>• Numerical Code – When enabled, the connection status is sent to the connected device using the following numeric codes:             <ul style="list-style-type: none"> <li>• 0 OK</li> <li>• 1 CONNECTED</li> <li>• 2 RING</li> <li>• 3 NO CARRIER</li> <li>• 4 ERROR</li> <li>• 6 ITERFACE DOWN</li> <li>• 7 CONNECTION REFUSED</li> <li>• 8 NO LISTENER</li> </ul> </li> </ul> <p>Default: Enabled</p> <ul style="list-style-type: none"> <li>• Verbose String – When enabled, the connection status is sent by text strings to the connected device.             <ul style="list-style-type: none"> <li>• Success – String that is sent to the serial device when a connection succeeds.</li> </ul> </li> </ul> <p>Default – CONNECT &lt;speed&gt;, for example, Connect 9600</p>
	<ul style="list-style-type: none"> <li>• Failure – String that is sent to the serial device when a connection fails.</li> </ul> <p>Default – NO CARRIER</p>
<p><b>Advanced</b></p>	
<p><b>Echo characters in command mode</b></p>	<p>When enabled, echoes back characters that are typed in (equivalent to ATE0/ATE1 commands). Default is Disabled</p>

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, ATIO, ATi3, ATSO, 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 <i>Advanced Serial Options</i> 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

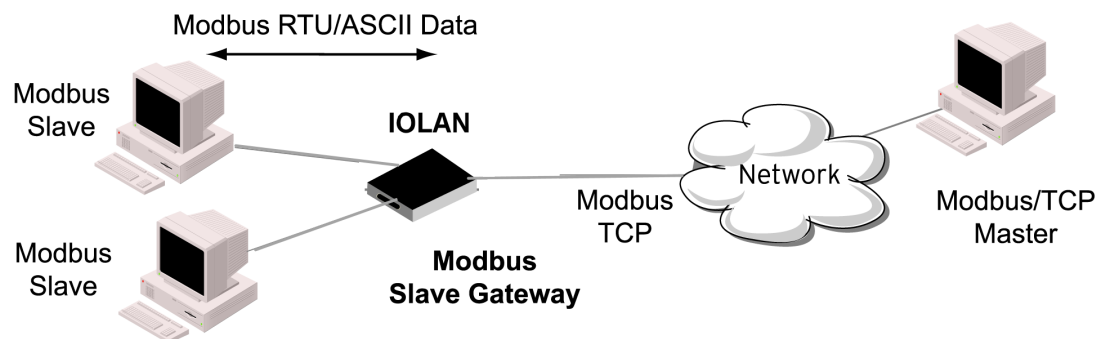
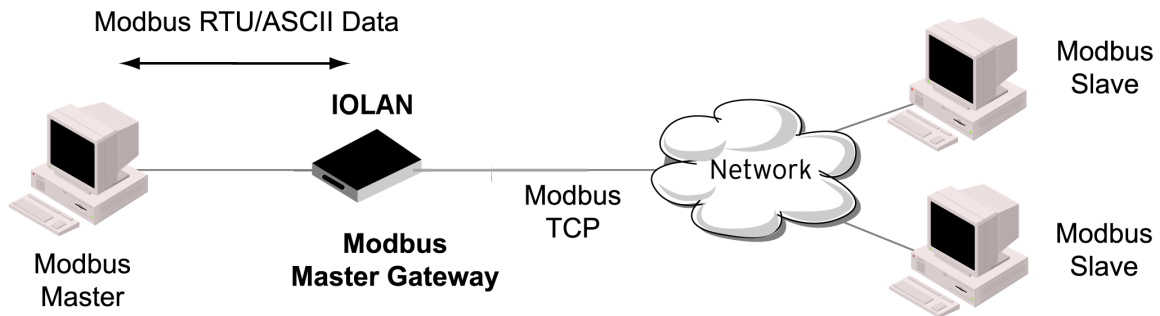
<p><b>Session Strings</b></p>	<p>Configures Send at Start, End and Delay after parameters for session control. See <a href="#">Session Strings</a></p>
<p><b>Packet Forwarding</b></p>	<p>Packet forwarding can be used to control/define how and when serial port data packets are sent fro the IOLAN to the network. See <a href="#">Packet Forwarding</a></p>
	<p>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</p> <ul style="list-style-type: none"> <li>• You can set up the IOLAN to act as an SSL/TLS client or server.</li> <li>• There is an extensive selection of SSL/TLS ciphers that you can configure for your SSL/TLS connection</li> </ul> <p>See <a href="#">SSL/TLS</a></p>

### 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



<i>Modbus Gateway</i>	
Settings Modbus Mode - Slave	Typically, the Modbus Master is accessing the IOLAN through the network to communicated to Modbus Slaves connected to the IOLAN'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	

<p><b>TCP/UDP Port</b></p>	<p>The network port number that the Slave Gateway will listen on for both TCP and UDP messages. Default: 502</p>
<p><b>Next Request Delay</b></p>	<p>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</p>
<p><b>Enable Serial Modbus Broadcast</b></p>	<p>When enabled, a UID of 0 (zero) indicates that the message will be broadcast to all Modbus Slaves. Default is disabled</p>
<p><b>Request Queuing</b></p>	<p>When enabled, allows multiple, simultaneous messages to be queued and processed in order of reception. Default is Enabled</p>
<p><b>UID Address mode</b></p>	<ul style="list-style-type: none"> <li>• Embedded – When this option is selected, the address of the slave Modbus device is embedded in the message header. Default – Enabled</li> <li>• 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.</li> </ul> <p>Default is Disabled</p>
<p><b>Remap UID</b></p>	<p>Specify the UID that will be inserted into the message header for the Slave Modbus serial device. Range is 1 – 247 Default is 1</p>
<p><b>Enable IP Aliasing</b></p>	<p>When enabled, allows for multiple requests to serial slaves (from an Ethernet Master/s) to be processed simultaneously. Default is Off</p>
<p><b>IP Address</b></p>	<p>IP Address – Set the IP address to be used for this serial port when using the IP Aliasing feature.</p>

<p><b>Enable SSL/TLS</b></p>	<p>When enabled, Modbus Slave Gateway messages to remote TCP Modbus Masters are encrypted via SSL/TLS. Default: Disabled</p>
<p><b>Protocol</b></p>	<ul style="list-style-type: none"> <li>• <b>Modbus/RTU</b> – Select this option when the Modbus/RTU protocol is being used for communication between the Modbus Master and Slave. Default: Disabled</li> <li>• <b>Modbus/ASCII</b> – Select this option when Modbus/ASCII protocol is being used for communication between the Modbus Master and Slave. Default: Enabled</li> <li>• <b>Append CR/LF</b> – When Modbus/ASCII is selected, adds a CR/LF to the end of the transmission; most Modbus devices require this option. Default: Enabled</li> </ul>
<p><b>Modbus Mode (Master)</b></p>	
<p><b>Add Slave Mapping</b></p>	
<p><b>UID Start</b></p>	<p>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 IOLAN will automatically increment the last digit of the configured IP address. Therefore, you can specify a UID range of 1-100, and the IOLAN 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)</p>
<p><b>UID End</b></p>	<p>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 IOLAN will automatically increment the last digit of the configured IP address. Therefore, you can specify a UID range of 1-100, and the IOLAN will route Master Modbus messages to all Modbus Slaves with IP addresses of 10.10.10.1 - 10.10.10.100.</p>

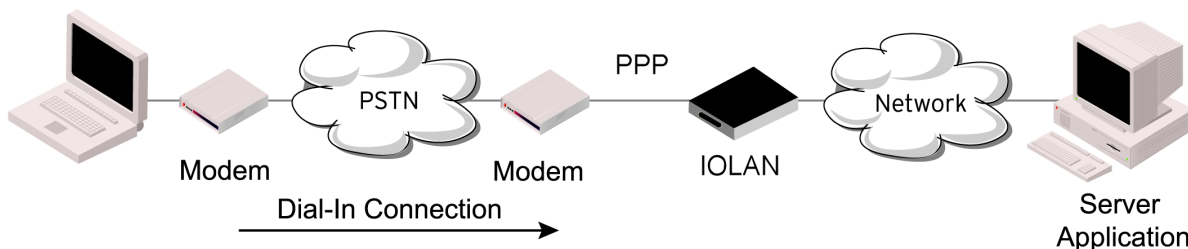
	<p>Range is 1 – 247 Default is 0 (zero)</p>
<b>Type</b>	<p>Specify the configuration of the Modbus Slaves on the network.</p> <p><b>Data Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Host</b> – The IP address is used for the first UID specified in the range. The last octet in the IPv4 address is then incremented for subsequent UID's in that range.</li> <li>• <b>Gateway</b> – The Modbus Master Gateway will use the same IP address when connecting to all the remote Modbus slaves in the specified UID range.</li> </ul> <p>Default is Host</p>
<b>Start IP Address</b>	<p>The IP address of the TCP/Ethernet Modbus Slave. Field Format IPv4 or IPv6 address</p>
<b>End IP Address</b>	<p>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</p>
<b>Protocol</b>	<p>Specify the protocol that is used between the Modbus Master and Modbus Slave(s). Data Options are TCP or UDP Default is TCP</p>
<b>UDP/TCP Port</b>	<p>The destination port of the remote Modbus TCP Slave that the IOLAN will connect to. Range is 0 – 65535 Default is 502</p>
<b>Advanced</b>	
<b>Idle Timeout</b>	<p>Use this timer to close a connection because of inactivity. When the idle Timeout expires, the IOLAN 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</p>



<p><b>Character Timeout</b></p>	<p>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</p>
<p><b>Message Timeout</b></p>	<p>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</p>
<p><b>Enable Modbus Exceptions</b></p>	<p>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</p>
<p><b>Session Strings</b></p>	<p>Configures Send at Start, End and Delay after parameters for session control. See <a href="#">Session Strings</a></p>
<p><b>Packet Forwarding</b></p>	<p>Packet forwarding can be used to control/define how and when serial port data packets are sent from the IOLAN to the network.                  See <a href="#">Packet Forwarding</a></p>
<p><b>SSL/TLS</b></p>	<p>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</p> <ul style="list-style-type: none"> <li>• You can set up the IOLAN to act as an SSL/TLS client or server.</li> <li>• There is an extensive selection of SSL/TLS ciphers that you can configure for your SSL/TLS connection</li> </ul> <p>See <a href="#">SSL/TLS</a></p>

### ***Remote Access (PPP)***

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



There are two options for PPP user authentication:

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

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

An example of the CHAP secrets file follows:

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

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

<b><i>Remote Access (PPP)</i></b>
<b>Settings IPv4</b>

<p><b>Local IP address</b></p>	<p>The IPV4 IP address of the IOLAN 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 IOLAN's (main) IP address in this field; if you do so, routing will not take place correctly.</p>
<p><b>IPv4 Remote IP Address</b></p>	<p>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 IOLAN. If you set the PPP parameter IP Address Negotiation to On, the IOLAN 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 IOLAN 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 IOLAN to use the remote IP address value configured here.</p>
<p><b>IPv4 Subnet Mask</b></p>	<p>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 IOLAN will use the value in the RADIUS file in preference to the value configured here.</p>
<p><b>Enable IP Address Negotiation</b></p>	<p>Specifies whether or not IP address negotiation will take place. IP address negotiation is where the IOLAN 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</p>

<p><b>Connection Method</b></p>	<p><b>Connect</b> – select the connection method.</p> <ul style="list-style-type: none"> <li>• <b>Direct Connect</b> – Specify this option when a modem is not connected to this serial port. Default is Enabled</li> <li>• <b>Dial In</b> – If the device is remote and will be dialing in via modem or ISDN TA, enable this parameter. Default is Disabled</li> <li>• <b>Dial Out</b> – If you want the modem to dial a number when the serial port is started, enable this parameter. Default is Disabled</li> <li>• <b>Dial in/Dial Out</b> – Enable this option when you want the serial port to do either of the following:             <ul style="list-style-type: none"> <li>• accept a call from a modem or ISDN TA</li> <li>• dial a number when the serial port is started.</li> </ul>                     Default is Disabled                 </li> </ul> <p><b>MS Direct</b> – select whether the MS-Direct is by Host or Guest.</p> <ul style="list-style-type: none"> <li>• <b>MS Direct Host</b> – Specify this option when the serial port is connected to a Microsoft Guest device. Default is enabled</li> <li>• <b>MS Direct Guest</b> – Enable this option when the serial port is connected to a Microsoft Host device. Default is Disabled</li> </ul>
<p><b>Dial Timeout</b></p>	<p>The number of seconds the IOLAN will wait to establish a connection to a remote modem.                      Range is 1-99                      Default is 45 seconds</p>
<p><b>Dial Retries</b></p>	<p>The number of times the IOLAN will attempt to re-establish a connection with a remote modem.                      Range is 0-99                      Default is 2</p>
<p><b>Modem init string</b></p>	<p>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&amp;Z1, AT&amp;Sn, AT&amp;Rn, AT&amp;Cn, AT&amp;F, ATs2, ATs12, ATO (ATD with no phone number), and ATDS1.</p>
<p><b>Phone number</b></p>	<p>The phone number to use when Dial Out is enabled.</p>

Authentication	
Authentication Type	<p>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 IOLAN. When setting either PAP and CHAP, make sure the IOLAN and the PPP peer, have the same setting. For example, if the IOLAN is set to PAP, but the remote end is set to CHAP, the connection will be refused.</p> <ul style="list-style-type: none"> <li>• None – no authentication will be preformed.</li> <li>• 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.</li> </ul>
	<ul style="list-style-type: none"> <li>• 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 IOLAN 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.</li> </ul> <p>Default is CHAP</p>

<p><b>User</b></p>	<p>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 IOLAN or you are using the IOLAN as a IOLAN (back-to-back with another IOLAN).</p> <p>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 IOLAN. The remote device will only authenticate your IOLAN'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.</p> <p>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 IOLAN. External authentication can not be used for this user.</p> <p>Field Format: you can enter a maximum of 254 alphanumeric characters.</p>
<p><b>Password</b></p>	<p>Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field and:</p> <ul style="list-style-type: none"> <li>• you wish to dedicate this serial port to a single remote user, who will be authenticated by the IOLAN or</li> <li>• you are using the IOLAN as a IOLAN (back-to-back with another IOLAN)</li> </ul> <p>Password means the following:</p> <ul style="list-style-type: none"> <li>• When PAP is specified, this is the password the remote device will use to authenticate the port on this IOLAN.</li> <li>• When CHAP is specified, this is the secret (password) known to both ends of the link upon which responses to challenges shall be based.</li> </ul> <p>Field Format is you can enter a maximum of 16 alphanumeric characters.</p>

<p><b>Remote User</b></p>	<p>Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field, and</p> <ul style="list-style-type: none"> <li>• you wish to dedicate this line to a single remote user, who will be authenticated by the IOLAN, or</li> <li>• you are using IOLAN back-to-back with another IOLAN</li> </ul> <p>When Dial In or Dial In/Dial Out is enabled, the Remote User is the name the IOLAN will use to authenticate the port on the remote device. Your IOLAN will only authenticate the port on the remote device when PAP or CHAP are operating.</p> <p>When connecting together two networks, enter a dummy user name; for example, DS_SALES.</p> <p>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 IOLAN. This option does not work with external authentication.</p> <p>Field Format is you can enter a maximum of 254 alphanumeric characters</p>
<p><b>Remote Password</b></p>	<p>Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field, and</p> <ul style="list-style-type: none"> <li>• you wish to dedicate this serial port to a single remote user, and this user will be authenticated by the IOLAN or</li> <li>• you are using the IOLAN back-to-back with another IOLAN</li> </ul> <p>Remote password means the following:</p> <ul style="list-style-type: none"> <li>• When PAP is specified, this is the password the IOLAN will use to authenticate the remote device.</li> <li>• When CHAP is specified, this is the secret (password) known to both ends of the link upon which responses to challenges will be based.</li> </ul> <p>Remote password is the opposite of the parameter Password. Your IOLAN will only authenticate the remote device when PAP or CHAP is operating.</p> <p>Field format is you can enter a maximum of 16 alphanumeric characters</p>

<p><b>Authentication Timeout</b></p>	<p>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.</p> <p>Range is 1-255 Default is 1 minute</p>
<p><b>CHAP Challenge Interval</b></p>	<p>The interval, in minutes, for which the IOLAN 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 IOLAN.</p> <p>Range is 0-255 Default is 0 (zero), meaning CHAP re-challenge is disabled</p>
<p><b>Enable Roaming Callback</b></p>	<p>A user can enter a telephone number that the IOLAN 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 IOLAN ends the call.</p> <p>Default is Disabled</p>
<p><b>Routing</b></p>	<p>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.</p> <p>Data Options:</p> <ul style="list-style-type: none"> <li>• None – Disables RIP over the PPP interface.</li> <li>• Send – Sends RIP over the PPP interface.</li> <li>• Listen – Listens for RIP over the PPP interface.</li> <li>• Send and Listen – Sends RIP and listens for RIP over the PPP interface.</li> </ul> <p>Default is None</p>



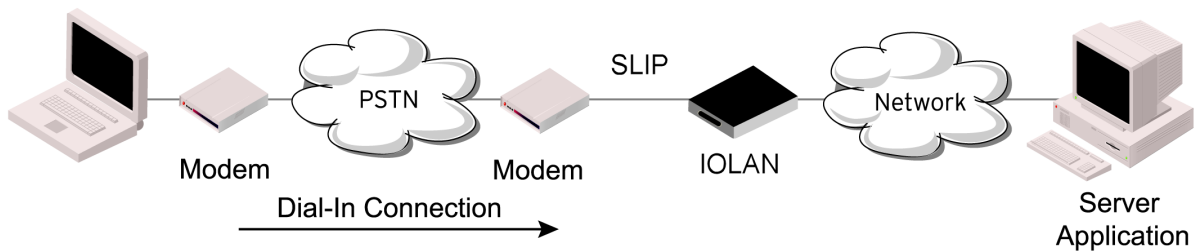
<p><b>ACCM</b></p>	<p>Specifies the ACCM (Asynchronous Control Character Map) characters that should be escaped from the data stream.</p> <p>The Field Formats is entered as a 32-bit hexadecimal number with each bit specifying whether or not the corresponding character should be escaped. The bits are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

<b>Terminate Request Timeout</b>	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
<b>Echo Request Retries</b>	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
<b>Echo Request Timeout</b>	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
<b>Configure NAK</b>	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
<b>Enable Address/Control Compression</b>	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
<b>Enable Protocol Compression</b>	This determines whether compression of the PPP Protocol field takes place on this link. Default is enabled
<b>VJ Compression</b>	When enabled, Van Jacobson Compression is used on this link. If your user is authenticated by the IOLAN, 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
<b>Enable Magic Negotiation</b>	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

<p><b>Idle Timeout</b></p>	<p>Use this timer to close a connection because of inactivity. When the Idle Timeout expires, the IOLAN 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</p>
<p><b>Session Strings</b></p>	<p>See <a href="#">Session Strings</a></p>
<p><b>Packet Forwarding</b></p>	<p>Packet forwarding can be used to control/define how and when serial port data packets are sent from the IOLAN to the network.                  See <a href="#">Packet Forwarding</a></p>

**Remote Access (SLIP)**

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



<p><b>Settings IPv4</b></p>	
<p><b>Local IP address</b></p>	<p>The IPV4 IP address of the IOLAN 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 IOLAN’s (main) IP address in this field; if you do so, routing will not take place correctly.</p>

<p><b>IPv4 Remote IP Address</b></p>	<p>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 IOLAN. If your user is authenticated by the IOLAN, 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 IOLAN will use the value in the RADIUS file in preference to the value configured here.</p>
<p><b>IPv4 Subnet Mask</b></p>	<p>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 IOLAN will use the value in the RADIUS file in preference to the value configured here.</p>
<p><b>MTU</b></p>	<p>The Maximum Transmission Unit (MTU) parameter restricts the size of individual SLIP packets being sent by the IOLAN. Enter a value between 256 and 1006 bytes; for example, 512. The default is 256. If your user is authenticated by the IOLAN, this MTU value will be over-ridden when you are a Framed-MTU value set for the user. If your user is authenticated by RADIUS and the RADIUS parameter Framed-MTU is set in RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here. Default is 256</p>
<p><b>Routing</b></p>	<p>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:</p> <ul style="list-style-type: none"> <li>• None – Disables RIP over the SLIP interface.</li> <li>• Send – Sends RIP over the SLIP interface.</li> <li>• Listen – Listens for RIP over the SLIP interface.</li> <li>• Send and Listen – Sends RIP and listens for RIP over the SLIP interface.</li> </ul> <p>Default is None</p>

<p><b>VJ Compression</b></p>	<p>When enabled, Van Jacobson Compression is used on this link. If your user is authenticated by the IOLAN, 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</p>
<p><b>Dial Options</b></p>	<p>Select the connection method.</p> <ul style="list-style-type: none"> <li>• Direct Connect – Specify this option when a modem is not connected to this serial port. Default is Enabled</li> <li>• Dial In – If the device is remote and will be dialing in via modem or ISDN TA, enable this parameter. Default is Disabled</li> <li>• Dial Out – If you want the modem to dial a number when the serial port is started, enable this parameter. Default is Disabled</li> <li>• Dial in/Dial Out – Enable this option when you want the serial port to do either of the following:             <ul style="list-style-type: none"> <li>• accept a call from a modem or ISDN TA</li> <li>• dial a number when the serial port is started.</li> </ul> </li> </ul> <p>Default is Disabled</p>
<p><b>Modem init string</b></p>	<p>You can specify additional modem commands that will affect how the modem starts. The following commands are supported: ATQn, ATVn, ATEn, +++ATH, ATA, ATIO, ATI3, ATS0, AT&amp;Z1, AT&amp;Sn, AT&amp;Rn, AT&amp;Cn, AT&amp;F, ATS2, ATS12, ATO (ATD with no phone number), and ATDS1.</p>
<p><b>Phone number</b></p>	<p>The phone number to use when Dial Out is enabled.</p>
<p><b>Session Strings</b></p>	<p>Configures Send at Start, End and Delay after parameters for session control. See <a href="#">Session Strings</a></p>
<p><b>Packet Forwarding</b></p>	<p>Packet forwarding can be used to control/define how and when serial port data packets are sent from the IOLAN to the network. See <a href="#">Packet Forwarding</a></p>

<i>Dial Options</i>	
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 IOLAN 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 IOLAN 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 IOLAN will not match the two numbers. Spaces will be ignored.
<i>Session Strings</i>	
Send at Start	<p>Session Strings</p> <p>Controls the sending of ASCII strings to serial device at session start as follows;</p> <p>Send at Start—If configured, this string will be sent to the serial device on power-up of the IOLAN, 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.</p> <p>Range is 0-127 alpha-numeric characters Range is hexadecimal 0-FF</p>

<p><b>Send at End</b></p>	<p>If configured, this string will be sent to the serial device when the TCP session on the IOLAN 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 &lt;027&gt;. The decimal numbers within the brackets must be 3 digits long (example 003 not 3).</p>
<p><b>Delay after Send</b></p>	<p>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</p>
<p><b><i>Packet Forwarding</i></b></p>	
<p>Packet forwarding can be used to control/define how and when serial port data packets are sent fro the IOLAN to the network.</p>	
<p>Define how the data received on the serial port with be forwarded to the network</p>	<p><b>Minimize Latency</b></p> <ul style="list-style-type: none"> <li>• This option ensures that all application data is immediatly forwarded to the serial device and that every character received from the serial device is immediatly sent on the network. Select this option for timing-sensitive applications.</li> </ul> <p>Default is disabled</p> <p><b>Optimize Network Throughput</b></p> <ul style="list-style-type: none"> <li>• 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.</li> </ul> <p>Default is disabled</p>

	<p><b>Prevent Message Fragmentation</b></p> <ul style="list-style-type: none"> <li>• 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.</li> </ul> <p>Default is disabled</p> <p><b>Custom Packet Forwarding</b></p> <ul style="list-style-type: none"> <li>• This option allows you to define forwarding rules based on the packet definition or the frame definition.</li> </ul> <p>Default is disabled</p>
<p><b>Delay Between Messages</b></p>	<ul style="list-style-type: none"> <li>• Minimize Latency</li> <li>• Optimize Network Throughput</li> <li>• Prevent Message Fragmentation</li> <li>• Custom Packet Forwarding</li> </ul>
<p><b>Custom Packeting Forwarding</b></p>	<p><b>Packet Definition</b></p> <ul style="list-style-type: none"> <li>• 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.</li> </ul> <p>Default is disabled</p> <p><b>Packet Size</b></p> <ul style="list-style-type: none"> <li>• 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.</li> </ul> <p>Range is 0–1024 bytes Default is 0</p>



	<p><b>Idle Time</b></p> <ul style="list-style-type: none"><li>• The amount of time, in milliseconds, that must elapse between characters before the packet is transmitted to the network. A value of zero (0) ignores this parameter.</li></ul> <p>Range is 0-65535 ms Default is 0</p> <p><b>End Trigger1 Character</b></p> <ul style="list-style-type: none"><li>• 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.</li></ul> <p>Range Hexadecimal 0-FF Default is 0</p> <p><b>End Trigger2 Character</b></p> <p>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 IOLAN 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.</p> <p>Range Hexadecimal 0-FF Default is 0</p> <p><b>Frame Definition</b></p> <ul style="list-style-type: none"><li>• 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.</li></ul> <p>Default is disabled</p>
--	---

	<p><b>SOF1 Character</b></p> <ul style="list-style-type: none"> <li>• 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.</li> </ul> <p>Range Hexadecimal 0-FF Default is 0</p> <p><b>SOF2 Character</b></p> <ul style="list-style-type: none"> <li>• 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 IOLAN waits for another SOF1 character to start the SOF1/SOF2 character sequence).</li> </ul> <p>Range Hexadecimal 0-FF Default is 0</p> <p><b>Transmit SOF Character(s)</b></p> <ul style="list-style-type: none"> <li>• 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.</li> </ul> <p>Default is 0</p> <p><b>EOF1 Character</b></p> <ul style="list-style-type: none"> <li>• 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.</li> </ul> <p>Range Hexadecimal 0-FF Default is 0</p>
--	--

	<p><b>EOF2 Character</b></p> <ul style="list-style-type: none"> <li>• 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 IOLAN 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.</li> </ul> <p>Range Hexadecimal 0-FF Default is 0</p> <p><b>Trigger Forwarding Rule</b></p> <ul style="list-style-type: none"> <li>• Determines what is included in the Frame (based on the EOF1 or EOF1/EOF2) or</li> <li>• Packet (based on Trigger1 or Trigger1/Trigger2). Choose one of the following options:             <ul style="list-style-type: none"> <li>• Strip-Trigger—Strips out the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings.</li> </ul> </li> </ul>
	<ul style="list-style-type: none"> <li>• Trigger—Includes the EOF1, EOF1/EOF2, Trigg1 or Trigger/Trigger2 depending on your settings.</li> <li>• Trigger+1—Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings, plus the first byte that follows the trigger.</li> <li>• Trigger+2—Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings, plus the next two bytes received after the trigger.</li> </ul> <p>Default is Trigger</p>

Use Global Settings	<b>SSL/TL Version</b> <ul style="list-style-type: none"> <li>• Any</li> <li>• TLSv1</li> <li>• TLSv1.1</li> <li>• TLSv1.2</li> </ul>
<b><i>SSL/TLS</i></b>	
Enable	Enable or disable SSL/TLS.
SSL/TLS Version	Select version of SSL/TLS. <ul style="list-style-type: none"> <li>• Any</li> <li>• TLSv1</li> <li>• TLSv1.1</li> <li>• TLSv1.2</li> </ul>
SSL/TLS Type	<ul style="list-style-type: none"> <li>• Client</li> <li>• Server</li> </ul>
<b>Add Cipher</b>	
Encryption	<ul style="list-style-type: none"> <li>• Any</li> <li>• AES</li> <li>• 3DES</li> <li>• ARCTWO</li> <li>• ARCFOUR</li> <li>• AES-GCM</li> </ul>
Minimum Key Size	<ul style="list-style-type: none"> <li>• 40</li> <li>• 56</li> <li>• 64</li> <li>• 128</li> <li>• 168</li> <li>• 256</li> </ul>
Maximum Key Size	<ul style="list-style-type: none"> <li>• 40</li> <li>• 56</li> <li>• 64</li> <li>• 128</li> <li>• 168</li> <li>• 256</li> </ul>

<p><b>Key Exchange</b></p>	<ul style="list-style-type: none"> <li>• Any</li> <li>• RSA</li> <li>• EHD-RSA</li> <li>• EDH-DSS</li> <li>• ADH</li> <li>• ECDH-ECDSA</li> </ul>
<p><b>HMAC</b></p>	<ul style="list-style-type: none"> <li>• Any</li> <li>• SHA1</li> <li>• MF5</li> <li>• SHA256</li> <li>• SHA384</li> </ul>
<p><b>Validate Peer Certificate</b></p>	<p>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 IOLAN, they need to be generated using the same SSL passphrase for both to work.</p> <p>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 IOLAN.</p> <p>Default is Disabled</p>
<p><b>Country</b></p>	<p>A country code; for example, US. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.</p> <p>Data option is two characters</p>
<p><b>State/Province</b></p>	<p>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.</p> <p>Data Option is Maximum 128 characters</p>
<p><b>Locality</b></p>	<p>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.</p> <p>Data Option is Maximum 128 characters</p>

<b>Organization</b>	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
<b>Organizational Unit</b>	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
<b>Common Name</b>	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
<b>Email</b>	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***

<b><i>Login</i></b>	
<b>Limit Connection to User</b>	Makes the serial port dedicated to the specified user. The user won't need to enter their login name - just their password.
<b>Terminal Pages</b>	The number of video pages the terminal supports. Range: 1-7 Default is 5 pages
<b><i>Telnet</i></b>	
<b>Terminal Type</b>	Type of terminal attached to this serial port. <ul style="list-style-type: none"> <li>• ansi</li> </ul>

	<ul style="list-style-type: none"> <li>• dumb</li> <li>• hp700</li> <li>• ibm3151te</li> <li>• tvi925</li> <li>• vt100</li> <li>• vt320</li> <li>• wyse60</li> <li>• term1</li> <li>• term2</li> <li>• term3</li> </ul>
<b>Enable Local Echo</b>	<p>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.</p> <p>Default is Disabled</p>
<b>Enable Line Mode</b>	<p>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.</p> <p>Default is Disabled</p>
<b>Enable Line Mode</b>	<p>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.</p> <p>Default is Disabled</p>
<b>Map CR to CR/LF</b>	<p>When enabled, maps carriage returns (CR) to carriage return line feed (CRLF). D</p> <p>Default: Disabled</p>
<b>Control Characters</b>	<ul style="list-style-type: none"> <li>• <b>Interrupt</b> – Defines the interrupt character. Typing the interrupt character interrupts the current process. This value is in hexadecimal. Default: is (ASCII value ^C)</li> <li>• <b>Quit</b> – Defines the quit character. Typing the quit character closes and exits the current telnet session. This value is in hexadecimal.</li> </ul>

	<p>Default is 1c (ASCII value FS)</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul> <p>Default is 4 (ASCII value ^D)</p> <ul style="list-style-type: none"> <li>• 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)</li> </ul>
	<ul style="list-style-type: none"> <li>• 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.</li> </ul> <p>Default: 5 (ASCII value ^E)</p> <ul style="list-style-type: none"> <li>• Escape – Defines the escape character. Returns you to the command line mode. This value is in hexadecimal.</li> </ul> <p>Default: 1d (ASCII value GS)</p>
<b><i>RLogin</i></b>	
<b>Terminal Type</b>	Type of terminal attached to this serial port; for example, ANSI or WYSE60.
<b>User</b>	This name is passed on to the specified host for the Rlogin session, so that the user is only prompted for a password.
<b><i>SSH</i></b>	
<b>Terminal Type</b>	Type of terminal attached to this serial port.



	<ul style="list-style-type: none"> <li>• ansi</li> <li>• hp700</li> <li>• ibm3151te</li> <li>• tvi925</li> <li>• vt100</li> <li>• vt320</li> <li>• wyse60</li> <li>• term 1</li> <li>• term 2</li> <li>• term 3</li> </ul> <p>Default is dumb</p>
<b>Verbose Mode</b>	<p>When enabled, displays debug messages on the terminal.</p> <p>Default is Disabled</p>
<b>Enable Compression</b>	<p>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.</p> <p>Default is Disabled</p>
<b>Strict Host Checking</b>	<p>When enabled, a host public key (for each host you want to ssh to) must be downloaded into the IOLAN.</p> <p>Default: is enabled</p>
<b>Login Automatically</b>	<p>When enabled, creates an automatic SSH login, using the name and Password values.</p> <p>Default is enabled</p>
<b>Name</b>	<p>The name of the user logging into the SSH session.</p> <p>Field Format: Up to 20 alphanumeric characters, excluding spaces.</p>
<b>Password</b>	<p>The user's password when auto login is enabled.</p> <p>Format: Up to 20 alphanumeric characters, excluding spaces.</p>
<b>Protocol</b>	
<b>SSH2 Cipher</b>	<ul style="list-style-type: none"> <li>• 3DES</li> <li>• Blowfish</li> </ul>

	<ul style="list-style-type: none"> <li>• AES-CBC</li> <li>• CAST</li> <li>• ARCFOUR</li> <li>• AES-CTR</li> <li>• AES-GCM</li> <li>• ChaCha20-Poly1305</li> </ul>
Authentication	<ul style="list-style-type: none"> <li>• RSA</li> <li>• DSA</li> <li>• Keyboard-interactive</li> </ul>
Keyboard Authentication	When enabled, the user types in a password for authentication. Default is enabled
<b><i>SLIP</i></b>	
Local IP address	The IPV4 IP address of the IOLAN 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 IOLAN'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 IOLAN. If your user is authenticated by the IOLAN, 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 IOLAN 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 IOLAN will use the value in the RADIUS file in preference to the value configured here.

<p><b>MTU</b></p>	<p>The Maximum Transmission Unit (MTU) parameter restricts the size of individual SLIP packets being sent by the IOLAN. Enter a value between 256 and 1006 bytes; For example, 512. The default value is 256. If your user is authenticated by the IOLAN 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 IOLAN will use the value in the Radius file in preference to the value configured here. Default is 256</p>
<p><i>PPP</i></p>	
<p><b>Settings IPv4</b></p>	
<p><b>Local IP address</b></p>	<p>The IPV4 IP address of the IOLAN 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 IOLAN's (main) IP address in this field; if you do so, routing will not take place correctly.</p>
<p><b>IPv4 Remote IP Address</b></p>	<p>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 IOLAN. If you set the PPP parameter IP Address Negotiation to On, the IOLAN 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 IOLAN 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 IOLAN to use the remote IP address value configured here.</p>
<p><b>IPv4 Subnet Mask</b></p>	<p>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 IOLAN will use the value in the RADIUS file in preference to the value configured here.</p>

<p><b>Enable IP Address Negotiation</b></p>	<p>Specifies whether or not IP address negotiation will take place. IP address negotiation is where the IOLAN 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</p>
<p><b>Authentication</b></p>	
<p><b>Authentication Type</b></p>	<p>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 IOLAN. When setting either PAP and CHAP, make sure the IOLAN and the PPP peer, have the same setting. For example, if the IOLAN is set to PAP, but the remote end is set to CHAP, the connection will be refused.</p> <ul style="list-style-type: none"> <li>• None – no authentication will be preformed.</li> <li>• 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.</li> <li>• 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 IOLAN 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.</li> </ul> <p>Default is CHAP</p>

<p><b>User</b></p>	<p>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 IOLAN or you are using the IOLAN as a IOLAN (back-to-back with another IOLAN).</p> <p>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 IOLAN. The remote device will only authenticate your IOLAN'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.</p> <p>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 IOLAN. External authentication can not be used for this user.</p> <p>Field Format: you can enter a maximum of 254 alphanumeric characters.</p>
<p><b>Password</b></p>	<p>Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field and:</p> <ul style="list-style-type: none"> <li>• you wish to dedicate this serial port to a single remote user, who will be authenticated by the IOLAN or</li> <li>• you are using the IOLAN as an IOLAN (back-to-back with another IOLAN)</li> </ul> <p>Password means the following:</p> <ul style="list-style-type: none"> <li>• When PAP is specified, this is the password the remote device will use to authenticate the port on this IOLAN.</li> <li>• When CHAP is specified, this is the secret (password) known to both ends of the link upon which responses to challenges shall be based.</li> </ul> <p>Field Format is you can enter a maximum of 16 alphanumeric characters.</p>

<p><b>Remote User</b></p>	<p>Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field, and</p> <ul style="list-style-type: none"> <li>• you wish to dedicate this line to a single remote user, who will be authenticated by the IOLAN, or</li> <li>• you are using the IOLAN back-to-back with another IOLAN</li> </ul> <p>When Dial In or Dial In/Dial Out is enabled, the Remote User is the name the IOLAN will use to authenticate the port on the remote device. Your IOLAN will only authenticate the port on the remote device when PAP or CHAP are operating.</p> <p>When connecting together two networks, enter a dummy user name; for example, DS_SALES.</p> <p>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 IOLAN. This option does not work with external authentication.</p> <p>Field Format is you can enter a maximum of 254 alphanumeric characters</p>
<p><b>Remote Password</b></p>	<p>Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field, and</p> <ul style="list-style-type: none"> <li>• you wish to dedicate this serial port to a single remote user, and this user will be authenticated by the IOLAN, or</li> <li>• you are using the IOLAN back-to-back with another IOLAN</li> </ul> <p>Remote password means the following:</p> <ul style="list-style-type: none"> <li>• When PAP is specified, this is the password the IOLAN will use to authenticate the remote device.</li> <li>• When CHAP is specified, this is the secret (password) known to both ends of the link upon which responses to challenges will be based.</li> </ul> <p>Remote password is the opposite of the parameter Password. Your IOLAN will only authenticate the remote device when PAP or CHAP is operating.</p> <p>Field format is you can enter a maximum of 16 alphanumeric characters</p>

<p><b>Authentication Timeout</b></p>	<p>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.</p> <p>Range is 1-255 Default is 1 minute</p>
<p><b>CHAP Challenge Interval</b></p>	<p>The interval, in minutes, for which the IOLAN 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 IOLAN.</p> <p>Range is 0-255 Default is 0 (zero), meaning CHAP re-challenge is disabled</p>
<p><b>Enable Roaming Callback</b></p>	<p>A user can enter a telephone number that the IOLAN 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 IOLAN ends the call.</p> <p>Default is Disabled</p>
<p><b>Advanced</b></p>	
<p><b>Routing</b></p>	<p>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.</p> <p><b>Data Options:</b></p> <ul style="list-style-type: none"> <li>• None – Disables RIP over the PPP interface.</li> <li>• Send – Sends RIP over the PPP interface.</li> <li>• Listen – Listens for RIP over the PPP interface.</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Send and Listen</b> – Sends RIP and listens for RIP over the PPP interface.</li> </ul> <p>Default is None</p>
<p><b>ACCM</b></p>	<p>Specifies the ACCM (Asynchronous Control Character Map) characters that should be escaped from the data stream.</p> <p>The Field Formats is entered as a 32-bit hexadecimal number with each bit specifying whether or not the corresponding character should be escaped. The bits are specified as the most significant bit first and are numbered 31-0. Thus if bit 17 is set, the 17th character should be escaped, that is, 0x11 (XON). The value 000a0000 will cause the control characters 0x11 (XON) and 0x13 (XOFF) to be escaped on the link, thus allowing the use of XON/XOFF (software) flow control. If you have selected soft Flow Control on the Serial Port, you must, you must enter a value of at least 000a0000 for the ACCM.</p> <p>Default is 00000000, which means no characters will be escaped</p>
<p><b>MRU</b></p>	<p>The Maximum Receive Unit (MRU) parameter specifies the maximum size of PPP packets that the IOLAN's port will accept. If your user is authenticated by the IOLAN, 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 IOLAN will use the value in the RADIUS file in preference to the value configured here.</p> <p>Range is 64-1500 bytes Default is 1500</p>
<p><b>Configure Request Retries</b></p>	<p>The maximum number of times a configure request packet will be re-sent before the link is terminated.</p> <p>Range is 0-255 Default is 10 seconds</p>
<p><b>Configure Request Timeout</b></p>	<p>The maximum time, in seconds, that LCP (Link Control Protocol) will wait before it considers a configure request packet to have been lost.</p> <p>Range is 1-255 Default is 3 seconds</p>



<b>Terminate Request Retries</b>	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
<b>Terminate Request Timeout</b>	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
<b>Echo Request Retries</b>	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
<b>Echo Request Timeout</b>	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
<b>Configure NAK</b>	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
<b>Enable Address/Control Compression</b>	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
<b>Enable Protocol Compression</b>	This determines whether compression of the PPP Protocol field takes place on this link. Default is enabled
<b>VJ Compression</b>	When enabled, Van Jacobson Compression is used on this link. If your user is authenticated by the IOLAN, 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

<p><b>Enable Magic Negotiation</b></p>	<p>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</p>
<p><b>Idle Timeout</b></p>	<p>Use this timer to close a connection because of inactivity. When the Idle Timeout expires, the IOLAN 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</p>
<p><b>Send at Start</b></p>	<p>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 IOLAN, 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</p>
<p><b>Delay after Send</b></p>	<p>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</p>
<p><b><i>SSL/TLS</i></b></p>	
<p><b>Enable SSL/TLS</b></p>	
<p><b>SSL/TLS cipher</b></p>	<ul style="list-style-type: none"> <li>• Any</li> <li>• TLSv1</li> <li>• SSLv3</li> <li>• TLSv1.1</li> <li>• TLSv1.2</li> </ul>
<p><b>Type</b></p>	<p>Select whether the mode is client or server.</p> <ul style="list-style-type: none"> <li>• client</li> <li>• server</li> </ul>
<p><b>Protocol</b></p>	

<b>SSH2 Cipher</b>	<ul style="list-style-type: none"> <li>• 3DES</li> <li>• Blowfish</li> <li>• AES-CBC</li> <li>• CAST</li> <li>• ARCFOUR</li> <li>• AES-CTR</li> <li>• AES-GCM</li> <li>• ChaCha20-Poly1305</li> </ul>
<b>Authentication</b>	<ul style="list-style-type: none"> <li>• RSA</li> <li>• DSA</li> <li>• Keyboard-interactive</li> </ul>
<b>Advanced Options</b>	See <i>Advanced Serial Options</i>
<b>Packet Forwarding</b>	<p>Packet forwarding can be used to control/define how and when serial port data packets are sent from the IOLAN to the network.</p> <p>See <i>Packet Forwarding</i></p>

### ***Port Buffering***

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

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

The data that is sent to the remote buffer file is appended to the end of the file (even through IOLAN 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 is not supported on all Service Types.

***Port Buffering***

<b>Serial Port Data Buffering</b>	
<b>Enable Local Buffering</b>	Enables/disables local port buffering on the IOLAN. Default is Disabled
<b>View Buffer string</b>	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
<b>Enable Remote (NFS) Buffering</b>	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
<b>NFS Host</b>	The NFS host that the IOLAN will send data to for its Remote Port Buffering feature. The IOLAN 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
<b>NFS Directory</b>	The directory and/or subdirectories where the Remote Port Buffering files will be created. For multiple IOLANs using the same NFS host, it is recommended that each IOLAN have its own unique directory to house the remote port log files. Default is device_server/portlogs
<b>Enable Port Buffering to Syslog</b>	When enabled, buffered data is sent to the syslog host to be viewed on the host's monitor.
<b>Level</b>	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
<b>Advanced Port Buffering</b>	

<p><b>Add Time Stamp</b></p>	<p>Enable/disable time stamping of the serial port buffer data. Default is Disabled</p>
<p><b>Enable Key Stroke Buffering</b></p>	<p>When enabled, key strokes that are sent from the network host to the serial device on the IOLAN's serial port are buffered. Default is Disabled</p>

**Remapping of Trueport Baud Rate**

<p><i>Trueport Baud Rate</i></p>	
<p>Mapping</p>	
<p>Trueport</p>	<p>Actual Baud Rate</p>
<p>50</p>	<p>300 or above Default is 57600</p>
<p>75</p>	<p>300 or above Default is 75</p>
<p>110</p>	<p>300 or above Default is 115200</p>
<p>134</p>	<p>300 or above Default is 230400</p>
<p>150</p>	<p>300 or above Default is 150</p>
<p>200</p>	<p>300 or above Default is 200</p>
<p>300</p>	<p>300</p>
<p>600</p>	<p>600</p>
<p>1200</p>	<p>1200</p>
<p>1800</p>	<p>1800</p>
<p>2400</p>	<p>2400</p>
<p>4800</p>	<p>4800</p>

9600	9600
19200	19200
38400	38400

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

<i>Advanced Serial Options</i>	
<b>Process Break Signals</b>	Enables/disables proprietary inband SSH break signal processing, the Telnet break signal, and the out-of-band break signals for TruePort. Default is Disabled
<b>Flush Data Before Closing Serial Port</b>	When enabled, deletes any pending outbound data when a port is closed. Default is Disabled
<b>Deny Multiple Network Connections</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• All data from previous connections on that serial port has drained</li> <li>• There are no other connections</li> <li>• Up to a 1 second interconnection poll timer has expired</li> </ul> <p>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</p>

<b>Data Logging</b>	<p>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 IOLAN causes all buffered data to be lost.</p>
<b>Buffer Size</b>	<p>Buffer size is 1 to 2000 Mb.                  Default size is 4 Mb</p>
<b>Monitor Connection Status</b>	
<b>Status Interval</b>	<p>Specify how often, in seconds, the IOLAN will send a TCP keep-alive to services that support TCP keep-alive.                  Default is 180 seconds</p>
<b>Retry Interval</b>	<p>The seconds between interval attempts.                  Default is 5 seconds</p>
<b>Retry (attempts)</b>	<p>The number of TCP keep-alive retries before the connection is closed.                  Default is 5                  Retries 1-32767</p>

## DHCP Server

The Perle IOLAN 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 IOLAN can act as a DHCP server so that clients can obtain addresses from its DHCP pool. Your IOLAN 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 IOLAN configuration parameters. You can use DHCP/BOOTP to perform the following actions on a single or multiple IOLANs 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 IOLANs' configuration in one DHCP/BOOTP file, rather than configure each IOLAN manually. Another advantage of DHCP/BOOTP is that you can connect your IOLAN to the

---

network, turn on its power and let autoconfiguration take place. All the configuration is carried out for you during the DHCP/BOOTP process.

### DHCP Parameters

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

- **SW\_FILE**—The full path, pre-fixed by hostname/IP address (IPv4 or IPv6), and file name of the software update.
- **CONFIG\_FILE**—The full path, pre-fixed by hostname/IP address (IPv4 or IPv6), and file name of the configuration file.
- **GUI\_ACCESS**—Access to the IOLAN from the HTTP or HTTPS-WebManager. Values are on or off.
- **AUTH\_TYPE**—The authentication method(s) employed by the IOLAN 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 IOLAN access to devices listed in the IOLANs host table. Values are yes or no.
- **TFTP\_RETRY**—The number of TFTP retries before aborting. This is a numeric value, for example, 5.
- **TFTP\_TMOUT**—The time, in seconds, before retrying a TFTP download/upload. This is a numeric value, for example, 3.

### Terminology

#### DHCP Pool

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

#### DHCP lease

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

#### DHCP Relay Agent

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



<i><b>DHCP Server</b></i>	
<b>Enable DHCP Server</b>	Enable or disabled DHCP Server. Default is enabled.
<b>DHCP Pools (Add, Edit or Delete)</b>	
<b>Pool Name</b>	Enter a name for this DHCP pool.
<b>Description</b>	Enter a description for this DHCP pool.
<b>Network address</b>	Specify the DHCP network.
<b>Network mask</b>	Specify the DHCP network mask.
<b>Specify Address Range within Network</b>	The IOLAN's DHCP pool will assign addresses to clients starting at X.X.X.X with an end address of X.X.X.X.
<b>Lease Duration</b>	<ul style="list-style-type: none"> <li>• <b>Infinite:</b> The DHCP lease will not expire</li> <li>• <b>Limited:</b> Set the time for the DHCP lease to expire, thereby releasing the address back to the DHCP pool</li> </ul>
<b>Default Gateway</b>	Specify the default gateway. This will normally be the IP address of your IOLAN.
<b>DNS Server</b>	Specify the DNS addresses to be used by the clients.
<b>Use Static Route</b>	
<b>Destination Network Prefix</b>	Specify a destination network prefix for this static route.
<b>Destination Network Mask</b>	Specify a destination network mask for this static route.
<b>Gateway Address</b>	Specify a the gateway for this static route.
<b>Reserved Addresses</b>	Enter reserved addresses (IP addresses that will not be served from this pool) and their corresponding MAC addresses.

<b>Options</b>	<p>Enter an option number. Range is 1-254</p> <p>Enter option data.</p> <ul style="list-style-type: none"> <li>• Ascii</li> <li>• Hex</li> <li>• IP addresses</li> </ul>
<b>Advanced</b>	
<b>Enable Authoritative Mode</b>	<p>Enable Authoritative is defaulted to On. This allows our IOLAN 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.</p>
<b>Bootfile</b>	<p>Specify the name of the bootfile to use.</p>
<b>Domain Name</b>	<p>Specify the Domain name of the server that has the bootfile.</p>
<b>Bootp Server Name</b>	<p>Specify the name of the bootp server that contains the bootp file.</p>
<b>DHCP Exclude Addresses (Add)</b>	
<b>Excluded Address</b>	<p>Specify addresses to exclude from the DHCP pool.</p>
<b>DHCPv6 Pools (Add, Edit, Delete)</b>	
<b>Pool name</b>	<p>Specify a pool name.</p>
<b>Lifetime</b>	<p>Configures the device lifetime value in IPv6 router advertisements on an interface.</p> <ul style="list-style-type: none"> <li>• Default valid lifetime Range is 0-4294967294</li> <li>• Maximum valid lifetime Range is 0-4294967294</li> <li>• Minimum valid lifetime Range is 0-4294967294</li> </ul>
<b>IPv6 Subnet Allocation</b>	
<b>Network Subnet</b>	<p>Enter the Network subnet for this network.</p>

<b>Network Mask</b>	<b>Enter the Network Mask for this network.</b>
<b>IPv6 Address Allocation (Add)</b>	
<b>Address</b>	<b>IPv6 address</b>
<b>Prefix Length</b>	<b>The number of bits in a prefix.</b>
<b>DNS Servers</b>	<b>Specify the DNS server addresses to be used by the clients.</b>
<b>SNTP Servers</b>	<b>Specify the SNTP server addresses to be used by the clients.</b>
<b>NIS Servers</b>	<b>Specify the NIS domain and server addresses to be used by clients.</b>
<b>NISP Servers</b>	<b>Specify the NISP domain and servers addresses to be used by clients.</b>
<b>SIP Servers</b>	<b>IPv6 address of SIP outbound proxy server. Domain name of the SIP outbound proxy server.</b>
<b>Domain</b>	<b>Specify the domain servers to be used by clients</b>
<b>Add Host</b>	<b>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</b>

## DHCP Relay

### Overview

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

### Terminology

#### DHCP Relay Agent

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

**Feature details / Application notes**

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

<i><b>DHCP Relay</b></i>	
<b>Enable DHCP Relay Agent</b>	Enable or disabled DHCP Relay Agent. Default is enabled
<b>Relay information forwarding policy</b>	If your IOLAN receives a packet which already contains an option 82 field, it can take one of the following actions; <ul style="list-style-type: none"> <li>• Replace the option 82 information and forward the frame (default action).</li> <li>• Drop – The frame is discarded.</li> <li>• Keep – The frame is forwarded with the received option 82 information.</li> <li>• 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.</li> </ul>
<b>Hop Count</b>	Set the maximum hop count before packets are discarded. Range is 0 – 255 Default is 10
<b>Packet size</b>	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
<b>Port</b>	Set the port used to relay DHCP client messages. Range 1 –65535 Default port is 67
<b>DHCP Relay Interfaces</b>	
<b>Interface</b>	Select the DHCP relay interface from the drop-down list.

<b>DHCP Server</b>	Specify the DHCP server associated with this relay interface.
--------------------	---

## Zero Touch Provisioning

### *Configuration over DHCP*

Zero Touch Provisioning (ZTP) allows IOLAN servers to be provisioned with configuration and/or software during their initial boot, from a DHCPv4 and file server. You must configure boot host dhcp under administration. See [Boot Configuration File](#).

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

<i>DHCP Option</i>	
150	TFTP server IP address. Only the first IP address is used.
66	TFTP server name
siaddr	BOOTP/DHCP header
54	Server Identifier

*Note: in decreasing order of precedence*

The DHCP options used for the IOLAN configuration file.

<i>DHCP Option</i>	
67	Bootfile name
Bootfile name	BOOTP/DHCP header

*Note: in decreasing order of precedence*

The DHCP option used for the IOLAN software and protocol selection.

<i>DHCP Option</i>	
125	Specify: <ol style="list-style-type: none"> <li>1. Software file name to be download</li> <li>2. Protocol to use to retrieve the bootfile (start-up config)</li> </ol>

<b>Enterprise #</b>	<b>0x00 0x00 0x07 0xae</b> In network byte order (1966 decimal; Perle's Enterprise #)	<b>4 bytes</b>	
<b>Data Length</b>	<b>Length of remaining fields not including this length type</b>	<b>1 byte</b>	
<b>Sub option optional fields</b>			
<b>Sub option code</b>	<b>0x05</b>	<b>1 byte</b>	<b>Software filename to download</b>
<b>Sub option data length</b>	<b>Length of software file name not including this length byte</b>	<b>1 byte</b>	
<b>Software file name</b>	<b>Name of the file containing the source parameter of an archive download-sw formatted command</b>  <b>This file contains the source parameter of an archive download-sw formatted command to download the software image.</b> <b>Example:tftp://174.16.21.1/IOLAN-4.1.G2.img</b>	<b>x byte</b>	
<b>Sub option code</b>	<b>0x10</b>	<b>1 byte</b>	<b>Protocol to use when retrieving the bootfile (startup config) and the software file (option 125 suboption 5)</b>
<b>Sub option data length</b>	<b>Must be 1</b>	<b>1 byte</b>	

<b>Protocol</b>	<b>0=TFTP</b> <b>1=HTTP</b> <b>2=HTTPS</b> <b>3=FTP</b>	<b>1 byte</b>	<b>Startup-config filename/ path is specified by option 67 or bootfile in the DHCP header (see above for order of precedence)</b>  <b>TFTP:</b> <b>Default if no protocol selected</b> <b>HTTPS:</b> <b>When using HTTPS, you must either disable server certificate validation (no http-client verify server) or load CA certificates on the IOLAN.</b> <b>FTP:</b> <b>When using FTP, username is anonymous and the password is &lt;serial# of the unit&gt;@&lt;oem-name&gt;.com</b>  <b>Examples</b> <b>IOLAN</b> <b>99-</b> <b>011319T001A4@Perle.com</b>
-----------------	--	---------------	---

DHCP requests including the following options.

DHCP Option	
<b>60</b> <b>Vendor class identifier</b>	<b>&lt;oem-name&gt;:&lt;serial#&gt; in ASCII</b> <b>IOLAN example: Perle:IOLAN SCR1618 RDAC :99-011319T001A4</b>
<b>61</b> <b>Client identifier</b>	<b>&lt;mac-addr&gt; &lt;ifname&gt; in ASCII</b> <b>IOLAN example: 0040.0298.9939-eth1</b>

---

## SNMP

### Overview

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

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

### *Connecting to the IOLAN Using SNMP*

Before you can connect to the IOLAN 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 IOLAN.
2. Configure a user for SNMP version 3 or a community for SNMP version 2c on the IOLAN.

### *Using the SNMP MIB*

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

### Pre-requisites

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

<b>SNMP</b>	
<b>Enable SNMP</b>	Enable or disable service. Default is disabled
<b>Location</b>	Define the SNMP location of your IOLAN. Max length is 32 characters
<b>Contact</b>	Defines the SNMP contact of your IOLAN. Max length is 14 characters
<b>SNMP Community (Add, Edit or Delete)</b>	
<b>Name</b>	Name of the community. Max length is 63 characters
<b>Permission</b>	Select the permission rights for this community. <ul style="list-style-type: none"> <li>• ip-access – restrict access to IP address (host or network as defined)</li> <li>• ro – readonly access with this community string</li> <li>• rw – read-write access with this community string</li> </ul>
<b>Access</b>	Select the access rights for this community. <ul style="list-style-type: none"> <li>• Any (Default) - allow access from any IP address</li> <li>• Access - access specified from specific host IP address or network subnets</li> </ul> Default is Any
<b>Add SNMP Host</b>	
<b>Community User</b>	Add the community user name.
<b>Add Hostname/IP address</b>	IPv4 address/hostname/network of SNMP client/s allowed to contact this IOLAN. Note: the host name must exist in the host table within your IOLAN.
<b>UDP port</b>	Enter the UDP port number. Range is 1 – 65535 Default is 162

<p><b>SNMP version</b></p>	<p>Select SNMP version.</p> <ul style="list-style-type: none"> <li>• V2c</li> <li>• V3</li> </ul>
<p><b>Enable Traps and Notifications</b></p>	
<p><b>Notifications</b></p>	<p>Individually enable/disable what conditions would generate a notification.</p> <ul style="list-style-type: none"> <li>• alarms</li> <li>• bgp</li> <li>• ipsec</li> <li>• openvpn</li> <li>• ospf</li> <li>• snmp</li> <li>• entity</li> <li>• authentication</li> <li>• envmon</li> <li>• dot11</li> </ul>
<p><b>SNMP Notification</b></p>	<ul style="list-style-type: none"> <li>• coldstart</li> <li>• authentication</li> <li>• linkdown</li> <li>• linkup</li> <li>• warmstart</li> </ul>
<p><b>SNMP Target Hosts</b></p>	<p>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)</p>
<p><b>Community User</b></p>	<p>Name of community user.</p>
<p><b>Hostname/IP address</b></p>	<p>Specify hosts or host name to receive notifications.</p>
<p><b>UDP port</b></p>	<p>UDP port the trap host is listening on. (default is 162).</p>
<p><b>SMNP Version</b></p>	<p>Version of trap:</p> <ul style="list-style-type: none"> <li>• v2c</li> <li>• v3</li> </ul> <p>Default is v2c</p>

<b>Add View</b>	
<b>OID</b>	Add OID for this view.
<b>Include</b>	Specify fields to include in this view.
<b>Exclude (optional)</b>	Exclude this fields from this view.
<b>Add Group</b>	
<b>Name</b>	Add the name of the group.
<b>Authentication Level</b>	Select Authentication Level. <ul style="list-style-type: none"> <li>• None</li> <li>• Authentication/no privacy</li> <li>• Authentication/privacy</li> </ul>
<b>View Access</b>	Select whether this group has View access. <ul style="list-style-type: none"> <li>• Read-Only</li> <li>• Read-Write</li> </ul>
<b>Write View</b>	Specify a write view name.
<b>Add User</b>	
<b>Username</b>	Specify the V3 user.
<b>Group</b>	Specify the group this user belongs to.
<b>Authentication/privacy passwords</b>	Set whether to use password or localized keys for this user.
<b>Authentication password</b>	Enter a authentication password.
<b>Privacy password</b>	Enter a privacy password.
<b>Authentication key</b>	Enter a authentication key.
<b>Privacy key</b>	Enter a privacy key.

<p><b>Default Engine ID</b></p>	<p>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 IOLAN.</p>
<p><b>Custom Default Engine ID</b></p>	<p>Specify your own custom Engine ID for your IOLAN.</p>

## 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 IOLAN should synchronize with. NTP will not synchronize with nodes whose time is significantly even if its stratum is lower. During this “settling” period, your IOLAN 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 IOLAN 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 IOLAN 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 IOLAN 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 IOLAN 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.

<b>NTP Settings</b>	
<b>Enable NTP (Network Time Protocol)</b>	<b>By default NTP is disabled globally. See reference for NTP per interface.</b>
<b>Internal Time Sources</b>	<b>Select the time sources.</b> <ul style="list-style-type: none"> <li>• Cellular System Time</li> <li>• GNSS (GPS)</li> </ul>
<b>Advanced NTP Settings</b>	

<b>Enable logging</b>	NTP messages will be logged.
<b>Auto-negotiate broadcast delay</b>	By default, your IOLAN 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.
<b>Broadcast delay (ms)</b>	Broadcast delay time is the estimated round-trip delay between the broadcast NTP server and your IOLAN. Microseconds are from 1-999999.
<b>Act as a master NTP clock</b>	Sets your IOLAN to act as the master clock source providing time to NTP clients.
<b>Stratum</b>	Specify how far your IOLAN 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
<b>NTP Server/Peer</b>	
<b>Hostname / IP address</b>	Enter the hostname or IPv4/IPv6 address of the NTP Server/Peer. <ul style="list-style-type: none"> <li>• IPv4 = A.B.C.D</li> <li>• IPv6 = 1:2:3:4::5:6</li> </ul>
<b>Resolve hostnames to</b>	<ul style="list-style-type: none"> <li>• IPv4 or IPv6</li> <li>• IPv4</li> <li>• IPv6</li> </ul>

<b>Type</b>	<ul style="list-style-type: none"> <li>• <b>Server</b>, a reliable clock source that is used to provide time to NTP clients.</li> <li>• <b>Peer command</b> 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.</li> </ul>
<b>Use authentication key</b>	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.
<b>Prefer this server/peer</b>	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.
<b>Advanced Options</b>	
<b>NTP version</b>	Version 1 – 4 are supported. Default is 4

<b>Minimum poll interval</b>	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
<b>Maximum poll interval</b>	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 IOLAN can monitor for global and individual port conditions. These alarms can be configured to send alert messages to an;

- External Syslog server
- SNMP trap server

### 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. 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"

## Port Alarms

Port Alarms (Add, Edit or Delete)



<b>Profile Name</b>	Provide a alarm profile name.
<b>Selected Alarm Relay</b>	<ul style="list-style-type: none"> <li>• None</li> <li>• major</li> <li>• minor</li> </ul>
<b>Not Operational</b>	
<b>Monitor</b>	Enable or disable to monitor for not operational alarms.
<b>Action</b>	Should this action occur: <ul style="list-style-type: none"> <li>• Send a Syslog message</li> <li>• Send a Trap message</li> <li>• Send a Relay message</li> </ul>
<b>Link Fault</b>	
<b>Monitor</b>	Enable or disable to monitor for not operational alarms.
<b>Action</b>	Should this action occur: <ul style="list-style-type: none"> <li>• Send a Syslog message</li> <li>• Send a Trap message</li> <li>• Send a Relay message</li> </ul>
<b>Facilities</b>	
<b>Dual Power Alarm</b>	
<b>Enable Alarm</b>	By default, the Alarm function will be enabled to monitor for dual power.
<b>Actions</b>	Send as a <ul style="list-style-type: none"> <li>•Syslog</li> <li>•Trap</li> </ul>

## Telnet/SSH

<b>Terminal</b>	
<b>Enable terminal history size</b>	Enter the size of the terminal history. Range is 1 – 256 Default is 20
<b>Terminal width</b>	Specify the width of the terminal Default is 80 columns
<b>Enable terminal pausing</b>	Pause the terminal at end of screen.
<b>Terminal length</b>	Specify the terminal length in line. Range is 1 – 512 Default is 24
<b>Session EXEC inactivity timeout</b>	Specify the days, hours, minutes and seconds for the timeout on EXEC sessions.
<b>SSH</b>	
<b>Client</b>	
<b>Strict Host Key Checking</b>	When enabled, a host public key (for each host you wish to ssh to) must be downloaded into the IOLAN. Default is Enabled
<b>Configure ciphers in order of preference</b>	Data Options: <ul style="list-style-type: none"> <li>• ChaCha20-Poly1305</li> <li>• AES128-CTR</li> <li>• AES192-CTR</li> <li>• AES256-CTR</li> <li>• AES128-GCM</li> <li>• AES192-GCM</li> <li>• AES128-CBC</li> <li>• AES-256-CBC</li> <li>• 3DES-CBC</li> </ul>

<p><b>Configure MACs for the ssh2 client in order of preference</b></p>	<p><b>Data Options:</b></p> <ul style="list-style-type: none"> <li>• UMAC-64-ETM</li> <li>• UMAC-128-ETM</li> <li>• HMAC-SHA2-256-ETM</li> <li>• HMAC-SHA2-512-ETM</li> <li>• HMAC-SHA1-ETM</li> <li>• UMAC-64</li> <li>• UMAC-128</li> <li>• HMAC-SHA2-256</li> <li>• HMAC-SHA2-512</li> <li>• HMAC-SHA1</li> </ul>
<p><b>Server</b></p>	
<p><b>Login timeout</b></p>	<p>The login timeout. Range 0 – 150 seconds Default is 120 seconds</p>
<p><b>Authentication retries</b></p>	<p>After this many incorrect retires the user will be locked out. Range is 1 – 5 Defaults is 3</p>
<p><b>Configure allowed ciphers for incoming ssh2 users</b></p>	<ul style="list-style-type: none"> <li>• ChaCha20-Poly1305</li> <li>• AES128-CTR</li> <li>• AES192-CTR</li> <li>• AES256-CTR</li> <li>• AES128-GCM</li> <li>• AES256-GCM</li> <li>• AES128-CBC</li> <li>• AES-192-CBC</li> <li>• AES-256-CBC</li> <li>• RIJNDEL-CBC</li> <li>• ARCFOUR</li> <li>• ARCFOUR128</li> <li>• ARCFOUR256</li> <li>• CAST128-CBC</li> <li>• BLOWFISH-CB</li> <li>• 3DES-CBC</li> <li>• 3DES-CBC</li> </ul>

---

<p><b>Configure allowed MACs for incoming ssh2 users</b></p>	<ul style="list-style-type: none"><li>• UMAC-64-ETM</li><li>• UMAC-128-ETM</li><li>• HMAC-SHA2-256-ETM</li><li>• HMAC-SHA2-512-ETM</li><li>• HMAC-SHA1-ETM</li><li>• HMAC-SHA1-96-ETM</li><li>• HMAC-RIPEMD160-ETM</li><li>• HMAC-MD5-ETM</li><li>• HMAC-MD5-96-ETM</li><li>• UMAC-64</li><li>• UMAC-128</li><li>• HMAC-SHA2-256</li><li>• HMAC-SHA2-512</li><li>• HMAC-SHA1</li><li>• HMAC-SHA-96</li><li>• HMAC-RIPEMD160</li><li>• HMAC-MD5</li><li>• HMAC-MD5-96</li></ul>
--	--

---

## Security

### *User Accounts*

#### **Overview**

In order to manage the IOLAN, users have to login. One of the methods which can be used to login involves a username and password. Add names to the IOLAN'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 the IOLAN.
- Privileged EXEC - Is able to perform all supported operations on your IOLAN.

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.

#### **User Sessions**

The Sessions tab is used to configure specific connections for users who are accessing the network through the IOLAN's serial port. Users who have successfully logged into the IOLAN (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 IOLAN 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 into the IOLAN.

#### **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 IOLAN, 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 IOLAN. This allows the administrator to copy users from one IOLAN 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*

<b>Add, Edit, Delete User</b>	Specify a username.
<b>Privilege Level</b>	<ul style="list-style-type: none"> <li>• No Admin, CLI only</li> <li>• Admin/Web User</li> </ul>
<b>Password</b>	Passwords can be up to 25 characters long. Blank passwords are also supported.
<b>Two Factor Authentication</b>	
<b>Two Factor authentication</b>	Enable Two Factor authentication. You must also enable and configure email settings under System/Email. See <a href="#">Email</a> for these settings.
<b>Format</b>	<ul style="list-style-type: none"> <li>• SMS</li> <li>• Email</li> </ul>
<b>Phone Number</b>	Specify the phone to receive the verification code.
<b>Email address</b>	Specify the email address to send the verification code.
<b>Serial Configuration</b>	
<b>Service</b>	<ul style="list-style-type: none"> <li>• Dslogin</li> <li>• Telnet</li> <li>• SSH</li> <li>• Rlogin</li> <li>• SLIP</li> <li>• PPP</li> <li>• TCP-Clear</li> <li>• SSL-Raw</li> </ul>
<b>Advanced</b>	
<b>Idle Timeout</b>	<p>The amount of time, in seconds, before the IOLAN 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.</p> <p>Range is 0-4294967 Default is 0</p>

<b>Session Timeout</b>	<p>The amount of time, in seconds, before the IOLAN 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.</p> <p>Range is 0-4294967 Default is 0</p>
<b>Enable Callback</b>	<p>When enabled, enter a phone number for the IOLAN to call the user back (the Enable Callback parameter is unrelated to the Serial Port Remote Access PPP profile Dial parameter).</p> <p>Note: the IOLAN will allow callback only when a user is authenticated. If the protocol over the link does not provide authentication, there will be no callback.</p> <p>Therefore, when the Serial Port profile is set to Remote Access (PPP), you must use either PAP or CHAP because these protocols provide authentication.</p> <p>The IOLAN supports another type of callback, Roaming Callback, which is configurable when the Serial Port profile is set to Remote Access (PPP). Default is disabled</p>
<b>Phone Number</b>	<p>The phone number the IOLAN will dial to callback the user (you must have set Enable Callback enabled).</p> <p>Restrictions enter the number without spaces.</p>

<p><b>Hot Key Prefix</b></p>	<p>The prefix that a user types to control the current session.</p> <p><b>Data Options:</b></p> <ul style="list-style-type: none"> <li>• <b>^a number</b> – 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 IOLAN Menu.</li> <li>• <b>^a n</b> –Display the next session. The current session will remain active. The lowest numbered active session will be displayed.</li> <li>• <b>^a p</b> – Display the previous session. The current session will remain active. The highest numbered active session will be displayed.</li> <li>• <b>^a m</b> – To exit a session and return to the IOLAN. You will be returned to the menu. The session will be left running.</li> <li>• <b>^a l</b> – (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.</li> <li>• <b>^r</b> – 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.</li> </ul> <p>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)</p>
<p><b>Sessions (1-4)</b></p>	<p>You can configure up to four (4) sessions that the user can select from to connect to a specific host after that user has successfully logged into the IOLAN (used only for serial ports configured for the Terminal profile).</p>



---

<b>Service</b>	Select the service for this session. <ul style="list-style-type: none"><li>• off – no connection is configured for this session</li><li>• Telnet – For information on the Telnet connection see <i>Telnet</i></li><li>• SSH – <i>SSH</i></li><li>• Rlogin – <i>RLogin</i></li></ul>
<b>Host</b>	Select the host you want to connect to from the pre-defined drop down list.
<b>Port</b>	Specify the TCP port that you will connect to for this session.
<b>Connect Automatically</b>	Specify whether or no the session(s) will start automatically when the user logs into the IOLAN.

---

## *AAA (Authentication, Authorization and Accounting)*

### **Overview**

This section describes how you set up AAA on your IOLAN.

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 IOLAN.

### **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 IOLAN to manage it. It also involves recording when your IOLAN 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 IOLAN.

#### **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 IOLAN.

### **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

<b><i>Login</i></b>	
<b>Authentication</b>	
Add, Edit, Delete Group	Specify a group name.
Group	Select the type of group; Local, Radius or TACACS+.
<b>Authorization</b>	
Add, Edit, Delete Group	Specify a group name.
Group	Select the type of group; Local, Radius or TACACS+.
<b>Accounting</b>	
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+.
<b><i>802.1X</i></b>	
<b>Accounting and Authentication</b>	
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).
<b><i>System</i></b>	
Accounting Settings	Select the type of messages you want to log; None, Start-Stop (login and log out) or Stop (logout). <ul style="list-style-type: none"> <li>• None</li> <li>• Start/Stop</li> </ul>
<b>Broadcast Methods (Add Group)</b>	
Group	Select the type of group; RADIUS or TACACS+.

<b><i>AAA Management</i></b>	
<b>HTTP/HTTPS Management</b>	
<b>Authentication method list</b>	<b>Select the list to be used for authentication</b>
<b>Accounting method list</b>	<b>Select the list to be used for accounting</b>
<b>Console Management (Enable)</b>	
<b>Authentication method list</b>	<b>Select the list to be used for authentication</b>
<b>Accounting method list</b>	<b>Select the list to be used for accounting</b>
<b><i>Two Factor Settings</i></b>	
<b>Pin Size</b>	<b>Number of PIN tries</b>
<b>Number of PIN Tries</b>	<b>Number of New two-factor PIN codes tries before failing authentication.</b>
<b>Number of PIN Attempts</b>	<b>Number of two-factor pin attempts before trying a new PIN.</b>

## ***Radius***

### **Overview**

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

### **Pre-requisites**

Basic AAA has been configured on your IOLAN.

### **Terminology**

#### **RADIUS - Remote Authentication Dial-In User Service**

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

#### **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 IOLAN to provide the following functions;

- Authenticate users logging into your IOLAN.
- Provide authorization information for users logging into your IOLAN.
- 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 IOLAN.
- 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.

<b>Radius</b>	
<b>Secret</b>	<b>Encryption key shared with RADIUS hosts.</b>
<b>Timeout (seconds)</b>	<b>Delay between unresponsive attempts. Range is 1-1000 seconds Default is 5 seconds</b>
<b>Retries</b>	<b>Number of attempts to reach host. Range is 1-100 Default is 3</b>
<b>Skip non -responsive servers</b>	<b>How long to ignore non-responsive servers.</b>
<b>IPv4 source interface</b>	<b>Select the source interface from the drop-down list.</b>
<b>Radius Servers (Add, Edit, Delete)</b>	
<b>Name</b>	<b>The name of this RADIUS host.</b>
<b>Hostname / IP address</b>	<b>Defines which IP address will be used when originating RADIUS messages from this IOLAN. 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</b>
<b>Authentication Port</b>	<b>Set the UDP authentication port for the requests to be received on the radius host. Both your IOLAN and radius server must match. Default is 1812.</b>

<b>Accounting Port</b>	Set the udp accounting port for the requests to be received on the radius host. Both your IOLAN and radius server must match. Default is 1813.
<b>Override Global Radius Settings</b>	You can override the global settings for the following three parameters for this RADIUS host.
<b>Secret</b>	Encryption key shared with RADIUS hosts.
<b>Timeout (seconds)</b>	Delay between unresponsive attempts. Range is 1-1000 seconds. Default is 5 seconds
<b>Retries</b>	Number of attempts to reach host. Range is 1-100 Default is 3

## *Login*

### **Overview**

In order to manage the IOLAN, users have to login into the IOLAN. One of the methods can be used to login involve a username and password. The user database on the IOLAN The user will be assigned one of two authorization levels.

- User EXEC - User is able to perform most monitoring functions but not allowed to perform configuration of IOLAN
- Privileged EXEC - User is able to perform all supported operations on the IOLAN

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 from 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 the IOLAN, 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 IOLAN. This allow the administrator to copy users from one IOLANto another with knowing what their passwords are.

<b>Login</b>	
<b>Set enable password</b>	Specify whether a user needs to provide an enable password to login into the EXEC mode.
<b>Enable password restrictions</b>	Password restrictions are not enabled by default.
<b>Enable user lockout</b>	The IOLAN can be configured to lockout a user after a configured number of failed attempts have occurred. Once a user is locked out, manual intervention by a privileged exec user must be to used to unlock the user. Only user-exec level users can get locked out. Value is 1-65535
<b>Maximum failed attempts before lockout</b>	Specify the number of failed attempts before the user will be locked out.
<b>Maximum failed logins before disconnection</b>	The attempts a user has before they disconnected from the login window. Default is 3
<b>On successful login</b>	<ul style="list-style-type: none"> <li>• Send Syslog message</li> <li>• Send Trap message</li> </ul> Specify the occurrence of these messages being sent. Value is 1-65535 Default is 1 occurrence
<b>Login Banner</b>	Display this Login banner when the Login prompt is shown.
<b>Message of the Day</b>	Displays the message of the day to users logging into the .IOLAN
<b>Login Prompt Timeout Banner</b>	Shows timeout login prompt message Default is % \$(prompt) timeout expired!
<b>Radius Servers (Add, Edit, Delete)</b>	
<b>Name</b>	The name of this RADIUS host.

<b>Hostname / IP address</b>	Defines which IP address will be used when originating RADIUS messages from this IOLAN. 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
<b>Authentication Port</b>	Set the UDP authentication port for the requests to be received on the radius host. Both your IOLAN and radius server must match. Default is 1812.
<b>Accounting Port</b>	Set the udp accounting port for the requests to be received on the radius host. Both your IOLAN and radius server must match. Default is 1813.
<b>Override Global Radius Settings</b>	You can override the global settings for the following three parameters for this RADIUS host.
<b>Secret</b>	Encryption key shared with RADIUS hosts.
<b>Timeout (seconds)</b>	Delay between unresponsive attempts. Range is 1-1000 seconds. Default is 5 seconds
<b>Retries</b>	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 IOLAN. Your IOLAN 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 IOLAN.

### **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 IOLAN. 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 IOLAN to provide the following functions.

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

<b>TACACS+</b>	
<b>Secret (Global)</b>	<b>Encryption key shared with all TACACS+ configured servers.</b>
<b>Timeout in seconds (Global)</b>	<b>Delay between unresponsive attempts. Range is 1-1000 Default is 5 seconds</b>
<b>Skip non-responsive servers (Global)</b>	<b>How long to ignore non-responsive servers.</b>
<b>IPv4 source interface</b>	<b>Select the source interface from the drop-down list.</b>
<b>TACACS+ Server (Add, Edit, Delete)</b>	
<b>Name</b>	<b>The name of this TACACS+ server.</b>
<b>Hostname / IP address</b>	<b>Defines which IP address will be used when originating TACACS+ messages from this IOLAN. The interface must be a management interface (i.e. has an IP address assigned).  Hostname or IPv4/IPv6</b>
<b>Secret</b>	<b>The encryption key for this TACACS+ server. This overrides the global secret.</b>
<b>Timeout in seconds</b>	<b>Delay between unresponsive attempts. Range is 1-1000 Default 5 seconds This overrides the global parameter for timeout.</b>

<b>TACACS+ Groups (Add, Remove)</b>	<b>Add one or more TACACS+ server(s) to the group. Group can be assigned to authentication, authorization and/or accounting functions.</b>
<b>Group Name</b>	<b>The name of this TACACS+ Server Group</b>
<b>Add a TACACS+</b>	<b>Select a TACACS+ server from the drop-down list to add to the server group.</b>

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

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.

<b>Firewall</b>	
<b>Source validation</b>	<ul style="list-style-type: none"> <li>• <b>IPv4 ping</b></li> <li>• <b>Broadcast Ping</b></li> <li>• <b>Handle IPv4 packet with source route option</b></li> <li>• <b>Handle received ICMPv6 redirected messages</b></li> <li>• <b>Handle IPv6 packet with routing ext-header</b></li> <li>• <b>Log IPv4 packet with invalid address</b></li> <li>• <b>Receive IPv4 redirect messages</b></li> <li>• <b>Sen IPv4 redirected messages</b></li> <li>• <b>SYN cookies</b></li> <li>• <b>RFC1337 TCP time-wait hazard protection</b></li> </ul>
<b>State Policy</b>	disable – no source validation loose – meaning any route (even default) strict – must match the inbound interface
<b>Firewall Rule (Add, Edit, Delete)</b>	
<b>Name</b>	Enter the name for this firewall rule.
<b>Description</b>	Enter a description for this firewall rule.
<b>Log packet hitting default action</b>	Log the packets that match the default action.
<b>Default Action</b>	<ul style="list-style-type: none"> <li>• <b>accept</b></li> <li>• <b>drop</b></li> <li>• <b>reject</b></li> </ul>
<b>Traffic Match (Add)</b>	

<b>Select Matching Criteria</b>	<b>Source IPv4-address</b> <ul style="list-style-type: none"><li>• Accept addresses or exclude addresses</li><li>• Use a range of addresses</li><li>• address and wildcard</li></ul> <b>Source MAC address</b> <b>Source Port (TCP/UDP)</b> <b>Destination IPv4-address</b> <b>Destination Port (TCP/UDP)</b> <b>Protocol</b> <ul style="list-style-type: none"><li>• ah</li><li>• dccp</li><li>• egp</li><li>• eigrp</li><li>• ggp</li><li>• gre</li><li>• hmp</li><li>• icmp</li></ul> <b>Protocol</b> <b>Match by ICMP</b> <b>Type Value</b> <ul style="list-style-type: none"><li>• TCMP Code</li><li>• idpr</li><li>• igmp</li><li>• ipv6-frag</li><li>• ipv6-icmp</li><li>• ipv6nonxt</li></ul>
---------------------------------	---

<p><b>Select Matching Criteria</b></p>	<ul style="list-style-type: none"> <li>• ipv6-opts</li> <li>• ipv6-route</li> <li>• isis</li> <li>• i2tp</li> <li>• manet</li> <li>• mpls-in-ip</li> <li>• narp</li> <li>• ospf</li> <li>• pim</li> <li>• rdp</li> <li>• rohc</li> <li>• rsvpsctp</li> <li>• sdrp</li> <li>• shim6</li> <li>• skip</li> <li>• tcp</li> </ul> <p>ack fin psh rst syn urg</p> <ul style="list-style-type: none"> <li>• udp</li> <li>• udplite</li> <li>• vrrp</li> <li>• xns-idp</li> <li>• IP Protocol number</li> </ul> <p>IP Protocol Number</p>
<p><b>Firewall Action</b></p>	<ul style="list-style-type: none"> <li>• accept</li> <li>• drop</li> <li>• reject</li> </ul>
<p><b>Schedule</b></p>	<ul style="list-style-type: none"> <li>• Use UTC</li> <li>• Enable Schedule</li> </ul> <p>Start time End Time (hh:mm:ss - 24 hour clock)</p>

<b>Type</b>	<ul style="list-style-type: none"> <li>• <b>Date – Start date - end date (Month/Day/Year)</b></li> <li>• <b>Weekdays – M, T, W, T, F, S, S, or All</b></li> <li>• <b>Days of the month –1-31 or All</b></li> </ul>
<b>Zones (Add, Edit, Delete)</b>	
<b>Name</b>	<b>Name of the zone.</b>
<b>Description</b>	<b>Description of the zone.</b>
<b>Local Zone</b>	<b>A local zone is the IOLAN itself, including interfaces on the IOLAN. All packets constructed on and actively sent from the IOLAN are regarded as from the local area.</b>
<b>Default Action</b>	<ul style="list-style-type: none"> <li>• <b>Drop</b></li> <li>• <b>Reject</b></li> </ul>
<b>Zones Pairs (Add, Edit, Delete)</b>	<ul style="list-style-type: none"> <li>• <b>From</b></li> <li>• <b>To</b></li> <li>• <b>Firewall</b></li> </ul>
<b>Firewall and Zone Interfaces</b>	
<b>Assign Firewall to Interface</b>	<ul style="list-style-type: none"> <li>• <b>Select interface</b></li> <li>• <b>Inbound Firewall</b></li> <li>• <b>Local Firewall</b></li> <li>• <b>Outbound Firewall</b></li> </ul>
<b>Assign Zones to Interfaces</b>	<ul style="list-style-type: none"> <li>• <b>Select interface</b></li> <li>• <b>Zone</b></li> </ul>

## ***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 IOLAN 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 IOLAN through the network unless you are configured to go through the IPsec tunnel (you can still access the IOLAN through the Console port).

You can configure the IOLAN 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 IOLAN to communicate data to a host/network).

<b>IPSEC</b>	
<b>Enable IPSEC</b>	Enable or disable IPSEC.
<b>Enable NAT Traversal</b>	Enable or disable NAT Traversal.
<b>NAT Network</b>	Specify the network to use for NAT transversal.
<b>Client Name</b>	Enter the name for this client connection.
<b>Connection Type</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• Disable – no connection (default)</li> <li>• Initiate – connection will be initiated by the client</li> <li>• Respond – the client will listen for a connection</li> </ul>
<b>Any Local Address</b>	<p>Use any local address for the tunnel or the IP address of the IOLAN. You should select Any when the IP address of the IOLAN is not always known (for example, when it gets it's IP address from DHCP). When Any is used, a default gateway must be configured under Routing/General Routing/Default Gateway</p> <p>Field Format is IPv4 address, IPv6 address, FQDN.</p>
<b>IKE Group</b>	Select an IKE group or use the default_ IKE group.
<b>Authentication</b>	
<b>Identity</b>	<p>The tunnel IP address of a specific host, or the network address that the IOLAN will provide a VPN connection to.</p> <p>Field Format is IPv4 address, IPv6 address, FQDN, @IPSEC Key-id</p>
<b>Remote Identity</b>	<p>The subnet mask of the local tunnel IPv4 network. Keep the default value when you are configuring a host-to-host VPN connection.</p> <p>Default is 255.255.255.255</p>

<p><b>Authentication</b></p>	<ul style="list-style-type: none"> <li>• None – no authentication</li> <li>• 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.</li> <li>• 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).</li> </ul>
<p><b>Tunnel ID</b></p>	<p>Enter an ID for this tunnel.</p>
<p><b>ESP Group</b></p>	<p>Select the Default ESP group or select one from the drop down list.</p>
<p><b>Local Address Family</b></p>	<p>Select either IPv4 or IPv6 for this tunnel connection. Default is IPv4</p>
<p><b>Local Address/Netmask</b></p>	<p>The IP address and netmask of your IOLAN.</p>
<p><b>Remote Address Family</b></p>	<p>Select either IPv4 or IPv6 for this tunnel connection. Default is IPv4</p>
<p><b>Remote Address/Netmask</b></p>	<p>The IP address of a specific host or the network address that the IOLAN 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.</p>
<p><b>IKE Groups</b></p>	
<p><b>Profile Name</b></p>	<p>Name of this IKE profile.</p>



<p><b>Aggressive mode</b></p>	<p>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</p>
<p><b>IKE Version</b></p>	<p>Select 1, 2 or both.</p> <p>Proposal IKEv1</p> <ul style="list-style-type: none"> <li>• Proposal ID - enter an ID number</li> <li>• Diffie-Hellman group – 2, 5, 14, 15, 16, 17, 18,19,20, 21,22, 23, 24, 25, 26</li> <li>• Encryption–3des, aes128, aes128gcm128, aes256, aes256gcm128, chacha20poly1305</li> <li>• Hash–SHA1,MD5, SHA1, SHA256, SHA384, SHA512</li> </ul> <p>Proposal IKEv2</p> <ul style="list-style-type: none"> <li>• Proposal ID - enter an ID number</li> <li>• Diffie-Hellman group – 2, 5, 14, 15, 16, 17, 18,19,20, 21,22, 23, 24, 25, 26</li> <li>• Encryption–3des, aes128, aes128gcm128, aes256, aes256gcm128, chacha20poly1305</li> <li>• SHA1,MD5, SHA1, SHA256, SHA384, SHA512</li> </ul> <p>Default is Version 2</p>
<p><b>Keep-alive lifetime</b></p>	<p>Time to keep connection alive. Range is 30-86400 Default is 3600 seconds</p>
<p><b>Dead Peer Detection (DPD)</b></p>	<p>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.</p>

<p><b>Action</b></p>	<ul style="list-style-type: none"> <li>• <b>Clear</b> – 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.</li> <li>• <b>Hold</b> – traffic from your local network to the remote network can trigger the IOLAN 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</li> <li>• <b>Restart</b> – re-initiate the VPN connection for three times over the detection timeout.</li> </ul> <p>Default Action is Hold Interval is 30 seconds Timeout is 120 seconds</p>
<p><b>Interval</b></p>	<p>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.</p> <p>Range is 2 – 86400 Default is 30 seconds</p>
<p><b>Timeout</b></p>	<p>Enter the value of detection timeout in seconds. If no response and no traffic over the timeout, declare the peer dead.</p> <p>Range is 10 – 86400 Default is 120 seconds</p>
<p><b>Add IKE Proposals</b></p>	
<p><b>Proposal ID</b></p>	<p>ID of this proposal. Values are 1 – 65535</p>

<p><b>Diffe-Hellman Group</b></p>	<ul style="list-style-type: none"> <li>• 2 – 1024-bit MODP Group (RFC6989)</li> <li>• 5 – 1536-bit MODP Group (RFC6989)</li> <li>• 14 – 2048-bit MODP Group (RFC6989)</li> <li>• 15 – 3072-bit MODP Group (RFC6989)</li> <li>• 16 – 4096-bit MODP Group (RFC6989)</li> <li>• 17 – 6144-bit MODP Group (RFC6989)</li> <li>• 18 – 8192-bit MODP Group (RFC6989)</li> <li>• 19 – 256-bit random ECP group (RFC6989)</li> <li>• 20 – 384-bit random ECP group (RFC6989)</li> <li>• 21 – 521-bit random ECP group (RFC6989)</li> <li>• 22 – 1024-bit MODP Group with 160-bit Prime Order Subgroup (RFC6989)</li> <li>• 23 – 1536-bit MODP Group with 224-bit Prime Order Subgroup (RFC6989)</li> <li>• 24 – 1536-bit MODP Group with 256-bit Prime Order Subgroup (RFC6989)</li> <li>• 25 – 192-bit Random ECP Group (RFC6989)</li> <li>• 26 – 224-bit Random ECP GroupMODP Group (RFC6989)</li> </ul> <p>Default is 2</p>
<p><b>Encryption</b></p>	<ul style="list-style-type: none"> <li>• 3des</li> <li>• aes128</li> <li>• aes128gcm128</li> <li>• aes256gcm128</li> <li>• chacha20poly1305</li> </ul> <p>Default is aes256</p>
<p><b>Hash</b></p>	<ul style="list-style-type: none"> <li>• MD5</li> <li>• SHA1</li> <li>• SHA256</li> <li>• SHA384</li> <li>• SHA512</li> </ul> <p>Default is SHA1</p>
<p><b>Add ESP Groups</b></p>	
<p><b>Profile Name</b></p>	<p>Add a name for this ESP profile.</p>
<p><b>Compression for IPSEC Connection</b></p>	<p>Use compression for this IPsec connection.</p>

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

## *OpenVPN* 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 IOLAN 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 IOLAN through the network unless you are configured to go through the IPsec tunnel (you can still access the IOLAN through the Console port).

You can configure the IOLAN 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 IOLAN to communicate data to a host/network).

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

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

<b>Ciphers</b>	<ul style="list-style-type: none"><li>• aes-128-cbc</li><li>• aes-128-gcm</li><li>• aes-192-cbc</li><li>• aes-192-gcm</li><li>• aes-256-cbc</li><li>• aes-256-gcm</li><li>• bf-cbc</li><li>• camellia-128-cbc</li><li>• camellia-192-cbc</li><li>• camellia-256-gcm</li><li>• cast-5-cbc</li><li>• des-cbc</li><li>• des-ede-cbc</li><li>• des-ede3-cbc</li><li>• desx-cbc</li><li>• rc2-40-cbc</li><li>• rc2-64-cbc</li><li>• seed-cbc</li></ul>
<b>Enable KeepAlive</b>	Enable keepalive timers.
<b>Keepalive interval</b>	Check for connection up every (interval time). Range is 1-65535
<b>Timeout</b>	Check for connection up every (interval time). Range is 1-65535

<b>Verbosity (Logging Level)</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• 0</li> <li>• 1</li> <li>• 2</li> <li>• 3</li> <li>• 4</li> <li>• 5</li> <li>• 6</li> <li>• 7</li> <li>• 8</li> <li>• 9</li> <li>• 10</li> <li>• 11</li> </ul>
<b>Preserve Tunnel Settings between Restarts</b>	Maintain tunnel connection between IOLAN restarts.
<b>Keys and Certificates</b>	
<b>PSK</b>	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 <i>Manage Files</i> files to import keys and certificates.
<b>PKI CA TrustPoint</b>	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 <i>Manage Files</i> files to import keys and certificates.
<b>PKI Certificate</b>	The PKI certificate to use for this secure connection. See <i>Manage Files</i> files to import keys and certificates.
<b>PKI Private Key</b>	The PKI private key to use for this secure connection. See <i>Manage Files</i> files to import keys and certificates.
<b>Advanced – Template</b>	Use template.
<i>Manage Files</i>	

Import File	
<b>Method</b>	<ul style="list-style-type: none"> <li>• Browser</li> <li>• FTP</li> <li>• HTTP</li> <li>• HTTPS</li> <li>• SCP</li> <li>• SFTP</li> <li>• TFTP</li> </ul>
<b>File Type</b>	<ul style="list-style-type: none"> <li>• CA</li> <li>• CERT</li> <li>• Diffie-Hellman</li> <li>• PKI Key</li> <li>• Pre-Shared Secret Key</li> <li>• Template</li> </ul>
<b>Name</b>	<b>Name of certificate/key to download</b>
<b>Import File</b>	<b>Select the file to import to the IOLAN</b>
<b>Installed Files</b>	<b>The installed certificate and keys in the IOLAN.</b>

## 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 IOLAN'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 refer to the 802.1x feature.

#### Supplicant

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

#### Authenticator



This refers to your IOLAN which the supplicant is attempting to connect to. Your IOLAN 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 IOLAN. 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 IOLAN supports a Radius host as the authenticating server. Your IOLAN 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 IOLAN 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.

**Suppliant**

- The port will authenticate with its peer which acts as the 802.1x authenticator.

<b>802.1X</b>	
<b>Enable 802.1X authentication</b>	<b>Select Enable to enable this feature.</b>

<p><b>Selected Port/all</b></p>	<ul style="list-style-type: none"> <li>• <b>Test 802.1X Readiness</b> – The 802.1x readiness check monitors 802.1X activity on all the IOLAN 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 IOLAN 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.</li> <li>• <b>Initialize</b> –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.</li> <li>• <b>Re-authenticate</b> –This command will re-authenticate all 802.1X port(s).</li> </ul>
<p><b>Advanced</b></p>	
<p><b>Enable 802.1X logging</b></p>	<p>Send 802.1X messages to a preconfigured syslog server.</p>
<p><b>802.1X test timeout</b></p>	<p>Timeout for device EAPOL capabilities test. Range is 1-65535 seconds Default is 10 seconds</p>
<p><b>Mode</b></p>	
<p><b>Supplicant</b></p>	<p>Port will authenticate with peer which is the authenticator.</p>
<p><b>Authenticator</b></p>	<p>Port will authenticate the device/devices (supplicants) connecting on the port.</p>
<p><b>Authenticator Settings</b></p>	

<p><b>Port control</b></p>	<ul style="list-style-type: none"> <li>• <b>Auto</b> – 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.</li> <li>• <b>Force authorized</b> – 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.</li> <li>• <b>Force unauthorized</b> – the port is secured/locked and will NEVER allow any traffic to ingress into our Ethernet port/s.</li> </ul>
<p><b>Host Mode</b></p>	<p><b>Single host</b></p> <ul style="list-style-type: none"> <li>• Only one device can authenticate and connect on the port.</li> <li>• This is the default mode of operation.</li> </ul> <p><b>Multiple host</b></p> <ul style="list-style-type: none"> <li>• 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.</li> </ul> <p><b>Multiple authentication</b></p> <ul style="list-style-type: none"> <li>• Each device connecting to your IOLAN is required to authenticate.</li> <li>• No limit as to the number of devices which can authenticate on the port.</li> </ul>
<p><b>MAB (MAC Authentication Bypass)</b></p>	<p>Allows devices which do not support 802.1X to be authenticated on your IOLAN. 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.</p> <p><b>Disabled</b>–no MAB enabled</p> <p><b>Fallback</b>–MAB is enabled, 802.1X is enabled</p> <ul style="list-style-type: none"> <li>• Use EAP</li> <li>• Enable periodic reauthentication</li> </ul> <p><b>Standalone</b>–MAB is enabled, 802.1X is disabled</p>
<p><b>Enable periodic reauthentication</b></p>	<p>When enabled, the supplicant will be asked to re-authenticated based on the Advanced setting -&gt; re-authentication timeout value.</p>

<b>Advanced Settings</b>	
<b>Supplicant response timeout</b>	<p>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.</p> <p>Range is 1-65535 seconds Default is 30</p>
<b>Transmit timeout</b>	<p>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.</p> <p>Default is 30 seconds</p>
<b>Quiet period timeout</b>	<p>Configure the number of seconds the interface remains in the wait state following a failed authentication attempt by a supplicant before reattempting authentication.</p> <p>Range is 1-65535 seconds Default is 60 seconds</p>
<b>Restart timeout</b>	<p>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)</p> <p>Range is 1-65535 seconds Default is 60 seconds</p>
<b>Maximum authentication retries</b>	<p>Set the number of times the authenticator will retransmit an EAP message to the supplicant.</p> <p>Range is 1-10 seconds Default is 2 seconds</p>
<b>Maximum re-authentication retries</b>	<p>Set the number of times the authenticator will attempt to re-authenticate a supplicant.</p> <p>Range is 1-10 seconds Default is 2 seconds</p>
<b>Credential Profile (Add, Edit, Delete)</b>	<p>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.</p>
<b>Profile Name</b>	Enter a profile name.
<b>Username</b>	Enter a username.

---

<b>Password</b>	<b>Enter the password.</b>
<b>EAP Profile (Add, Edit, Delete)</b>	
<b>Profile Name</b>	<b>Enter the profile name.</b>
<b>PKI trustpoint</b>	<b>Enter the PKI trustpoint name.</b>
<b>Methods</b>	<ul style="list-style-type: none"><li>• EAP-MD5</li><li>• EAP-MSCHAPV2</li><li>• EAP-GTC</li><li>• EAP-TLS</li><li>• TTLS-MSCHAP</li><li>• TTLS-MSCHAPV2</li><li>• TTLS-CHAP</li><li>• TTLS-EAP-MSCHAPv2</li><li>• TTLS-EAP-GTC</li><li>• PEAP-MD5</li><li>• PEAP-EAP-MSCHAPv2</li><li>• PEAP-GTC</li></ul>

## Monitor and Statistics

Your IOLAN can allow you to view statistics for general information about your IOLAN, view the logs, interface statuses and alarms.

### *System/General*

[Home](#) > [General Information](#)

<b>Last alarm:</b>	Redundant Power missing or failed
<b>System description:</b>	Perle SCR Series Routers
<b>System name:</b>	PerleSCR
<b>System location:</b>	
<b>System contact:</b>	
<b>System up time:</b>	2 hours 32 minutes 8 seconds
<b>System date:</b>	2020-03-31 12:37:06 EDT (GMT -04:00)
<b>Hardware revision:</b>	A
<b>Base MAC address:</b>	00:40:02:98:01:30
<b>Startup configuration state:</b>	Synchronized with running configuration
<b>CPU utilization:</b>	1%
<b>Memory (free):</b>	354956 KB
<b>Flashdisk (free):</b>	1252 MB

## View Logs

Home > View Log

Log Buffer

```
Mar 31 10:10:35 EDT %TRAPMGR-6: SNMP_EVENT: Interface eth2 has changed to link down. The administrative status is up and the operational status is down
Mar 31 10:10:35 EDT %TRAPMGR-6: SNMP_EVENT: Interface eth30 has changed to link down. The administrative status is up and the operational status is down
Mar 31 10:10:35 EDT %TRAPMGR-6: SNMP_EVENT: Interface eth14 has changed to link down. The administrative status is up and the operational status is down
Mar 31 10:10:35 EDT %TRAPMGR-6: SNMP_EVENT: Interface eth13 has changed to link down. The administrative status is up and the operational status is down
Mar 31 10:10:35 EDT %TRAPMGR-6: SNMP_EVENT: Interface eth32 has changed to link down. The administrative status is up and the operational status is down
Mar 31 10:10:35 EDT %TRAPMGR-6: SNMP_EVENT: Interface eth16 has changed to link down. The administrative status is up and the operational status is down
Mar 31 10:10:35 EDT %TRAPMGR-6: SNMP_EVENT: Interface eth31 has changed to link down. The administrative status is up and the operational status is down
Mar 31 10:10:35 EDT %TRAPMGR-6: SNMP_EVENT: Interface eth15 has changed to link down. The administrative status is up and the operational status is down
Mar 31 10:10:35 EDT %TRAPMGR-6: SNMP_EVENT: Interface eth26 has changed to link down. The administrative status is up and the operational status is down
```

## Interface Status

Home > Interface Status

Interface	
eth1	Ethernet
eth2	Ethernet
eth9	Ethernet
eth10	Ethernet
eth11	Ethernet
eth12	Ethernet
eth13	Ethernet
eth14	Ethernet
eth15	Ethernet


**General**

<b>Interface state</b>	Enabled
<b>Link</b>	Up
<b>MAC Address</b>	0040.0298.0130
<b>Speed</b>	1000 Mbps
<b>Duplex</b>	Full-duplex
<b>MTU</b>	1500 Bytes



## Alarms

Home > Alarms

Alarm Status					
Source	Severity	Description	Actions	Time	
PerleSCR	 MAJOR	Redundant Power missi...	Relay: None, LOG	Mar 31 202...	

---

## Administration

Your IOLAN 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 using DHCP/BOOTP.
- **Import Keys and Certificates** including importing and exporting of HTTPS, Server, SSH and SSL host/client/user keys and certificates.
- **Managing Flash/NVRAM Files** including exporting and importing files to/from flash.
- **Reboot/Reset** your IOLAN , resetting to factory defaults and shutting down your IOLAN .

### *Software Management*

#### Updating IOLAN Software Versions

##### Overview

This section describes how to manage the Perle IOLAN 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 IOLAN will check the Perle repository and inform you if your IOLAN 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 IOLAN 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 IOLAN is rebooted.
- Currently Running software is the actual software image that is executing on your IOLAN.
- Backup software is the software that is stored in backup. A new backup is created in the IOLAN 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

### IOLAN Software Versions

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

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

### Create Backup of Startup Software

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

## Boot Configuration File

Specify the BOOTP server name that contains the bootfile and the timeout value.

Configure DHCP Client parameters per interface. See [Interfaces](#).

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

---

## *Keys and Certificates*

### **Overview**

This feature allows for the management of keys and certificates on your IOLAN. 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 IOLAN.

#### **Server SSH key**

This RSA key is used to identify the server when a client connects via SSH to your IOLAN. When your IOLAN boots, if there is no SSH server key present, then your IOLAN will automatically generate a SSH2. You can optionally import your own key.

The public portion of the key can then be exported from your IOLAN 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 IOLAN is reset to factory default or is replaced, this key can be downloaded to your IOLAN 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 IOLAN you must enter a Passphrase which is used to encrypt the key. This passphrase is required when restoring the key to your IOLAN and protects it from unauthorized usage.

#### **SSH Host keys**

When your IOLAN 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 IOLAN. 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 IOLAN 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 IOLAN 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 supplicant and the RADIUS host.
- This is a global client key which is used as the credentials for your IOLAN
- The user imports the public key into our IOLAN.

**SSL Client Certificate**

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

**Managing the HTTPS Certificate**

- This is the certificate which identifies our IOLAN to clients which use HTTPS to access our IOLAN and need the certificate to validate our identity.
- This certificate/key is also used by the TTY services that have SSL/TLS enabled.
- Your IOLAN 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 IOLAN 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 IOLAN (i.e. after a reset to factory or if your IOLAN was replaced due to a service issue). This would allow all the existing clients to continue to treat your IOLAN as they did before.

<i>Manage HTTPS Certificate</i>	
<b>Import HTTPS Certificate for the WebManager</b>	
<b>Method</b>	<ul style="list-style-type: none"> <li>• Browser</li> <li>• FTP</li> <li>• HTTP</li> <li>• HTTPS</li> <li>• SCP</li> <li>• SFTP</li> <li>• TFTP</li> </ul>
<p>Your IOLAN 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 IOLAN. You also need to set the SSL Passphrase parameter with the same password that was used to generate the key.                      Note: Your IOLAN has a built-in self signed certificate.</p>	
<b>Type</b>	<ul style="list-style-type: none"> <li>• PEM</li> <li>• PKCS#12</li> </ul>
<b>Passphrase</b>	Enter the passphrase to use with the certificate.
<b>Import HTTPS Certificate File</b>	Select the certificate to be imported into the IOLAN.
<i>Manage Server SSH Key</i>	
<b>Import and Export server SSH-2 RSA Key. This key is used to identify the IOLAN to incoming SSH clients.</b>	
<b>Public Key</b>	OpenSSH
<b>Private Key</b>	PEM
<b>Method</b>	<ul style="list-style-type: none"> <li>• Browser</li> <li>• FTP</li> <li>• HTTP</li> <li>• HTTPS</li> <li>• SCP</li> <li>• SFTP</li> <li>• TFTP</li> </ul>

<b>Transfer server SSH key directly through your web browser.</b>	
<b>Import Options</b>	
<b>Passphrase</b>	Enter the passphrase to be used with this private server SSH key.
	Import the private server SSH key.
<b><i>Manage SSH Host Keys</i></b>	
Import SSH-2 RSA host public keys in OpenSSH format. These keys are used to authenticate other SSH servers for outgoing SSH connections.	
<b>Method</b>	<ul style="list-style-type: none"> <li>• Browser</li> <li>• FTP</li> <li>• HTTP</li> <li>• HTTPS</li> <li>• SCP</li> <li>• SFTP</li> <li>• TFTP</li> </ul>
<b>Transfer SSH host keys directly through your web browser</b>	
<b>SSH Hostname/IP address</b>	Enter the host name or IP address where the SSH host key resides.
	Select SSH Host Key to import to the IOLAN
<b>Installed Keys</b>	You can view/delete installed keys.
<b><i>Manage SSH User Keys</i></b>	
Import SSH-2 RSA user public keys in OpenSSH format. These keys are used to authenticate users for incoming SSH connections.	
<b>Method</b>	<ul style="list-style-type: none"> <li>• Browser</li> <li>• FTP</li> <li>• HTTP</li> <li>• HTTPS</li> <li>• SCP</li> <li>• SFTP</li> <li>• TFTP</li> </ul>

<b>Transfer SSH user keys directly through your web browser</b>	
<b>SSH User</b>	Enter the name of the SSH user.
	Import SSH User Key for this user.
<b>Installed Keys</b>	You can view/delete installed keys.
<b><i>Manage Server/CA Certificates</i></b>	
<p>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 IOLAN is acting as an 802.1x supplicant.</p> <p>Import server/CA Certificates</p>	
<b>Method</b>	<ul style="list-style-type: none"> <li>• Browser</li> <li>• FTP</li> <li>• HTTP</li> <li>• HTTPS</li> <li>• SCP</li> <li>• SFTP</li> <li>• TFTP</li> </ul>
<b>Transfer server/CA Certificate directly though your web browser</b>	
<b>Type</b>	<ul style="list-style-type: none"> <li>• PEM</li> <li>• PKCS#12</li> </ul>
<b>Passphrase</b>	Enter the passphrase to use with the certificate
<b>Import Server/CA Certificate</b>	Select the certificate to be imported into the IOLAN.
<b>Installed Certificates</b>	You can view/delete installed certificates.
<b><i>Manage SSL Client Key</i></b>	
<p>Key pair is generated externally to your IOLAN and the public portion of the key is imported to your IOLAN.</p> <p>Import server/CA Certificates</p>	



<b>Method</b>	<ul style="list-style-type: none"> <li>• Browser</li> <li>• FTP</li> <li>• HTTP</li> <li>• HTTPS</li> <li>• SCP</li> <li>• SFTP</li> <li>• TFTP</li> </ul>
<b>Transfer SSL key directly through your web browser.</b>	
<b>Type</b>	<ul style="list-style-type: none"> <li>• PEM</li> <li>• PKCS#12</li> </ul>
<b>Passphrase</b>	<b>Enter the passphrase to use with your SSL client key.</b>
<b>Import SSL Client Key</b>	<b>Select the SSL Client Key to be imported into the IOLAN.</b>
<b><i>Manage SSL Client Certificate</i></b>	
<b>Import SSL Client Certificate</b>	
<b>Method</b>	<ul style="list-style-type: none"> <li>• Browser</li> <li>• FTP</li> <li>• HTTP</li> <li>• HTTPS</li> <li>• SCP</li> <li>• SFTP</li> <li>• TFTP</li> </ul>
<b>Transfer SSL Client Certificate directly through your web browser.</b>	
<b>Type</b>	<ul style="list-style-type: none"> <li>• PEM</li> <li>• PKCS#12</li> </ul>
<b>Passphrase</b>	<b>Enter the passphrase to use with your SSL client certificate.</b>
<b>Import SSL Client Key</b>	<b>Select the SSL Client Certificate to be imported into the IOLAN.</b>

## *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 IOLAN based on:

- reboot now
- reboot in hours/minutes

<b><i>Reboot/Reset</i></b>	
<b>Reboot</b>	<b>Reboot now</b>
<b>Reboot in</b>	<b>Schedule a time to reboot in hours and minutes</b>
<b><i>Reset to Factory Defaults</i></b>	
<b>Reset to Factory</b>	<p>This will reset all configuration, operational information and certificates to factory default settings. Ethernet settings are 192.168.0.1. with DHCP enabled</p> <ul style="list-style-type: none"> <li>• <b>Reset Now</b></li> </ul>
<b><i>Shutdown</i></b>	

---

<b>Shutdown</b>	<b>This will shutdown the IOLAN The Reset button will power the IOLAN back up.</b> <ul style="list-style-type: none"><li>• <b>Shutdown now</b></li></ul>
-----------------	--

---

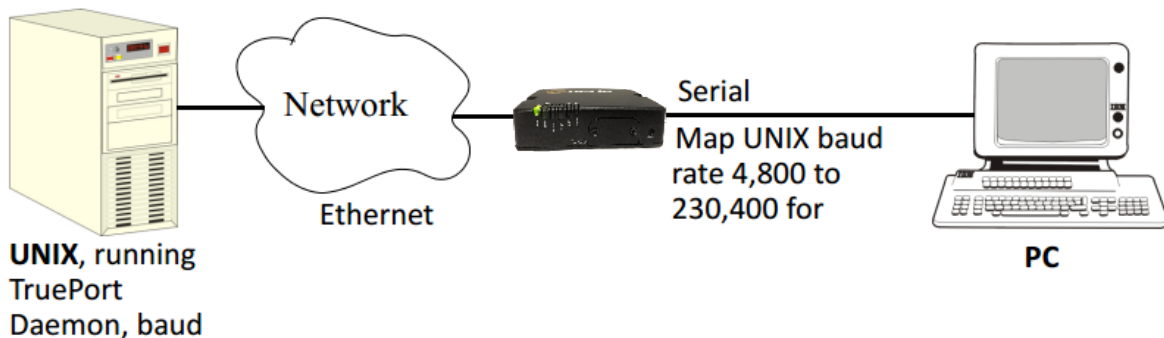
## Trueport

This chapter provides information on TruePort Redirect utility.

Trueport is a com port redirector utility for the IOLAN. 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 IOLAN.

You use TruePort when you want to connect extra terminals to a server using the IOLAN 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 IOLAN. 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.

---

## 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 IOLAN translate the UID to a different UID for the slave device. The Master UID has to be unique on the . The Slave UID must be unique on each serial port. The translate rules are controlled by a file downloaded to the IOLAN.

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 IOLAN 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 IOLAN 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 IOLAN 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-SHA256	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-SHA256	Kx=DH	Au=DSS	Enc=AES-GCM	128	SHA256
EDH-RSA-AES128-GCM-SHA256	Kx=DH	Au=RSA	Enc=AES-GCM	128	SHA256
EDH-RSA-AES128-SHA256	Kx=DH	Au=RSA	Enc=AES	128	SHA256
EDH-DSS-AES128-SHA256	Kx=DH	Au=DSS	Enc=AES	128	SHA256
EDH-RSA-AES128-SHA	Kx=DH	Au=RSA	Enc=AES	128	SHA1
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
RC4-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

---

<b>Full Name</b>	<b>Key-Exchange</b>	<b>Auth</b>	<b>Encryption</b>	<b>Key-Size</b>	<b>HMAC</b>
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 on your IOLAN.

### ***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 IOLAN.

The traceroute utility accepts a single parameter which is the destination your IOLAN 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 IOLAN)
- bgp – add bgp messages to logging
- clpd – add command line parser
- dialer – add dial on demand debugging to logging
- dot1x-authenticator – add 802.1x authenticator messages to logging
- dot1x-suppliant – 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
- 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 IOLAN if the user has also been set up as a local user in the IOLAN, 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 IOLAN 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 IOLAN'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 IOLAN itself then a port number of 0 is sent.
6	Service-Type	Response	Indicates the service to use to connect the user to the IOLAN. A value of 6 indicates administrative access to the IOLAN. Supported values are: <ul style="list-style-type: none"> <li>● 1—Login</li> <li>● 3—Callback-Login Equivalent to the IOLAN <b>User Service</b> set by Type 15, Login-Service.</li> <li>● 2—Framed</li> <li>● 4—Callback-Framed Equivalent to the IOLAN <b>User Service</b> set by Type 7, Framed-Protocol.</li> <li>● 7—NAS prompt</li> <li>● 9—Callback NAS-prompt Equivalent to IOLAN <b>User Service DSLogin</b>.</li> <li>● 6—Administrative User</li> <li>● 11—Callback Administrative User Equivalent to IOLAN <b>User Service DSLogin</b> and the User gets Admin privileges.</li> </ul>
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: <ul style="list-style-type: none"> <li>● 1—PPP</li> <li>● 2—SLIP</li> </ul>
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.

Table 0-1

Type	Name		Description
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: <ul style="list-style-type: none"> <li>• 1—Van Jacobson TCP/IP compression.</li> </ul>
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 IOLAN User Service to use to connect the user a host. Supported values are: <ul style="list-style-type: none"> <li>• 0—Telnet</li> <li>• 1—Rlogin</li> <li>• 2—TCP Clear</li> <li>• 5—SSH</li> <li>• 6—SSL Raw</li> </ul>
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 IOLAN will add routes to the user's PPP interface in the same order they were received
25	Class	Response	Received attributes are send in the Accounting Reply messages.
26	Vendor-Specific	Response	Perle's defined attributes for line access rights and user level. See <a href="#">Perle RADIUS Dictionary Example</a> for an example of this file. <p>Line Access Rights for port <i>n</i> (where <i>n</i> is the line number):</p> <p>Name: Perle-Line-Access-Port-<i>n</i></p> <p>Type: 100 + <i>n</i></p> <p>Data Type: Integer</p> <p>Value: Disabled (0), ReadWrite(1), ReadInput(2), ReadInputWrite (3), ReadOutput (4), ReadOutputWrite (5), ReadOutputInput (6), ReadOutputInputWrite (7)</p> <p>Name: Perle-User-Level</p> <p>Type: 100</p> <p>Data Type: Integer</p> <p>Value: Admin(1), Normal(2), Restricted(3), Menu(4)</p> <p>Name: Perle-Clustered-Port-Access</p> <p>Type: 99</p> <p>Data Type: Integer</p> <p>Value: Disabled(0), Enabled(1)</p>
27	Session-Timeout	Response	Maximum number of seconds the user will be allowed to stay logged on.

Table 0-1

Type	Name		Description
28	Idle-Timeout	Response	Use this timer to close a connection because of inactivity. When the Idle-Timeout expires, the IOLAN will end the connection. The maximum value is 4294967 seconds (about 49 days). A value of 0 (zero) means the Idle-Timeout will not expire, so the connection is permanently open.
31	Calling-Station-Id	Response	For reverse telnet and reverse ssh the IP address of the client will be sent. All other server type do not send this field.
32	NAS-Identifier	Response	If the identifier is configured then this field will be sent.
61	NAS-Port-Type	Response	For reverse telnet and reverse ssh connections, a type of Virtual (5) will be sent. For a PPP connection type a type of Async (0) will be sent. For all direct connect service types a type of Async (0) will be sent.
87	NAS-Port-Id	Response	For sessions originating from the serial port: <line-name> or "SERIAL:xx", where xx starts at serial port 1.  For reverse Telnet and SSH Ethernet sessions: "ETH:REVSESS:xx", where xx is the serial port being accesses, otherwise 00 for a ILOAN management session.  For HTTP sessions: "HTTP"
95	NAS-IPv6-Address	Response	The IPv6 address of the IOLAN.
96	Framed-Interface-Id	Response	The remote IPv6 interface identifier for the remote end of the PPP link.
98	Login-IPv6-Host	Response8	For LOGIN and CALLBACK service types, the IPv4 address of the login host is sent to the radius accounting host.
99	Framed-IPv6-Route	Response	When the PPP IPv6 interface comes up, the IOLAN 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 IOLAN 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 IOLAN 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 IOLAN itself then a port number of 0 is sent.

Type	Name	Description
6	Service-Type	<p>Indicates the service to use to connect the user to the IOLAN. A value of 6 indicates administrative access to the IOLAN. Supported values are:</p> <ul style="list-style-type: none"> <li>● 1—Login</li> <li>● 3—Callback-Login</li> </ul> <p>Equivalent to the IOLAN <b>User Service</b> set by Type 15, Login-Service.</p> <ul style="list-style-type: none"> <li>● 2—Framed</li> <li>● 4—Callback-Framed</li> </ul> <p>Equivalent to the IOLAN <b>User Service</b> set by Type 7, Framed-Protocol.</p> <ul style="list-style-type: none"> <li>● 7—NAS prompt</li> <li>● 9—Callback NAS-prompt</li> </ul> <p>Equivalent to IOLAN <b>User Service DSPrompt</b>.</p> <ul style="list-style-type: none"> <li>● 6—Administrative User</li> <li>● 11—Callback Administrative User</li> </ul> <p>Equivalent to <b>IOLAN User Service DSPrompt</b> and the User gets Admin privileges.</p>
14	Login-IP-Host	For LOGIN and CALLBACK service types, the IPv4 address of the login host is sent to the radius accounting host.
31	Calling-Station-Id	For reverse telnet and reverse ssh the IP address of the client will be sent. All other server type do not send this field.
32	NAS-Identifier	If the identifier is configured then this field will be sent.
40	Acct-Status-Type	Indicates if this is the beginning or end of a session. Supported values are: 1 = Start 2 = Stop.
42	Acct-Input-Octets	Number of bytes which were received from the user during this session.
43	Acct-Output-Octets	Number of bytes where were transmitted to the user during this session.
44	Acct-Session-ID	A string which identifies the session. The same string must be used in the start and stop messages.
45	Acct-Authentic	Indicates how the user was authenticated. Supported values are: 1 = Local 2 = RADIUS.
46	Acct-Session-Time	Number of seconds for which the user has been connected to a specific session.
47	Acct-Input-Packets	Number of packets which were received from the user during this session.
48	Acct-Output-Packets	Number of packets which were transmitted to the user during this session.
49	Acct-Terminate-Cause	Indicates how the session was terminated: Supported values include: 1 = User Request 2= Lost Carrier 3=Lost Service 4= Idle Timeout 5= Session Timeout 14 = Port Suspended 16 = Callback.

Type	Name	Description
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 IOLAN management session.  For HTTP sessions: “HTTP”
95	NAS-IPv6-Address	The IPv6 address of the IOLAN
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 IOLAN 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 IOLAN are discarded. Below is a list of the RADIUS parameters and their IOLAN parameters:

**RADIUS Parameter**

Service-Type	This has no IOLAN 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. <i>Caution:</i> 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 IOLAN.
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.

<b>Callback-Number</b>	<b>Combination of the Enable Callback and Phone Number fields under User, Advanced settings.</b>
<b>Callback-ID</b>	<b>Combination of the Enable Callback and Phone Number fields under User, Advanced settings.</b>

### *Perle RADIUS Dictionary Example*

The IOLAN has defined Vendor Specific RADIUS attributes in order for the RADIUS server to be configured to support the IOLAN features of Line Access Rights and User Level. These attributes have been defined in [Supported Radius Parameters](#) to allow the RADIUS server to be configured for RADIUS users to have this level of configuration.

See below for an example of the Perle defined attributes for the RADIUS server for an IOLAN.

```
# 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 IOLAN parameters if the user has also been set up as a local user in the IOLAN, 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 IOLAN after authentication for users accessing the IOLAN from the serial side and users accessing the IOLAN from the Ethernet side connections.

### Accessing the IOLAN through Serial Port Users

This section describes the attributes which will be accepted by the IOLAN 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 IOLAN 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 IOLAN. If no value is specified, DSPrompt is the default User Service.



Name	Value(s)	Description
service = telnet { addr = port = }	IPv4 or IPv6 address TCP port number	Settings when Perle_User_Service is set to 0.
service = rlogin { addr = }	IPv4 or IPv6 address	Settings when Perle_User_Service is set to 1.
service = tcp_clear { addr = port = }	IPv4 or IPv6 address TCP port number	Settings when Perle_User_Service is set to 2.
service = slip { routing = addr = }	true (Send and Listen) false (None) IPv4 or IPv6 address	Settings when Perle_User_Service is set to 3.
service = ppp { routing = addr = port = ppp-vj-slot-compression callback-dialstring }	true (Send and Listen) false (None) IPv4 or IPv6 address TCP port number true or false phone number, no punctuation	Settings when Perle_User_Service is set to 4.
service = ssh { addr = port = }	IPv4 or IPv6 address TCP port number	Settings when Perle_User_Service is set to 5.
service = ssl_raw { addr = port = }	IPv4 or IPv6 address TCP port number	Settings when Perle_User_Service is set to 6.

---

## Accessing the IOLAN Through a Serial Port User Example Settings

The following example shows the parameters that can be set for users who are accessing the IOLAN 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 IOLAN from the Network Users

This section describes the attributes which will be accepted by the IOLAN 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 IOLAN 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 IOLAN from the Network User Example Settings

The following example shows the parameters that can be set for users who are accessing the IOLAN 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 IOLAN 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