Perle IOLAN SCR
Command Reference Guide

Updated Aug 2024
Version A1.08.13.2024
Document Part# 5500493-10

www.perle.com

Table of Contents

Preface

About This Book

This guide provides the information you need to:

- configure the Perle IOLAN SCR using the Command Line Interface (CLI)
- Some CLI commands are not available, on some models

Intended Audience

This guide is for administrators who will be configuring the Perle IOLAN SCR hereafter known as the IOLAN.

Some prerequisite knowledge is needed to understand the concepts and examples in this guide:

- If you are using an external authentication application(s), working knowledge of the authentication application(s).
- Knowledge of the file transfer protocols the IOLAN uses.

Typeface 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:

Typeface Example	Usage
clear {**[ip dhcp binding]**}	Commands are in bold blue text and keywords for those command use bold green text.
<WORD>	Arguments in which you supply the values are in purple italics.
username **[nopassword] | [privilege 1] | 15] | [secret 0** ***<cleartext-password>*****] | [5** ***<hidden-user-secret>*** **|** ***<cleartext-password>*****]**	Square brackets means optional elements, but not required to complete the command. Such as command username does not require nopassword, privilege or secret for completion. Vertical bars within this example separate alternative choices and can be viewed as an or between parameters.
snmp-server {**contact** ***<contact-name>***}	Curly braces surround the entire keyword/ optional commands.
IOLAN SCR User's Guide	This typeface indicates a book or document title.
See ***About This Book*** for more information.	This indicates a cross-reference to another chapter or section that you can click on to jump to that section.

Setting up the IOLAN

For information on how to set up your IOLAN for the first time, see the Hardware Installation Guide (HIG) or User's Guide for your product. These are available on the Perle Web site at https://www.perle.com/downloads/.

1 Using the Command-Line Interface

This book provides the command line interface (CLI) options available for the Perle IOLAN. This chapter describes how to use the command-line interface (CLI) to configure software features. Commands are grouped by Command modes. Some CLI commands may not be applicable to your model or running software.

Command Modes

Command Mode	Prompt	Exit Mode	Access Next Mode
User EXEC mode	Perle>	**logout** command	**enable** command
Privileged EXEC mode	Perle#	**disable** command	**configure** command
Global configuration mode	Perle(config)#	**end** or **exit** command	**interface** command
Interface configuration mode	Perle(config-if)# Perle(config-if-range)#	**end** command	**interface** command, interface type, interface number
Line configuration mode	Perle(config-line)#	**end** command	**interface** command, interface type, interface number

Each command is broken down into several categories:

- **Description**—Provides a brief explanation of how the command is used.
- **Syntax**—Shows the actual command line options. The options can be typed in any order on the command line. The syntax explanation will use the following command to break down the command syntax:

```
For example: telnet 172.16.4.92
This command opens a telnet session to the host with the
IP address of 172.16.4.92. If you use a name rather than
an IP address, you can use the /ipv4 option to force the
connection to use an IPv4 format for the network address.

For example: sdm [default|dual-ipv4-and-ipv6]
This command sdm has an option of either default or dual
ipv4 and ipv6. You can choose either option but not both.
```

Braces ({}) group required choices and vertical bars (|) separate the alternative choices. Square brackets ([]) show the options that are available for the command or to show the options grouped together for readability. You can type a command with each option individually, or string options together in any order you want. Brace and vertical bars within square brackets {[]} means requires a choice within and optional element. The pipe (|) within a square bracket means a choice between the elements.

For example, valid values for (config)#ip **{**community-list **[**expanded **|** standard**]}**. Valid values are expanded or standard but you cannot select both at the same time.

- **Options**—Provides an explanation of each of the options for a command and the default value if there is one. Some commands do not have any options, so this category is absent.
- **UP arrow**—show a history of the previous commands entered.

Command Shortcuts

When you type a command, you can specify the shortest unique version of that command or you can press the **TAB** key to complete the command. For example, the following command:

```
Perle(config)#service dhcp
```

can be typed as:

```
Perle(config)#se d
```

or, you can use the **TAB** key to complete the lines as you go along:

```
se<TAB>d<TAB>
```

where the **TAB** key was pressed to complete the option as it was typed.

Command Options

When you are typing commands on the command line (while connected to the IOLAN, you can view the options by typing a question mark (**?**), after any part of the command to see what options are available/valid. For example:

Perle#terminal ?

```
help
history
length
monitor
no
width
```

Common Commands

default

Use the default command to set a command back to it’s defaults.

disable

Use the disable command to de-elevate from Privilege EXEC mode to User Exec mode.

do-exec

Run exec commands while in config mode.

enable

Use the enable command to elevate to Privilege EXEC mode from User Exec mode.

exit

The exit command in User EXEC mode logs you out of the IOLAN. In command mode it takes you to down one level of authority.

help

The help command gives you full help or partial help depending on your needs.

Usage Guidelines

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list is empty and you must backup until entering a '?' shows available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. show ?.)
2. Partial help is provided when an abbreviated argument and you want to know what arguments match the input (e.g. 'show pr?'.)

login

Log into the IOLAN.

logout

Log out of the IOLAN.

no

Use the no command to negate a command.

User Exec Mode

```
Perle> ?
```

- The ">" indicates that the current mode is "User EXEC". Depending on the model, some options may not be available.

clear	Reset functions
enable	Switch to privilege mode
exit	Exit from EXEC
help	Description of the interactive help
line-attach	Attach to a configured terminal line
logout	Logout of current user
ping	Send echo messages
release	Release a resource
renew	Renew a resource
show	Display internal settings
ssh	Open a secure shell client connection
telnet	Open a telnet connection
terminal	Set terminal characteristics
testemail	Send a test email message
traceroute	Trace route to destination
wireguard	Wireguard configuation

Example:

```
>clear ip dhcp binding *
```

Privilege EXEC Mode

Perle# ?

- The "#" indicates that the current mode is "Priviliged EXEC". Depending on the model, some options may not be available.

archive	Manage archive files
boot	Modify system boot parameters
cd	Change current directory
cellular	Cellular commands
clear	Reset functions
clock	Manage system clock
configure	Switch to (config)#
container (OCI)	Container operational commands
copy	Copy from one file to another
debug	Debugging functions (see also ’undebug’)
delete	Delete files
dir	List files on a file system
disable	Leave privileged mode
disconnect	Disconnect an existing network connection
dot1x	IEEE 802.1X Exec commands
exit	Exit from the EXEC
help	Description of interactive help
kill	Reset the serial line
line-attach	Attach to a configured terminal line
logout	Logout of current user
mkdir	Create a new directory
more	Display the contents of a file
no	Negate a command or set to defaults
ping	Send echo messages
pwd	Display present working directory
release	Release a resource
reload	Reboot the IOLAN

rename	Rename a file
renew	Renew a DHCP lease
reset	Reset commands
rmdir	Remove a directoy
serialt	Take a serial trace
show	Display internal settings
ssh	Open a ssh connection
telnet	Open a telnet connection
terminal	Set terminal characteristics
testemail	Send a test email message
traceroute	Trace route to destination
two-factor	Change your two factor settings
undebug	Disable debugging function (also see ’debug’)
virtual-machine	Virtual machine commands
vrrp	VRRP commands
wireguard	Wireguard configuration

Example:

```
Perle# archive update
```

Global Configuration Mode

```
Perle(config)# ?
```

- The "(config)#" indicates that the current mode is "Global config mode ". Depending on the model, some options may not be available.

aaa	Authentication, Authorization and Accounting
alarm	Environmental facilities
archive	Archive software and configuration commands
arp	Set ARP options or static entry
banner	Define a login banner
boot	Modify system boot parameters
bridge	Bridge group and spanning-tree logging
cellular	Cellular configuration parameters
class-map	Configure class map
clock	Configure time-of-day clock
container (OCI)	Configure container (OCI) applications
container management (OCI)	Configure container (OCI) management
controller	Configure a specific controller
crypto	Encryption operations
default	Set a command to its default
do-exec	Run exec command in config mode
dot1x	IEEE 802.1X global configuration commands
eap	EAP global configure commands
email	Email notifications configuration
enable	Set enable password
end	End the config session
exit	Exit config mode
help	Description of interactive help
hostname	Set system’s network name
interface	Select an interface
ip	Global configuration commands
ipv6	Global IPv6 configuration commands

key	Key management
ldap	LDAP server configuration command
line	Configure a terminal line
lldp	Global LLDP configuration subcommands
logging	Set logging
login	Login configuration
mac	Global MAC configuration subcommands
management-access	Management access commands
nat66	NAT66 interface commands
network-watchdog	Configure network watchdog
no	Negate a command or set its default
ntp	Configure NTP
policy-map	Configure policy map
power-supply	Set the system power supply settings
radius	RADIUS configuration
radius-server	RADIUS server configuration
remote-management	Configure remote management/RESTful API
route-map	Create route map or enter route map mode
router	Enable a routing process
sdm	Configure system network profile (enable IPv6)
serial	Serial commands
service	Network based services configuration
snmp-server	Enable SNMP, modify SNMP engine parameters
tacacs	TACACS+ configuration
tacacs-server	TACACS+ server configuration
tty	Configure terminal controller
usb	Configure USB parameters
username	Configure user name authentication
virtual-machine	Virtual Machine commands

wan	Configure WAN management
zone	Firewall with zoning
zone-pair	Zone pair firewall

```
Perle#configure
Configuring from terminal
Perle(config)#
Perle(config)#interface eth 1
Perle(config-if)#
```

Show Command Filtering and Redirection

The IOLAN's CLI command prompt provides you ways of searching through large amounts of show/more output and then filtering the output according to parameters (regular expressions) that you supply on the command line. This allows you to filter on patterns such as a phrase, number, or more complex patterns.

A regular expression can be a single-character pattern or a multiple-character pattern. That is, a regular expression can be a single character that matches the same single character in the command output or multiple characters that match the same multiple characters in the command output. The pattern in the command output is referred to as *<LINE>*. This section describes creating both single-character patterns and multiple-character patterns.

```
[begin | count | exclude | include} <LINE> |
        section [exclude | include] <LINE> |
        format json |
        redirect flash: <file-name> |
           ftp:///[[username:password@]{hostname | host-ip}/directory]/<filename> |
           http://[[username:password]@]{hostname | host-ip}/ [directory]/<filename> |
           http://[[username:password]@]{hostname | host-ip}/ [directory]/<filename> |
           nvram:<file-name> |
           scp://[[username:password@location]/directory]/<filename> |
           sftp://[[//username:password]@location]/directory]/<filename> |
           tftp://[{hostname | host-ip}/ [directory]/<filename> |
        append flash: <file-name> | nvram:<file-name> |
        tee /append]flash:<file-name> |
           ftp:///[[username:password@]{hostname | host-ip}/directory]/<filename> |
           http://[[username:password]@]{hostname | host-ip}/ [directory]/<filename> |
           http://[[username:password]@]{hostname | host-ip}/ [directory]/<filename> |
           nvram:<file-name> |
           scp://[[username:password@location]/directory]/<filename> |
           sftp://[[//username:password]@location]/directory]/<filename> |
           tftp://[{hostname | host-ip}/ [directory]/<filename>}
```

Output Modifiers

append — Appends redirected output to the specified flash: or nvram: filename.

begin — Begin unfiltered output with the first line that contains the regular expression and every line there after.

count — Displays a count of the number of occurrences of the regular expression.

exclude — Display output lines that do not contain the regular expression.

format — Format the output using the specified format.

include — Display output line that contain the regular expression.

redirect — Redirect output to specified URL and file name. The file is created or overwrites it if it already exists.

section — Displays output lines that contain the regular expression as well as any lines associated, (any lines immediately following the line that contains the regular expression).

tee — Display the output on-screen while being redirected or appended to the specified URL and file name.

line — This is a regular expression that is used to filter the output.
A regular expression is a pattern (a phrase, number, or more complex pattern) that the IOLAN's CLI command uses to match against show or more command output. Regular expressions are case-sensitive and allow for simple matching requirements such as "include" entries like "serial or 138".

Single-Character Patterns

The simplest regular expression is a single character that matches the same single character in the command output.
You can use any letter

- (A-Z, a-z)
- or digits (0-9)
- or characters such as ! or ~

Certain key board characters have special meaning using in regular expressins.The table below lists the keyboard character that have special meaning.

Character	Special Meaning
.	Match any single character, including white space.
*****	Matches 0 or more sequences of the pattern.
+	Displays output lines that do not contain the regular expression.
?	Matches 0 or 1 occurrences of the pattern. Use <ctl-v) if you need to enter a "?".
^	Matches the beginning of the string.

$	Redirect output to specified URL and file name. The file is created or overwrites it if it already exists.
(underscore)	Matches a comma (,), left brace ({), right brace (}), right parenthesis ()), left parenthesis ((), the beginning of the string, the end of the string, or a space.

To use these special characters as single-character patterns, you must remove the special meaning by preceding each character with a backslash (\).
For example:
\$ = $ (dollar sign)
_ = _ (underscore)
\+ = + (plus symbol

You can also specify a range of single-character matches against the command output by placing the square brackets around the characters to be matched.
For example:
[abcd] or simply [a-d]

You can include a left square bracket ([) as a single-character pattern in your range, by preceding the ([) with a backslash. The following example match son character a-d and ([)
For example:
[a-d\[]

You can reverse the matching of the range by including a caret (^) at the start of the range. The following example matches any letter except the ones listed.
For example:
[^a-dqsk]

Multiple-Character Patterns

When creating regular expressions, you can also specify a pattern containing multiple characters. You create multiple-character regular expressions by joining letters, digits, or keyboard characters that do not have special meaning.
For example:
a4% = a multiple-character regular expression.
Note: Insert a backslash before the keyboard characters that have special meaning when you want to indicate that the character should be interpreted literally.
\$ = $ (dollar sign)
_ = _ (underscore)
\+ = + (plus symbol

Order is important with multiple-character patterns. The regular expression b5! matches the character b followed by a 5 followed by a ! symbol. If the string does not have b5!, in that order, pattern matching fails.

In this example the multiple-character regular expression b.uses the special meaning of the period character to match the letter a followed by any single character. The use of (.) period character within a multiple-character expression has a special meaning in that any character matching after the initial character is deemed a match.
For example:
b. = matches bb, b!, b2

Note: You can remove the special meaning of the period character by inserting a backslash before it. For example, when the expression b\. is used in the command syntax, only the string b. is matched.

You can also create multiple-character regular expressions with combination of letters, digits, and other keyboard characters.
For example:
abc33vu77 is a valid regular expression.

2 User Exec Mode

Once you have accessed the IOLAN, you are automatically in User Exec mode. The following commands are valid in User EXEC mode. Some CLI commands may not be applicable to your model or running software.

clear ip dhcp binding

Syntax Description	clear ip dhcp binding
* | *A.B.C.D*}	Type * to clear all automatic bindings. Type the IPv4 address of the specific DHCP binding to clear.
Command Modes	Perle>clear ip dhcp binding

Usage Guidelines

Use this command to clear DHCP client bindings. The * parameter clears all or enter the IPv4 address to clear.

Examples

This example clears all IP DHCP client bindings.

```
Perle>clear ip dhcp binding *
```

This example clears IP DHCP bindings for a specified IP address.

```
Perle>clear ip dhcp binding 172.16.113.44
```

Related Commands

renew

release

enable

Syntax Description	enable
Command Modes	Perle>enable

Usage Guidelines

Use this command to elevate the user from user exec level to privileged level.

Examples

This example sets user level to privileged level.

```
>enable
Password:perle
Perle#
```

Related Commands

disable

exit

exit

Syntax Description	exit
Command Modes	Perle>exit

Usage Guidelines

Use this command to exit from EXEC mode.

Related Commands

logout

disable

line-attach

Syntax Description	line-attach
{[tty*<1-x>* *<WORD>*] |	Applies only to models with serial ports. Number of serial ports depends on model. Displays available serial ports configured for ssh or telnet protocol. On user log in, line access privileges will be based on this authentication not the original authentication request. *<WORD>* SSH user name is optional. If it is not entered, the username logged into the IOLAN's main session is used.
[usb *<1-8>* *<WORD>*]}	Applies only to models with serial USB ports. Available ports are configured for SSH or Telnet protocol. On user log in, line access privileges will be based on this authentication not the original authentication request. *<WORD>* SSH user name is optional. If it is not entered, the username logged into the IOLAN's main session is used.
Command Modes	Perle>line-attach

Usage Guidelines

Use this command to connect to serial ports configured as Console Management ports. The available ports for both Telnet and SSH are displayed. This feature only exists on models which have serial port/s.

Examples

This example connects a user to serial port 1.

```
Perle>line-attach tty 1
```

logout

Syntax Description	logout
logout	Logs out of the IOLAN.
Command Modes	Perle>logout

Usage Guidelines

Use this command to log out of the IOLAN.

Examples

This example logs you out of your IOLAN.

```
Perle>logout
```

password

Syntax Description	password
Command Modes	Perle>password

Usage Guidelines

Allows logged in user to change their own password.

Examples

This example changes a logged in user's password.

```
Perle> password
Password must be less than 128 characters long
May not use 5 previous Passwords
Enter Old password
Enter New password
Re-Enter new password
```

ping

Syntax Description	ping
{*<WORD>* **data** *<HEX DIGITS>* **| repeat** *<1–2147483647>* **| size** *<36–18024>*}	Configure the destination. • IPv4 address or IPv6 address • Host name (pre-configured in your IOLAN's host table) or a DNS server needs to be reachable • Data—input in hex data to repeat • Repeat—how many time to run the ping command • Size—Configure the size of the packet to ping with

Command Default	56 (84) bytes of data 10 times
Command Modes	Perle>ping

Usage Guidelines

Use this command to ping a remote host.

This example pings a host with an IP address of 172.16.113.44 and repeats the ping 10 times.

```
Perle>ping 172.16.113.44 repeat 10
64 bytes from 172.16.4.90: icmp_seq=1 ttl=64 time=2.91 ms
64 bytes from 172.16.4.90: icmp_seq=1 ttl=64 time=1.17 ms
64 bytes from 172.16.4.90: icmp_seq=1 ttl=64 time=2.93 ms
64 bytes from 172.16.4.90: icmp_seq=1 ttl=64 time=1.666 ms
64 bytes from 172.16.4.90: icmp_seq=1 ttl=64 time=0.921 ms
64 bytes from 172.16.4.90: icmp_seq=1 ttl=64 time=1.05 ms
64 bytes from 172.16.4.90: icmp_seq=1 ttl=64 time=1.118 ms
64 bytes from 172.16.4.90: icmp_seq=1 ttl=64 time=1.00 ms
64 bytes from 172.16.4.90: icmp_seq=1 ttl=64 time=1.00 ms
64 bytes from 172.16.4.90: icmp_seq=1 ttl=64 time=1.50 ms
64 bytes from 172.16.4.90: icmp_seq=1 ttl=64 time=0.897 ms
```

Related Commands

testemail
show ip interface

release

Syntax Description	**release dhcp | dhcpv6**
{**dhcp | dhcpv6 [bvi** *<1–9999>*] | [**ethernet** *<1-x>*. *<1–4000>*] | [**sfp** *<1-x>*]}	Type the Ethernet interface (and sub-interface) or BVI interface to release the DHCP/DHCPv6 IP address. Ethernet values are ***<1-x>*** <1-x> = maximum number of Ethernet ports, (depends on the model) sub-interfaces 1–4000 bvi values are 1–9999 SFP values 1-x (depends on the model)
Command Modes	Perle>release dhcp

Usage Guidelines

Use this command to release the DHCP/DHCPv6 IP address given to the IOLAN by the DHCP/DHCPv6 server. To obtain a new DHCP/DHCPv6 IP address lease, use the DHCP/DHCPv6 renew command.

Examples

This example releases the DHCP IP address for Ethernet interface 2.

```
Perle>release dhcp ethernet 2
```

Related Commands

renew

renew

Syntax Description	renew dhcp | dhcpv6
{**dhcp | dhcpv6 [bvi** *<1–9999>*] | [**ethernet** *<1-x>*. *<1–4000>*] | [**sfp** *<1-x>*]}	Type the Ethernet interface (and sub-interface) or BVI interface to renew the DHCP/DHCPv6 IP address. Ethernet values are ***<1-x>***, sub-interfaces 1–4000 <1-x> = maximum number of ethernet ports, (depends on the model) Bvi values are 1-9999 SFP values 1-x (depends on the model)
Command Modes	Perle>renew dhcp

Usage Guidelines

Use this command to renew the DHCP/DHCPv6 IP address lease from the DHCP/ DHCPv6 server pool.

Examples

This example renews the DHCP lP address lease on Ethernet 1.

```
Perle>renew dhcp eth 1
```

Related Commands

release

show alarm

show alarm

Syntax Description	show alarm
{**description port |**	Displays alarm statuses. • 1—Link Fault • 2—Port not-forwarding • 3—Port not operating

profile [<*WORD*>] |	Type the alarm profile name to view.
settings enabled |	Displays settings for enabled alarms.
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show alarm

Usage Guidelines

Depending on the model, your show alarms output maybe different.

Use this command to display alarm descriptions, profiles, and enabled alarms.

Link has failed—The IOLAN generates a link fault alarm when problems with a port's physical layer causes unreliable data transmission. A typical link fault condition is loss of signal or clock. The link fault alarm clears automatically when the link fault condition clears. The severity for this alarm is error condition, level 3.

Port not forwarding—Only used for Ethernet ports. The IOLAN generates a port not-forwarding alarm when a port is not forwarding packets. This alarm clears automatically when the port begins to forward packets. The severity for this alarm is warning, level 4.

Port not operating—The IOLAN generates a port not-operating alarm when a port fails during the startup self-test. When triggered, the port not-operating alarm only clears when the IOLAN is restarted and the port is operational. The severity for this alarm is error condition, level 3.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

To show alarm descriptions.

```
Perle>show alarms description
1 Link Fault
2 Port not Forwarding
3 Port Not Operating
```

```
Perle>show alarms profile

     Alarms     link fault, not operating
     Syslog     link fault, not operating
     Notifies   link fault, not operating
```

Related Commands

alarm

show arp

Syntax Description	**show arp**

{<A.B.C.D> |	Displays the ARP table or entry.
{[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show arp

Usage Guidelines

Use this command to display the ARP table or entry.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays the ARP table.

```
Perle>show arp
Address          Hardware Addr       Interface       Hw Type
172.16.23.124        6c:3b:e5:20:26:db    eth3            ether
172.16.73.200        a4:bb:6d:ac:5c:65    eth3            ether
```

Related Commands

clear arp-cache

arp

show clock

{[<*filter/redirection options*>]}

Syntax Description	**show clock**
{[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show clock

Usage Guidelines

Use this command to display current clock information.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example shows you how to display clock information.

```
Perle>show clock
.Tue Mar 16 17:58:02 EDT 2021
```

Related Commands

clock

show crypto

Syntax Description	show crypto
{ipsec [client <*WORD*>] | [esp-group <*WORD*>] | [ike-group <*WORD*>] | [ipsec.conf] | [12tp] | [status] |	Displays crypto details. Displays L2TP details. Displays status. IPsec client (peer)—typically @leftside or a hostname.
openvpn ca [<*NAME*>] | cert [<*NAME*>] | connection [<*WORD*>] | dh [<*WORD*>] | key [<*NAME*>] | secret [<*NAME*>] | [status] | template [<*NAME*>] |	Displays OpenVPN details.
pki client trustpoint | openvpn ca [<*NAME*>] | cert [<*NAME*> | key [<*NAME*>] | server trustpoints [<*WORD*>] | [status] |	Displays details for pki client trustpoints, and OpenVPN.
r**adsec ca <*NAME*> | cert <*NAME*> | key <*NAME*> |**	Displays detail for RadSec trustpoint, certificate, and private key
ssl |	Displays SSLdetails.
wireguard [interface address | description | information | peer <*NAME*> | port | status] | public-key}	Displays WireGuard details.
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show crypto

Usage Guidelines

Use this command to display session information for encryption based services.

Examples

This example displays the version of SSL installed on the IOLAN.

```
Perle>show crypto ssl
SSL cipher suite: TLS v1.2
```

Related Commands

crypto

show dot1x

Syntax Description	show dot1x
{**[all** | **details** | **statistics]** |	Select all, details, or statistics to view dot1x connection details.
[credential ***<WORD>*****]** |	Displays the credential profile for this user.
interface ethernet ***<1-x>*** | **sfp** ***<1-x>*** | **details** | **statistics]** |	Enter the Ethernet interface to show connections authenticated with dot1x. <1-x> = maximum number of ethernet ports, SFP values 1-x (depends on the model)
[radius statistics interface [ethernet ***<1-x>*****]** | **[sfp** ***<1-x>*****]** |	Displays RADIUS statistics for authenticator mode. <1-x> = maximum number of ethernet ports, (depends on the model) SFP values 1-x (depends on the model)
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show dot1x

Usage Guidelines

Use this command to display the connection information for Dot1x supplicant and authenticator connections.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Related Commands

dot1x

(config-dot1x-creden)

show eap

Syntax Description	show eap
{**profile** ***<WORD>*** |	Displays pre-defined EAP profiles.
registrations |	Displays registered EAP methods.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show eap

Usage Guidelines

Use this command to display configured methods and pki-trustpoints for EAP configured profiles. EAP profiles are configured using the eap profile <name> command. The registration show command displays the EAP methods supported by your IOLAN.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays eap registrations.

```
Perle>show eap registrations

Registered EAP Methods:
=======================
 Method  Type          Name
   4     Auth and Peer   MD5
   6     Auth and Peer   GTC
   13    Auth and Peer   TLS
   21    Auth and Peer   TTLS
   25    Auth and Peer   PEAP
   26    Auth and Peer   MSCHAPV2
```

Related Commands

eap

(config-eap-profile)

show environment

Syntax Description	**show environment**
{**all | power status** |	Show power details.
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show environment

Usage Guidelines

Use this command to show the IOLAN's environment. Output can be different depending on your model.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example shows power supply statuses.

```
Perle>show environment power status
POWER SUPPLY 1 is DC OK
  Power sensor value: 12.00 Volts
POWER SUPPLY 2 is DC OK
  Power sensor value: 12.00 Volts
```

show facility-alarm

Syntax Description	**show facility-alarm**
{**status |**	Displays source and severity of the alarm.
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show facility-alarm

Usage Guidelines

Use this command to display alarm statuses. Output can be different depending on your model.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example shows facility alarms.

```
Perle>show facility-alarms

Source          Severity Description                          Actions          Time
---------------- -------- ------------------------------------ ---------------- --------------------
Sfp1            MAJOR    Link Fault                                             Sep  1 2023 16:35:03
```

show flash:

Syntax Description	**show flash:**
{[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show flash:

Usage Guidelines

Use this command to display files on the internal flash drive.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

```
Perle>show flash:
Directory of flash:
 14      drwx     4096 Dec 31 2019 19:00 -04:00 doc
 32      -rw-      932 Nov 23 2020 16:52 -04:00 perle-internal.log
2254      dr-x     1024 Jan 3 2020 20:36 -04:00 copyright
 37      -rw-   717385 Mar 14 2021 04:12 -04:00 managed-devices.yaml
 28      -rw-        5 Jan 5 2020 18:27 -04:00 update-sw-control.txt

1372160 KBytes total (1282048 KBytes free)
```

Related Commands

delete

mkdir

copy

dir

cd

rmdir

show hosts

Syntax Description	show hosts
{[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show hosts

Usage Guidelines

Use this command to display the host table.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays host table information.

```
Perle>show hosts
Default domain name is Perle
DNS lookup is enabled
Name servers are not configured

Host Table:
accounting-host 172.16.77.99
banking-host 172.16.88.99
test-host 172.16.55.44
```

Related Commands

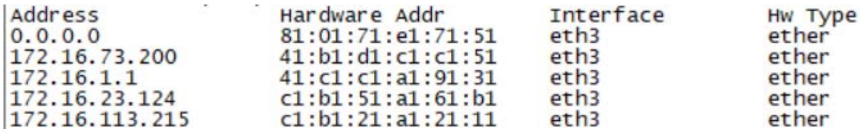
ip host

show ip arp

Syntax Description	show ip arp
{<*A.B.C.D*> |	Enter the arp ip address.
{[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show ip arp

Examples

Perle>show ip arp



```
Address                    Hardware Addr        Interface        Hw Type
0.0.0.0                    81:01:71:e1:71:51    eth3             ether
172.16.73.200              41:b1:d1:c1:c1:51    eth3             ether
172.16.1.1                 41:c1:c1:a1:91:31    eth3             ether
172.16.23.124              c1:b1:51:a1:61:b1    eth3             ether
172.16.113.215             c1:b1:21:a1:21:11    eth3             ether
```

Usage Guidelines

Use this command to display ARP entries.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Related Commands

arp

show ip ddns

Syntax Description	show ip ddns
{**service [bvi** <*1–9999*>**] | [cellular** <*0–0*>>**] | [dialer** <*0–15*>**] | [ethernet** <*1-x*>**] | [sfp** <*1-x*>**] | [openvpn-tunnel** <*0–999*>**] | [tunnel** <*0–999*>**] |**	Displays interfaces with DDNS service enabled. <1-x> = maximum number of ethernet ports, (depends on the model) SFP values 1-x (depends on the model)
use-web [bvi <*1–9999*>**] | [cellular** <*0–0*>>**] | [dialer** <*0–15*>**] | [ethernet** <*1-x*>**] | [sfp** <*1-x*>**] | [openvpn-tunnel** <*0–999*>**] | [tunnel** <*0–999*>**] |**	Web check used for obtaining the external IP address. <1-x> = maximum number of ethernet ports, depends on the model SFP values 1-x (depends on the model)
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show ip ddns

Usage Guidelines

Use this command to display information for Dynamic DNS (DDNS).

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays the DDNS service configured on Ethernet port 2.

```
Perle>show ip ddns service ethernet 1
Service dyndns
  Login      testddns
  Password   ********
```

show ip dhcp

[*<filter/redirection options>*]}

Syntax Description	**show ip dhcp**
{**bindings | pool** *<WORD>* |	Displays current bindings.
[pool *<WORD>*] |	Displays current DHCP configured pools.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show ip dhcp

Usage Guidelines

Use this command to display DHCP bindings and pool information.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays the configured DHCP pools.

```
Perle>show ip dhcp pool
Pool pooltest:
  Total addresses: 11
  Leased addresses : 2
  Exluded addresses: 0
  IP address Range: 172.16.113.60 - 172.16.113.70
```

Related Commands

renew

release

show ip host-group

Syntax Description	**show ip host-group**
{[*<WORD>*] |	Displays IP host group.

[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show ip host-group

Usage Guidelines

Use this command to display IP Host Group information.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays all IP host groups.

```
Perle>show ip host-group
Host list: Perle
 172.16.66.99
  radius
  Rad2
```

show ip http

Syntax Description	**show ip http**
{**server status** |	Displays the configured HTTP server parameters.
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show ip http

Usage Guidelines

Use this command to display HTTP server information.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays the parameters for the HTTP server.

```
Perle>show ip http server status
HTTP server status: Enabled
HTTP server port:80
User session idle timeout: 1440 seconds
HTTP secure server status: Enabled
HTTP secure server port: 443
```

Related Commands

ip http

show ip interface

Syntax Description	show ip interface
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show ip interface

Usage Guidelines

Use this command to display all interfaces on the IOLAN.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays the IP interfaces.

```
Perle>show ip interface
```

Related Commands

(config-if)#
(config-if)#cellular
(config-if)#openvpn-tunnel
(config-if)#tunnel

show ip ssh

Syntax Description	show ip ssh
{[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show ip ssh

Usage Guidelines

Use this command to display IP SSH information.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays SSH information.

```
Perle>show ip ssh
SSH version: 2
SSH server: Enabled
Authentication timeout: 120 seconds
Authentication retries: 3
SSH public key:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCgAtvWaaM0CeMWoZV1H00sni2J8TYaI
vSyysQGyBDIOAydaaKv1+s1Imj00FL2Boi3ke/
SoKhvuLJQ+bMVFXD7kXw2fk71Mo8f8Dd/
rOuuF4kE6hKV+LLI44kJKwCUC2w2m4L1IH8Zn8HuX89Qcv2oqPUdkBfO1neIU3gc6g
N4v1ckC069Tgg9hrhghCiBECCCYxmAJUhIy4dQcPwO1DQ6Acp2p3IW2RYdgUvRAI
r8oLiVdrEvT7zZECpYgCMYWmfsTtUhvv8yZpvNAhV9nRm5E93YI0V2J15qImIISGKn
0iiLRW42xjQ4MT5XmWdIXj+NpuMIQRtFzyYPkR2HMf+9
```

Related Commands

ip ssh

show ipv6

Syntax Description	show ipv6
{**dhcp binding | interface client-mode | pool |**	Shows DHCP parameters.
interface |	Shows interface configuration and status.
neighbours [bvi *<1-9999>*] **[cellular** *<0-0>*]| **[ethernet** *<1-x>*] | **[sfp** *<1-x>*] | **[tunnel** *<0-999>*] |	Shows neighbours cache entries. <1-x> = maximum number of ethernet ports SFP values 1-x (depends on the model)
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show ipv6

Usage Guidelines

Use this command to display IPv6 information.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

Show IPv6 interfaces.

```
Perle>show ipv6 interface
```

Related Commands

clear ipv6

ipv6

show ldap

Syntax Description	**show ldap**
{**ldap statistics [details]** |	Shows LDAP statistics details.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show ldap

Usage Guidelines

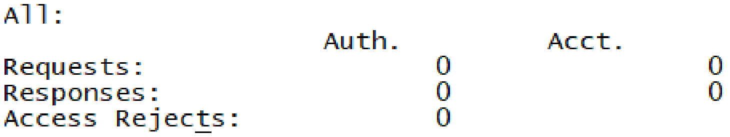
Use this command to display LDAP statistic details.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

Shows LDAP statistics details.

Perle>show ldap statistic details



```
All:
                          Auth.          Acct.
Requests:                    0                    0
Responses:                   0                    0
Access Rejects:              0
```

Related Commands

ldap

show line

Syntax Description	**show line**
{**console** *<0–0>* |	Applies only to models with serial, and console ports. Shows configured parameters.
tty *<1-x>* |	Shows configured parameters. Depends on the model.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***

Command Modes	Perle>show line

Usage Guidelines

Use this command to display primary terminal line.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

Shows line statuses.

```
Perle>show line
```

```
Console in use: Serial
Baud rate (TX/RX) is 9600/9600, parity none, 1 stop
bit, 8 data bits
```

Related Commands

line

show lldp

Syntax Description	**show lldp**
{**interface ethernet** *<1-x>* **| |** **[sfp** *<1-x>***] |**	Displays LLDP interface configuration.< 1-x> = maximum number of ethernet ports, (depends on the model) SFP values 1-x (depends on the model)
neighbors interface [ethernet *<1-x>***] | [sfp** *<1-x>***] [detail | summary] |**	Displays LLDP neighbors information.< 1-x> = maximum number of ethernet ports, (depends on the model) SFP values 1-x (depends on the model)
traffic summary |	Displays LLDP statistics.
[*<filter/redirection options>***]**}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show lldp

Usage Guidelines

Use this command to display LLDP interface configuration, neighbors statistics and traffic statistics.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

Show LLDP configuration for Ethernet port 10.

```
Perle>show lldp interface ethernet 10
Tx: enabled
Rx: enabled
Maximum Neighbors: 10
TLVs Advertised:
port-description, system-name, system-description, system-capabilities,
management-address mac-phy-cfg, max-frame-size
```

Related Commands

clear lldp

lldp

show mab

Syntax Description	**show mab**
{**all details** | **statistics** |	Displays MAB information.
interface ethernet *<1-x>* | **[sfp** *<1-x>*] **details** | **statistics** |	Displays interface MAB details. <1-x> = maximum number of ethernet ports, (depends on the model) SFP values 1-x (depends on the model)
radius statistics interface ethernet *<1-x>* | **[sfp** *<1-x>*] |	Displays RADIUS MAB details. <1-x> = maximum number of ethernet ports, (depends on the model) SFP values 1-x (depends on the model)
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show mab

Usage Guidelines

Use this command to display MAB (MAC Authentication Bypass) for the Ethernet interfaces or RADIUS.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples:

Shows the MAB interface details for Ethernet interface 1.

```
Perle>show mab interface ethernet 1 details
Interface           Mac-Auth-Bypass
-----------------------------------
Ethernet3           Enabled
MAC Auth Bypass Client List
--------------------------
Supplicant           = 00:16:d3:2f:62:bb
 EAP Method           = None
 Port Control State  = Auto
 Auth SM State        = AUTHENTICATED
 Auth BkEnd SM State = IDLE
 Session ID          = B8B01A9D-00000001
 Session Time         = 855
 Identity            = 0016d32f62bb
Eapol Frame Counters: ..............
 ..........................................................................................................
```

show mac

Syntax Description	show mac
{[**access-list [all] | [interfaces] | [list-name <*WORD*>] |**	Displays MAC access list by all, interfaces or list-name.
[address-table [address <*H.H.H*>] | [dynamic] | [interface ethernet <*1-x*> | [sfp <*1-x*>] | [multicast] | [static] |	Show MAC address details. <1-x> = maximum number of ethernet ports, (depends on the model) SFP values 1-x (depends on the model)
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show mac

Usage Guidelines

Use this command to display a listing of MAC addresses and MAC access lists.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

Show the dynamic MAC address table.

```
Perle>show mac address-table dynamic
```

```
 Mac Address Table
----------------------------------------
Vlan    Mac Address       Type       Ports
----    --------------    -------    -----
  99    0016.3e08.2cbc    DYNAMIC    eth1
  99    0018.f37b.6bb0    DYNAMIC    eth1
  99    0024.c4a2.1762    DYNAMIC    eth1
  99    0080.d406.1df3    DYNAMIC    eth1
  99    00a0.45d9.56dc    DYNAMIC    eth1
  99    24b6.fd13.8885    DYNAMIC    eth1
  99    3085.a9a7.b59e    DYNAMIC    eth1
  99    3c97.0e37.120d    DYNAMIC    eth1
  99    588a.5a44.1903    DYNAMIC    eth1
  99    7071.bc23.1a8f    DYNAMIC    eth1
  99    80ce.62ee.8ab7    DYNAMIC    eth1
  99    80ce.62ee.8c2d    DYNAMIC    eth1
  99    e840.f24a.2cce    DYNAMIC    eth1
  99    f092.1ce3.5748    DYNAMIC    eth1
  99    f48e.3898.ee2c    DYNAMIC    eth1
Total Mac Addresses for this criterion: 15
```

Related Commands

mac

show mac

show ntp

Syntax Description	**show ntp**
{**[associations] |**	NTP clock associations information.
[status] |	NTP clock status.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show ntp

Usage Guidelines

Use this command to display NTP associations and status.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

```
Perle>show ntp associations
remote          refid       st t when poll reach   delay   offset jitter
==============================================================
 172.16.55.77    .INIT.         16 u    - 1024    0    0.000    0.000   0.000
 172.16.113.55   .INIT.         16 s    -   32    0    0.000    0.000   0.000
Perle>show ntp status
Clock is not synchronized, stratum 16, no reference clock
Precision is 2**-18 s
Reference time is 00000000.00000000 (Thu, Feb 7 2036 2:28:16.000)
Clock offset is 0.000000 msec, root delay is 0.000 msec
Root dispersion is 1265.970 msec
System poll interval is 8 s
```

Related Commands

ntp

show nvram:

Syntax Description	**show nvram:**
{[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show nvram:

Usage Guidelines

Use this command to display the contents of nvram: file system.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

```
Perle>show nvram:
Directory of nvram:
89        -rw-     8436 Feb 16 2021 20:50 06:00 startup-config.log.2
 18        -rw-      285 Jan 9 2020 05:06 06:00 no-default-config
 21        -rw-     8950 Feb 19 2021 21:05 06:00 startup-config
 90        -rw-     9054 Feb 18 2021 23:37 06:00 startup-config.log.1
 81        -rw-     9054 Feb 19 2021 21:09 06:00 startup-config.log
 86        -rw-    12289 Nov 23 2020 22:24 06:00 y
 16        -rw-      636 Jan 9 2020 05:06 06:00 default-config

1372160 KBytes total (970752 KBytes free)
```

Related Commands

delete

dir

mkdir

rename

rmdir

pwd

cd

show radius

Syntax Description	show radius
{[statistics [details] |	Show RADIUS server statistics.
[radsec] |	Show Radsec information.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show radius

Usage Guidelines

Use this command to show RADIUS or RadSec details.

Examples

Use this command to display RADIUS statistics.

```
Perle>show radius statistics
All:
                Auth.          Acct.
Requests           3              3
Responses          3              3
Access Requests    3
```

Related Commands

clear radius

aaa

radius

radius-server

ip radius

show snmp

Syntax Description	show snmp
{[contact] |	Displays contact information

[location] |	Displays location information.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show snmp

Usage Guidelines

Use this command to show configured options for SNMP.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example show the contact information.

```
Perle>show snmp contact
Labarea
```

Related Commands

snmp-server

show ssh

Syntax Description	**show ssh**
{[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show ssh

Usage Guidelines

Use this command to display users connected via SSH.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example show which users are connected.

```
Perle>show ssh
Line      User      Host              Idle      Location
 1   vty 1 admin     idle              00:28:26   172.16.113.31
```

Related Commands

show ip ssh

show tacacs

Syntax Description	show tacacs
{[statistics [details] |	Displays TACACS+ statistics.
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show tacacs

Usage Guidelines

Use this command to display TACACS+ server details.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

Show TACACS+ statistics.

```
Perle>show tacacs statistics
All:
               Auth.          Acct.
Requests          3              3
Responses         3              3
Access Requests   3
```

Related Commands

clear tacacs

(config-sg-tacacs)

tacacs

(config-tacacs-server)

show terminal

Syntax Description	show terminal
{[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show terminal

Usage Guidelines

Use this command to display terminal parameters length, width, history enabled, history size, and logging monitor.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This examples displays the parameter for terminal.

```
Perle>show terminal
  Terminal length = 24
  Terminal width = 79
  Terminal history is enabled
  Terminal history size = 11
  Terminal logging monitor is OFF
```

show users

Syntax Description	**show users**
{**[all] |**	Displays all users.
[console] |	Displays users connected to the console if your model supports a console port.
[rest-api] |	Displays RESTful API users.
[vty] |	Displays users connected via ssh or telnet.
[web] |	Displays web users (HTTP/HTTPS).
[*<filter/redirection options>***]**}	Output modifiers see ***Show Command Filtering and Redirection***

Command Modes	Perle>show users

Usage Guidelines

Use this command to display active users.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This examples displays all attached web users.

```
Perle>show users web
User      IP Address                Idle
Lyn       172.16.113.215            00:11:59
```

Related Commands

username

show users

show version

Syntax Description	**show version**

{**[backup] |**	Displays backup version of software.
[flash:] |	Displays version information about an image in the flash: file system.
[startup] |	Displays the version of software used for startup.
[verbose]}	Displays details about software running on your IOLAN.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show version

Usage Guidelines

Use this command to display software version information.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays the startup version of software.

```
Perle>show version
```

ssh

Syntax Description	**ssh**
{**[*<A.B.C.D> <X:X:X:X::X>* [-c | -h | -l | -p *<A.B.C.D>*]**}	Configure a ssh session to a remote host. IPv4 or IPv6 address or hostname to connect to in ***<A.B.C.D> <X:X:X:X::X>*** format. ● c–select the encryption method ● h–select HMAC algorithm ● l–log in using this user name ● p–connect to this port
Command Modes	Perle>ssh

Usage Guidelines

Use this command to SSH from your IOLAN to a host supporting the SSH protocol.

Examples

This example connects to host (172.16.4.90) using lyn as the user.

```
Perle>ssh -l lyn 172.16.4.90
```

Related Commands

show ssh

telnet

Syntax Description	**telnet**
{*<A.B.C.D>* | *<X:X:X:X::X>*}	Configure a Telnet session to a remote host.
Command Modes	Perle>telnet

Usage Guidelines

Use this command to telnet from your   into a host that supports the telnet protocol.

Examples

This example telnets to host 172.16.4.90.

```
Perle>telnet 172.16.4.90
Trying 172.16.4.90...
Connected to 172.16.4.90.
Escape character is '^]'.
```

```
Red Hat Linux release 9 (Shrike)
Kernel 2.4.20-8custom on an i686
login:
```

Related Commands

ssh

terminal

Syntax Description	**terminal**
{**[history size** *<0–256>***]** |	Configure the size of the history buffer.
[length *<0–512>***]** |	Configure the length of the terminal screen
[monitor *<0–512>***]** |	Copies debugging logging output to the current terminal line.
[width *<0–512>***]**}	Configure width of the screen.
Command Default	length–24 width–132
Command Modes	Perle>terminal

Usage Guidelines

Use this command to configure parameters for your terminal session.

Examples

This example sets the terminal width to 132.

```
Perle>terminal width 132
```

Related Commands

show terminal

testemail

Syntax Description	testemail
{**email address**}	Configure the email address. Format is user@company.com
Command Modes	Perle>testemail

Usage Guidelines

Use this command to send a test email message.

Examples

```
Perle>testemail ltest@bigshow.com
Email Test message sent to lfelton@perle.com
```

Related Commands

ping

traceroute

Syntax Description	traceroute
{*<A.B.C.D>* | **hostname**| **icmp** *<A.B.C.D>* | **hostname**}	Destination hostname or address.
Command Modes	Perle>traceroute

Usage Guidelines

Use this command to trace network connections from one location to another. When a traceroute is run, it returns a list of network hops and displays the host name and IP address of each connection. It also returns the amount of time it took for each connection to take place (usually in milliseconds). This shows if there were any delays in establishing the connection. Therefore, if a network connection is slow or unresponsive, a traceroute can often explain why the problem exists and also show the location of the problem.

Examples

This example displays the hops it takes from the IOLAN to IP host address 172.16.4.90.

```
Perle>traceroute 172.16.4.90 (172.16.4.90), 30 hop max, 60 bytes packets
1 172.16.4.90 (172.16.4.90)   2.094ms    1.113 ms     0.826 ms
```

Related Commands

ping

wireguard

Syntax Description	traceroute
[activate] |	Activate wireguard.
[deactivate] |	Deactivate wireguard.
Exports public key	
export public-key terminal | url flash:filename | ftp:[[//username[:password]@location]/directory]/filename | http://[[username:password]@][hostname | host-ip [directory] /filename | scp:[[username@location]/directory]/filename | sftp:[[//username[:password]@location]/directory]/filename | tftp:[[//location]/directory]/filename | usb *<1-8>*	
generate key default-keypair |	Generates wireguard interface key-pair.
Import wireguard private and public key.	

import private-key terminal | url flash:filename | ftp:[[//username[:password]@location]/directory]/filename | http://[[username:password]@][hostname | host-ip [directory] / filename | https://[[username:password]@][hostname | host-ip [directory] /filename | scp:[[username@location]/directory]/filename | sftp:[[//username[:password]@location]/directory]/filename | tftp:[[//location]/directory]/filename | usb ***<1-8>*** **| public-key terminal | url flash:filename | ftp:[[//username[:password]@location]/directory]/filename | http:// [[username:password]@][hostname | host-ip [directory] /filename | https://[[username:password]@][hostname | host-ip [directory] /filename | scp:[[username@location]/directory]/filename | sftp:[[//username[:password]@location]/directory]/filename | tftp:[[//location]/directory]/filename | usb** ***<1-8>***

Import wireguard private and public key.

import private-key terminal | url flash:filename | ftp:[[//username[:password]@location]/directory]/filename | http://[[username:password]@][hostname | host-ip [directory] / filename | https://[[username:password]@][hostname | host-ip [directory] /filename | scp:[[username@location]/directory]/filename | sftp:[[//username[:password]@location]/directory]/filename | tftp:[[//location]/directory]/filename | usb ***<1-8>*** **| public-key terminal | url flash:filename | ftp:[[//username[:password]@location]/directory]/filename | http:// [[username:password]@][hostname | host-ip [directory] /filename | https://[[username:password]@][hostname | host-ip [directory] /filename | scp:[[username@location]/directory]/filename | sftp:[[//username[:password]@location]/directory]/filename | tftp:[[//location]/directory]/filename | usb** ***<1-8>***

remove key default-keypair}	Remove wireguard interlace Key-pair.
Command Modes	Perle>wireguard

Usage Guidelines

Use this command to manage options for Wireguard.

Examples

This example exports a wireguard public-key from flash:

```
Perle>wireguard export public-key url flash:filename
```

Related Commands

show crypto

crypto

3 Privileged EXEC mode

This chapter contains the CLI commands for Privileged EXEC mode. Some CLI commands may not be applicable to your model or running software.

archive

Syntax Description	archive
{**config** |	Archives the running configuration. This configuration is saved to a predefined location as specified in the archive command. See to set up the path to where the configuration file is stored.
Downloads firmware to your IOLAN. **/force-reload**—unconditionally forces a system reload after successfully downloading the software image. **/reload**—reloads the system (if no unsaved configuration changes have been made) after a successful upgrade. **/no-version-check**—download the software without verifying it's version compatibility with the image running.	
download-sw | **[flash:***perle-image-name.img***]** | **[ftp://***[[username:password]@location]/directory]/perle-image-name.img***]** | **[http://***[[username:password]@][hostname* | *host-ip [directory] /perle-image-name.img***]** | **[https://***[[username:password]@][hostname* | *host-ip [directory] /perle-image-name.img***]** **[scp://***[[username:password@location]/directory]/perle-image-name.img***]** | **[sftp://***[[//username:password]@location]/directory]/perle-image-name.img***]** | **[tftp:***[[//location]/directory]/perle-image-name.img***]** | **usb** *<1-8>* |	
[update-sw auto-download | check] |	Checks if a software update is available. **auto-download**—automatically download firmware if new version found during check. **check**—check to see if a software update is available.
Command Modes	#archive

Usage Guidelines

Use this command to manage archive files.

Where a username or password is required it can be specified in the IOLAN configuration using the "scp | ftp | sftp | http" command to configure the username and password used instead of specifying it on the archive command.

flash:*image-file*

The syntax for FTP:

[ftp://*[[username:password]@location]/directory]/perle-image-name.img*] |

The syntax for an HTTP server:

http://*[[username:password]@][hostname* | *host-ip] [directory]/perle-image-name.img*

- The syntax for an HTTPS server:

https://*[[username:password]@][hostname* | *host-ip [directory]/perle-image-name.img*

- The syntax for an SCP server:

[scp://*[[username:password@location]/directory]/perle-image-name.img*] |

- The syntax for an SFTP server:

[sftp://*[[//username:password]@location]/directory]/perle-image-name.img*] |

- The syntax for an TFTP server:

[tftp:*[[//location]/directory]/perle-image-name.img*]

Examples

This example downloads software from a server with an IP address of 172.16.4.182 to your IOLAN using secure HTTP (https) and certificate named apache.crt

Step 1) Download a secure certificate to your IOLAN.
(config)#crypto pki import server apache pem url
tftp://172.16.4.182/apache.crt
Step 2)
Configure your IOLAN with the certificate you just downloaded.
(config)#ip http client secure-trustpoint apache

Step 3)
Set validation off if you do not want to valid the certificate. (You must have created the certificate with validation if you want to valid the certificate)
#archive download-sw
https://172.16.4.182/public/IOLAN-software.img or .emg
depending on the running firmware.

The software is download using secure https.
This example upload software from a server with an IP address of 172.16.4.92 using scp.
This command is only supported on some models.
Perle#archive upload-sw
scp://lyn:mypassword@172.16.4.92/public/IOLAN.img or .emg file
depending on the running firmware.

Related Commands

show archive

(config-archive)#

boot

{system backup}

Syntax Description	boot
{system backup}	Boots the system with the backup image.
Command Modes	Perle#boot

Usage Guidelines

Use this command to boot the IOLAN using an older saved software version. Older software versions can be stored as backup software using the archive command.

Examples

This example sets your IOLAN to boot using the backup software.

```
Perle#boot system backup
```

cd

{[flash: | nvram: | ssd | usb *<1-8>*]}

Syntax Description	cd
{[flash: | nvram: | ssd; | usb: *<1-8>*]}	Change directory on flash, nvram, ssd or usb.
Command Modes	Perle#cd

Usage Guidelines

Use this command to change directory within a file system.

Examples

This example changes to directory testdir under the flash file system.

```
Perle#cd flash:testdir
```

Related Commands

delete

pwd

mkdir

more

cd

rename

clear aaa

Syntax Description	**clear aaa**
{**aaa local user [fail-attempts all | username *<WORD>*] | [lockout all | username *<WORD>*]**}	Resets a locked out user. Resets this locked out user. Resets all locked out users. Resets this user using user name.
Command Modes	Perle#clear aaa

Usage Guidelines

Use this command to reset locked out users.

Examples

This example resets locked out user Marie.

```
#clear aaa local user lockout username Marie
```

Related Commands

aaa

clear arp-cache

Syntax Description	**clear arp-cache**
[bvi *<1-9999>*] |cellular *<0-0>* | s **[dialer *<0-15>*] | [ethernet *<1-* p** ***x> . <1-4000>*] | [openvpn- f** **tunnel *<0-999>*] | [sfp *<1-x>*] | f** **[tunnel *<0-999>*]**} **f**	Clears ARP cache on IP address or interface. <1-x> = maximum number of ethernet ports, (depends on the model) sfp <1-x> (depends on the model)
Command Modes	Perle#clear arp-cache

Usage Guidelines

Use this command to clear ARP entries from the ARP table.

Examples

This example clears all ARPs from the ARP table for Ethernet interface 1.

```
#clear arp-cache ethernet 1
```

Related Commands

show arp

arp

clear bridge

Syntax Description	clear bridge
{**spanning-tree counters interface bvi** *<1-9999>* | **ethernet** *<1-x>* . *<1-4000>* | **[sfp** *<1-x>***]**}	sClears spanning tree counters. p<1-x> = maximum number of ethernet ports, f(depends on the model) sfp <1-x> (depends on the model)
Command Modes	Perle#clear bridge

Usage Guidelines

Use this command to clear spanning tree counters.

Examples

This example clears spanning tree counters on Ethernet interface 1.

```
Perle#clear bridge spanning-tree counters interface ethernet 1
```

Related Commands

show bridge

bridge

clear counters

Syntax Description	clear counters
{**[bvi** *<1-9999>***]** | **[ethernet** *<1-x>***]** | **[sfp***<1-x>***]** | **[loopback]** | **[tunnel** *<0-999>***]**}	Clears counters on specified interface. <1-x> = maximum number of ethernet ports, (depends on the model) SFP values 1-x
Command Modes	Perle#clear counters

Usage Guidelines

Use this command to clear counters back to zero on the specified interface.

Examples

This example clears all counters for Ethernet interface 1.

```
Perle#clear counters ethernet 1
Clear "show interface" counters on this interface [confirm]
```

clear ip

Syntax Description	clear ip
{**[alg connections]** |	Clears ALG connections.

[bgp * | *<1-4294967295>* | *<A.B.C.D>* | *<X:X:X:X::X:X>* | [external in | out | soft] |	Type * to clear all BGP sessions or connections. Type the connection number, IPv4, or IPv6 address of the session or connection you want to reset. Configure whether it is an inbound or outbound session. No in/out parameters clears both in and outbound.
[dhcp binding <* | *<A.B.C.D>*] |	Type * to clear all automatic client bindings Type the ip address of the client you want to clear the DHCP binding.
[firewall *<WORD>*] |	Clears the specified firewall statistics.
[ospf process] |	Reset OSPF process.
[rip process] |	Reset RIP process.
route-policy name *<WORD>* counters | rule *<1-9998>* counters}	Clears counters for route policies.
Command Modes	Perle#clear ip

Usage Guidelines

Use this command to clear IP connections and statistics.

You can clear all DHCP bindings using the * parameter or clear only the binding for a specific IP address by entering in the IP address to clear.

You can also use this command to clear firewall statistics and counters for route policies.

Examples

This example clears all DHCP ip bindings from your DHCP IOLAN table.

```
Perle#clear ip dhcp bindings *
```

This example clears all BGP connections.

```
Perle#clear ip bgp *
```

clear ipv6

Syntax Description	clear ipv6
{firewall name *<WORD>* |	Clears IPv6 firewalls.
neighbors *<X:X:X:X::X:X>* | interface [bvi *<1-9999>*] | [cellular *<0-0>*] | [dialer *<0-15>*] | [ethernet *<1-x>* . *<1-4000>*] [vrrp *<1-255>*] | [openvpn-tunnel *<0-999>*] | [sfp *<1-x>*] | [tunnel *<0-999>*] |	Clears IPv6 neighbors. <1-x> = maximum number of ethernet ports, (depends on the model) sfp <1-x> depends on the model

route-policy name *<WORD>* counters | rule}	Clears IPv6 route policies.
Command Modes	Perle#clear ipv6

Usage Guidelines

Use this command to clear IPv6 entries for IPv6 firewalls, neighbors, and route policies.

Examples

This example clears route policy warehouse.

```
Perle#clear ipv6 route-policy warehouse
```

Related Commands

show ipv6

ipv6

clear ldap

Syntax Description	**clear ldap**
{**statistics**}	Clears LDAP statistic information.
Command Modes	Perle#clear ldap

Usage Guidelines

Use this command to clear LDAP statistic information.

Examples

This example clears LDAP statistics information on your IOLAN.

```
Perle#clear ldap statistics
```

Related Commands

(config-ldap-server)

show ldap

clear line

Syntax Description	**clear line**
{[**console *0-0***] |	Clears the console. Console and tty command only available on models with console ports/serial ports.
[vty *<0-15>*] |	Clears vty or tty sessions.

[tty [<*1-x*>]}	Clears tty sessions. Console and tty command only available on models with console ports/serial ports. <1-x> = maximum number of tty ports, (depends on the model)
Command Modes	Perle#clear line

Usage Guidelines

Use this command to clear the console, vty, or tty session. The session is disconnected and all statistics are cleared.

Examples

This example clears vty line 1.

```
Perle#clear line vty 1
[confirm]
[Dec 9 16:14:20 %REQHANDLE-6: Cleared VTY1 session
OK]
```

Related Commands

(config-line)#console

(config-line)#tty and #usb

clear lldp

Syntax Description	**clear lldp**
{counters | table}	Clears LLDP counters or table.
Command Modes	Perle#clear lldp

Usage Guidelines

Use this command to clears LLDP counters and table.

Examples

This example clears the LLDP table.

```
Perle#clear lldp table
```

Related Commands

show lldp

lldp

clear logging

Syntax Description	**clear logging**
{logging}	Clears the logging buffer.

Command Modes	Perle#clear logging

Usage Guidelines

Use this command to clear logging buffer.

Examples

This example clears the logging buffer.

```
Perle#clear logging
Clear logging buffer[confirm]
```

Related Commands

show logging

clear radius

Syntax Description	**clear radius**
{**radius statistics**}	Clears RADIUS statistics.
Command Modes	Perle#clear radius

Usage Guidelines

Use this command to clear RADIUS statistics.

Examples

This example clears RADIUS statistics.

```
Perle#clear radius statistics
```

Related Commands

radius

radius-server

(config-radius-server)

ip radius

clear tacacs

Syntax Description	**clear tacacs**
{**tacacs statistics**}	Clears TACACS+ statistics.
Command Modes	Perle#clear tacacs

Usage Guidelines

Use this command to clear TACACS+ statistics.

Examples

This example clears TACACS+ statistical information.

```
Perle#clear tacacs statistics
```

Related Commands

tacacs

tacacs-server

ip tacacs

(config-tacacs-server)

clock

Use the no form of this command to negate a command or set to defaults.

Syntax Description	clock
{**set hh:mm:ss | 1-31 | month | 2001-2037**}	Configure the current time and date. hh:mm:ss (hour, mins, secs) Day of the month 1-31 Month is ● January ● February ● March, ● April ● May ● June ● July ● August ● September ● November, ● December Year is 2001-2037
Command Modes	Perle#clock

Usage Guidelines

Use this command to configure the clock.

Examples

This example configures the clock to 5 hours off from UTC.

```
Perle#clock set 12:30:10 28 jan 2020
```

Related Commands

show clock

configure

Syntax Description	configure
{**[confirm] |**	Cancels the revert timer.
[revert now | timer <*1-120* > | idle <*1-120*>] |	Configure the parameters for reverting this config using the rollback feature.
[terminal lock | revert timer <*1-120*> | idle <*1-120*>]}	Locks configuration mode. Revert timer.
Command Modes	Perle#configure

Usage Guidelines

Use this command to change from privileged level mode to configuration mode.

This command is also used to configure the parameters for the rollback and terminal lock features.

Examples

This example changes the user from privileged level mode to terminal configuration mode.

```
Perle#configure
Configuring from terminal, memory, or network [terminal]?
Perle(config)#
```

Related Commands

(config-archive)#

archive

container (OCI)

Syntax Description	container
[connect <*WORD*>] |	Container instance name. You must have a valid image loaded in your container in order to connect. To escape container instance type <CTRL>-p <CTRL>-q.
[exec <*WORD*> <*CMDLINE*> <*WORD*>] |	Executes the given command and arguments then redirects the output to your CLI screen. <WORD>–container name <CMDLINE>–command line to execute
[export-changes <*WORD*> flash:<*WORD*>] |	Export changes made in a container from the base container. Filename will normally end with a “tar.gz” because it will be a compressed tar file, although this is not required. Export-changes must be based on the “same” container image(such as alpine to alpine, not alpine to ubuntu).

[image [add *<WORD>* *<WORD>* | load-from *flash:*] | delete *<WORD>* | update **filename *<WORD>* *<WORD>*** **|**	Pull the specified image for a container or load a tar image from our flash: volume. If no tag is specified then the tag of latest will be used. **Add**–container image path and name container image tag or digest load-from–flash: **Delete**–image name (tag can be included) **Update**–container image path and name container image tag or digest
Command Modes	Perle#container

Usage Guidelines

Use this command to manage Open Container Initiative (OCI) containers images.

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

Your IOLAN allow you to deploy and run Open Containers Initiative (OCI) compatible containers from both public and private container registries, such as Open Containers, GitHub and Docker Hub. Your IOLAN supports the following OCI container specifications:

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

Examples

This example shows you how to add an image to your container, then connect to that container.

```
Perle#container image add alpine
Pulling from library/alpine
Digest:sha256:bc41182d7ef5ffc53a40b044e725193bc10142a1243f395ee852a8d9
Status: Image is up to date for alpine:latest
#(config) container network test-network
(config-container-net)#network-interface bvi 1
#(config) container name test-container
#config) container network test-network
(config-container)#image alpine
#container restart test-container
#container connect test-container
/#
```

Related Commands

show container (OCI)

show container-management (OCI)

copy

Syntax Description	copy

Copies from a file from one location to another.

[flash:*perle-image-name.img*] |
[ftp://*[[username:password]@location]/directory]/perle-image-name.img*] | [http://*[[username:password]@][hostname* | *host-ip [directory] /perle-image-name.img*] |
[https://*[[username:password]@][hostname* | *host-ip [directory] /perle-image-name.img*]
[nvram: <*filename*>] |
[running-config <*filename*>] |
[scp://*[[username:password@location]/directory]/perle-image-name.img*] |
[sftp://*[[//username:password]@location]/directory]/perle-image-name.img*] |
[ssd: <*filename*>] |
[tftp:*[[//location]/directory]/perle-image-name.img*] |
[usb: <*1-8*> filename>]}

Command Modes	Perle#copy

Usage Guidelines

Use this command to copy a file from one location to another.

Examples

This example copies a file from the flash: directory to a TFTP server with an IPv4 address of 172.16.4.90.

```
Perle#copy flash:running-config-save tftp:
Address or name of remote host[ ]?172.16.4.90
Destination filename [ ]?backup-running-config<cr>
4922 bytes copied in 0.013 seconds
```

Related Commands

boot
delete
pwd
mkdir
more
cd
rename

debug

Use the no form of this command to negate this command.

Syntax Description	debug
{**[alarmmgr] |**	Starts alarm manager debug logging

[all] |	Starts all debugging logging. Setting all debug On can seriously effect the speed of your IOLAN.
[bgp events | filters | fsm | keepalives | messages | rib | updates] |	Starts debug BGP messages.
[bridge spanning-tree packet] |	Starts debug spanning-tree packets.
[clpd] |	Starts debug clpd messages.
[container-management] |	Starts debug for container management.
[dialer] |	Starts debug Dial on Demand messages.
[dot1x-authenticator] |	Starts debug dot1x authenticator mode messages.
[dot1x-supplicant] |	Starts debug for dot1x supplicant mode messages.
[drmgrd] |	Starts debug device remote manager daemon messages.
[email] |	Starts debug email messages.
init |	Starts debug init messages.
[ip dhcp client | relay-agent | server] |	Starts debug dhcp client, relay agent and server messages.
[ip ospf events | ism | lsa | nsm | nssa | packets | rib | rip events | packets | rib] |	Starts debug OSPF messages.
[ip rip events | packets | rib] |	Starts debug RIP messages.
[ipsec] |	Starts debug IPsec messages.
[kernel] |	Starts debug kernel messages.
[lldp] |	Starts debug for LLDP messages
[logging] |	Starts debug logging messages.
[ntp] |	Starts debug NTP messages.
[rest-api] |	Starts debug RESTful-api logging.
[snmp] |	Starts debug SNMP messages.
[trapmgr] |	Starts debug trapmgr messages.
[tty] |	Starts debug tty messages.

[vrrp] |	Starts debug for VRRP messages.
[vty] |	Starts debug for vty device messages.
[wan-highavail] |	Starts High availability and IP health logging.
[wanifmgr] |	Starts WAN Interface Manager messages.
[wireguard]}	Starts debug for Wireguard messages.
Command Default	All debug off
Command Modes	Perle#debug

Usage Guidelines

Use this command to set debug On for features or functions. Setting debug On for all features seriously impacts system performance.

Examples

This example sets debug on for NTP.

```
Perle#debug ntp
```

This example sets debug on for dhcp server.

```
Perle##debug ip dhcp server
```

Related Commands

ping

undebug

delete

Syntax Description	**delete**

{**[flash:*perle-image-name.img*] |**

[ftp://*[[username:password]@location]/directory]/perle-image-name.img*] |

[http://*[[username:password]@][hostname* | *host-ip [directory] /perle-image-name.img*] |

[https://*[[username:password]@][hostname* | *host-ip [directory] /perle-image-name.img*]

[nvram: <*filename*>] |

[running-config <*filename*>] |

[scp://*[[username:password@location]/directory]/perle-image-name.img*] |

[sftp://*[[//username:password]@location]/directory]/perle-image-name.img*] |

[ssd: <*filename*>] |

[tftp:*[[//location]/directory]/perle-image-name.img*] |

[usb: <*1-8*> filename>]}

Command Modes	Perle#delete

Usage Guidelines

Use this command to delete a file on a file system.

Examples

This example deletes backup.config on flash.

```
Perle#delete flash:backup.config
```

Related Commands

boot

delete

pwd

mkdir

more

cd

rename

copy

dir

Syntax Description	**dir**
{**[flash:*perle-image-name.img*] |** **[nvram: <*filename*>] |** **[ssd: <*filename*>] |** **[usb: <*1-8*> <*filename*>]**}	Displays the contents of a file system.
Command Modes	Perle#dir

Usage Guidelines

Use this command to display the contents of a file system.

Examples

```
Perle#dir
 34      -rw-     1992 Mar 25 2019 17:39 -04:00 running-config
39      -rw-     2016 Mar 27 2019 12:35 -04:00 -Mar-27-12-35-22-0
 24      -rw-      896 Jan  4 2001 16:46 -04:00 backup.config
 42      -rw-     2068 Mar 28 2019 15:33 -04:00 -Mar-28-15-33-44-3
 41      -rw-     2047 Mar 27 2019 16:24 -04:00 -Mar-27-16-24-31-2
 40      -rw-     2047 Mar 27 2019 16:24 -04:00 -Mar-27-16-24-26-1
```

Related Commands

boot

delete

pwd

mkdir

cd

copy

disable

Syntax Description	**disable**
Command Modes	Perle#disable

Usage Guidelines

Use this command to leave privileged mode.

Examples

This example sets privileged level to user level.

```
Perle#disable<cr>
Perle>
```

Related Commands

enable

disconnect

Syntax Description	**disconnect**
Command Modes	Perle#disconnect

Usage Guidelines

Use this command to disconnect an active ssh session.

Examples

This example disconnects active ssh session vty 1.

```
Perle#disconnect ssh vty 1
[confirm]
[OK]
```

Related Commands

line

dot1x

Syntax Description	dot1x
[initialize interface ethernet <1-x> . <1-4000>| [sfp <1-x>] |	Devices connected on this Ethernet interface are forced to authenticate. The connection is secured. <1-x> = maximum number of ethernet ports, (depends on the model) SFP values 1-x (depends on the model)
[re-authenticate interface ethernet <1-x>. <1-4000> | [sfp <1-x>] |	Devices connected on this Ethernet interface are forced to re-authenticate. <1-x> = maximum number of ethernet ports, (depends on the model) SFP values 1-x (depends on the model)
[test interface ethernet <1-x>. <1-4000> | [sfp <1-x>]}	Run a 802.1x readiness test to detect any 802.1x clients that are EAPoL capable. <1-x> = maximum number of ethernet ports, (depends on the model) SFP values 1-x

Command Modes Perle#dot1x

Usage Guidelines

Use this command to initialize, re-authenticate, and test connected dot1x devices.

Examples

This example forces devices on Ethernet interface 1to re-authenticate.

```
Perle>#enable
Perle#dot1x re-authenticate interface eth 1
```

This example tests for EAPol capable devices.

```
Perle>#enable
Perle#dot1x test eapol-capable interface eth
```

```
Perle#show logging
*Oct 18 02:41:15 %PORT-AUTH-6: eth2: STA 00:13:20:92:29:82 IEEE 802.1X:
INFO_EAPOL_PING_RESPONSE: The interface Ethernet1 has an 802.1x capable
client with MAC (00.13.20.92.29.82)
 *Oct 18 01 02:41:15 %PORT-AUTH-6: eth2: STA 00:16:d3:2f:62:bb IEEE 802.1X:
INFO_EAPOL_PING_RESPONSE: The interface Ethernet1 has an 802.1x capable
client with MAC (00.16.d3.2f.62.bb)
```

Related Commands

dot1x

show eap

exit

Syntax Description	exit
Command Modes	Perle#exit

Usage Guidelines

Use this command to exit from EXEC mode.

Related Commands

disable

kill

Syntax Description	kill
{[line tty *<1-x>* |	Only available on models with serial ports. Resets the tty device. <1-x> = maximum number of ethernet ports, (depends on the model)
[usb *<1-8>*]}	Resets the USB port.
Command Modes	Perle#kill

Usage Guidelines

Only available on models with serial ports.

Use this command to kill a serial line session.

Killing a line resets that serial line and loads any newly configured parameters.

Examples

This example resets (kills) the line for tty 1. Any users connected are disconnected.

```
Perle#kill line tty 1
```

Related Commands

line

line-attach

Syntax Description	line-attach

{**tty** *<1-x> <WORD>***usb** *<1-x>*}	Only available on models with serial ports. Displays available serial ports configured for ssh or telnet protocol. If the user logs in, line access privileges are based on this authentication not the original authentication request. *<WORD>*SSH user name is optional. If it is not entered, the username which logged into the IOLAN's main session are used. <1-x> = maximum number of serial ports, (depends on the model)
usb *<1-8>*}	Resets the USB port.
Command Modes	Perle#line-attach

Usage Guidelines

Use this command to connect to serial ports configured as Console Management ports. The available ports for both Telnet and SSH are displayed.

Examples

This example allows a user to connect to serial port 1using the SSH protocol and ssh user sshlyn.

```
Perle#line-attach tty 1 sshlyn
```

Related Command

(config-line)#tty and #usb

logout

Syntax Description	**logout**
{**logout**}	Logs you out of your IOLAN.
Command Modes	Perle#logout

Usage Guidelines

Use this command to log out of your IOLAN.

mkdir

Syntax Description	**mkdir**
{**mkdir:**}	Makes a directory on the flash file system.
Command Modes	Perle#mkdir

Usage Guidelines

Use this command to make a new directory on the flash file system.

Examples

This example makes a directory under the flash file system.

```
Perle>#enable<cr>
Perle#mkdir flash:testing<cr>
Perle#dir
Directory of flash:
130307    drwx      4096 Jan 2 2019 19:58 -05:00 testdir
130306    -rw-     1508 Jan 2 2019 17:46 -05:00 test-config
130308    drwx      4096 Jan 3 2019 18:49 -05:00 testing
```

Related Commands

delete

pwd

mkdir

more

cd

boot

more

Syntax Description	**more**
{/ascii] | [binary] | [flash:*perle-image-name.img*] | [nvram: <*filename*>] | [ssd: <*filename*>] | [usb: <*1-8*> filename>]}	Displays the contents of a file system.
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#more

Usage Guidelines

Use the more command to display a file contents. Specify whether to show the contents in ASCII or binary format.

Output modifiers (Pipe redirect)—allows you to pipe the output to the redirect options as specified.

Examples

This example views the file contents of nvram.

```
Perle#more nvram:no-default-config
```

password

Syntax Description	password
{**password**}	Changes password for current logged in user
Command Modes	Perle#password

Usage Guidelines

Use this command to change the password for the current user.

Examples

This example changes the password for the current logged in user.

```
Perle#password

Password must be less than 128 characters long
May not use 5 previous passwords
Enter Old Password:
Enter New Password:
Re-Enter Password:
Password Changed Successfully
```

ping

Syntax Description	ping
{**[*<WORD>*** **[data *<HEX DIGITS>*]** | **[repeat *<1-2147483647>*]** | **[size *<36-18024>*]**}	Host name must be predefined in the host table. Data hex pattern is from 1 to 32 hex characters. Repeat count is from 1–2147483647. Datagram size is from 36–18024.
Command Modes	Perle#ping

Usage Guidelines

Use this command to ping a remote host.

Examples

This example pings a host with an ip address of 172.16.113.44 repeating the ping request 10 times.

```
Perle#ping 172.16.113.44 repeat 10
```

This example pings a host with an ip address of 172.16.113.44 with hex data pattern of f1f1f1f1f1.

```
Perle#ping perlehost data f1f1f1f1f1
```

This example pings a host with an ip address of 172.16.113.44 with a data packet size of 4o bytes.

```
Perle#ping perlehost size 40
```

Related Commands

undebug

pwd

Syntax Description	**pwd**
Command Modes	Perle#pwd

Usage Guidelines

Use this command to display your current file system.

Examples

This command displays the file system you are in.

```
Perle#cd nvram:
Perle#pwd<cr>
#nvram:
```

Related Commands

copy

boot

delete

pwd

mkdir

more

cd

rename

release

See ***release***

reload

Syntax Description	reload
{[at *hh:mm*] |	Configure **at**—the time in hours and minutes when to reload the firmware on the IOLAN.
[cancel] |	Configure **cancel**—any pending reload commands.
[in *mmm* | [*hh:mm*]}	Configure **in**—minutes 1-999 or hours minutes when to reload the firmware on the IOLAN.
Command Modes	Perle#reload

Usage Guidelines

Use this command to reload the IOLAN ‘s firmware. The IOLAN powers off and then reboots. Any configuration not copied from running-config to startup-config is lost.

Examples

Reloads the firmware on the IOLAN in 10 hours and 20 mins.

```
Perle#reload 10:20
```

Cancels the previous reload command.

```
Perle#reload cancel
*****
***** ----SHUTDOWN ABORTED ---
******
```

Related Commands

show reload

Note: Before reloading the IOLAN copy running config to startup config to save any changes that you want permanently saved.

rename

Syntax Description	rename
{[flash:*perle-image-name.img*] | [nvram: *<filename>*] | [ssd: *<filename>*] | [usb: *<1-8> <filename>*]} Renames the file.	
Command Modes	Perle#rename

Usage Guidelines

Use this command to rename a file on flash or nvram.

Examples

This example rename a file on flash from testdir to newdir.

```
Perle#rename flash:testdir flash:backup
Destination file name[backup]?
```

Related Commands

delete

pwd

mkdir

more

cd

rename

boot

renew

See ***renew***

reset

Syntax Description	reset
{**[factory] |**	Resets the IOLAN to factory default— removing all configuration files, certificates and keys.
[remove-container-management-images | clear-all | erase-vm-parition]}	Remove container management images. Clear all container and Virtual Machine partitions. Erase Virtual Machine partition.
Command Modes	Perle#reset

Usage Guidelines

Use this command to set the IOLAN to factory defaults, as well as, remove container images, all container and virtual Machine partitions or erase Virtual Machine partitions.

Related Commands

boot

rmdir

Syntax Description	rmdir

{**flash:** ***<WORD>*** ***<WORD>***}	Removes the directory on flash.
Command Modes	Perle#rmdir

Usage Guidelines

Use this command to remove a file on flash.

Examples

This example removes a directoy on flash.

```
#rmdir flash:testit
Remove Directory name [testit]?
```

Related Commands

boot

delete

pwd

renew

mkdir

serialt

Syntax Description	**serialt**
{**[*<WORD>*** **#[mask] [...] [-full] [-size=# [-show]**}	Only available on models with serial ports. Takes a serial line trace.
Command Modes	Perle#serialt

Usage Guidelines

Use this command to capture data on the serial line.

Examples

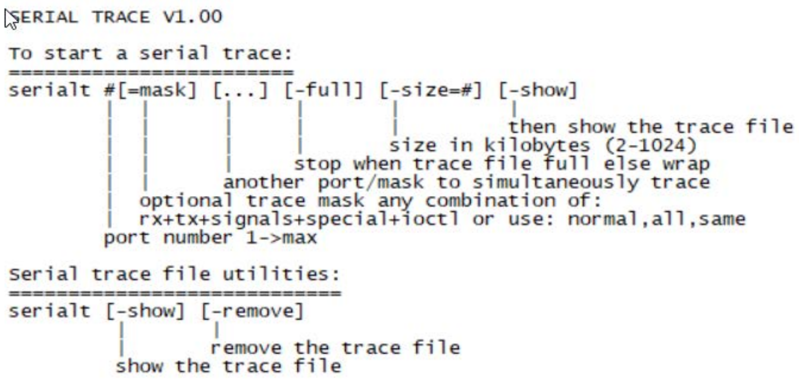
This example captures all data on serial port 1 and displays it to the screen.

```
Perle#serialt 1 -show
Tracing port 1=rx+tx+signals+special

To stop the trace press Ctrl-C
9
Use the "Space Bar" and the keys 1,2,3,4 to control the scrolling speed.
Please press the "Space Bar" to continue..............

Use the "Space Bar" and the keys 1,2,3,4 to control the scrolling speed.
Please press the "Space Bar" to continue..............

Decode Complete... 0 entries processed
```



```
SERIAL TRACE V1.00

To start a serial trace:
========================
serialt #[=mask] [...] [-full] [-size=#] [-show]
        |  |      |     |       |         |
        |  |      |     |       |         then show the trace file
        |  |      |     |       size in kilobytes (2-1024)
        |  |      |     stop when trace file full else wrap
        |  |      another port/mask to simultaneously trace
        |  optional trace mask any combination of:
        |  rx+tx+signals+special+ioctl or use: normal,all,same
        port number 1->max

Serial trace file utilities:
============================
serialt [-show] [-remove]
         |       |
         |       remove the trace file
         show the trace file
```

Related Commands

undebug

show aaa

Syntax Description	**show aaa**
{**[aaa local user lockout] |**	Displays users locked-out of the IOLAN.
[*filter/redirection options*>]	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show aaa

Usage Guidelines

Use this command to display the current locked-out users on the IOLAN.

Output modifiers (Pipe redirect)—allows you to pipe the output to the redirect options as specified.

Examples

This example shows you the current locked out users on the IOLAN.

```
Perle#show aaa local user lockout
Locked-out users: Lyn
```

Related Commands

aaa

show alarm

See ***show alarm***

show archive

Syntax Description	show archive
{[config rollback timer] |	Displays configuration rollback and timer information.
[update-sw] |	Displays the Check Software update option.
[*<filter/redirection options>*]}	Output modifiers see *Show Command Filtering and Redirection*
Command Modes	Perle#show archive

Usage Guidelines

Use this command to display config rollback and the update feature.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays the config for the rollback feature.

```
Perle#show archive
The maximum archive configurations allowed is 14.
There are currently 9 archive configurations saved.
The next archive file is named flash:-<timestamp>-9
Archive #  Name
Archive #  Name
  1       flash:-May-19-14-14-16-0
  2       flash:-May-19-14-17-50-1
  3       flash:-May-1914-19-00-2 4       flash:-May-19-14-19-14-3
  4       flash:-May-19-14-19-14-3
  5       flash:-May-19-14-20-55-4
  6       flash:-May-19-14-24-31-5
  7       flash:-May-19-15-05-37-6
  8       flash:-May-19-03-37-55-7
  9       flash:-May-19-03-38-10-8 <- Most Recent
```

Related Commands

archive

show arp

See *show arp*

show bgp

Syntax Description	show bgp
{[bgp community] |	Displays the routes matching the communities.

<table>
<tr><td><b>[community-list <i>&lt;1-500 &gt;</i> | <i>&lt;WORD&gt;</i> exact-match] |</b></td><td>Displays the routes matching the community list.</td></tr>
<tr><td><b>[filter-list <i>&lt;WORD&gt;</i>] |</b></td><td>Displays the routes conforming to the filter list.</td></tr>
<tr><td><b>[memory] |</b></td><td>Displays Global BGP memory statistics.</td></tr>
<tr><td><b>[neighbors <i>&lt;A.B.C.D&gt;</i> | <i>&lt;X:X::X:X&gt;</i>] |</b></td><td>Detailed list for TCP and BGP neighbor connections.</td></tr>
<tr><td><b>[prefix-list <i>&lt;WORD&gt;</i>] |</b></td><td>Displays the routes matching the prefix-list.</td></tr>
<tr><td><b>[regexp <i>&lt;LINE&gt;</i>] |</b></td><td>Displays the routes matching the AS path regular expression.</td></tr>
<tr><td><b>[route-map <i>&lt;LINE&gt;</i>] |</b></td><td>Displays the routes matching the route-map.</td></tr>
<tr><td><b>[<i>&lt;filter/redirection options&gt;</i>]</b>}</td><td>Output modifiers see
<b><i>Show Command Filtering and Redirection</i></b></td></tr>
<tr><td><b>Command Modes</b></td><td>Perle#show bgp</td></tr>
</table>

Usage Guidelines

Use this command to show BGP information.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays BGP neighbors.

```
Perle#show bgp neighbors
BGP neighbor is 172.16.39.2, remote AS 65537, local AS 65536, external link
  BGP version 4, remote router ID 172.16.39.2
  BGP state = Established, up for 00:14:28
  Last read 05:39:27, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    4 Byte AS: advertised and received
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
```

```
Message statistics:
   Inq depth is 0
   Outq depth is 0
        Sent       Rcvd
Opens:              1         0
   Notifications:       0         0
   Updates:             1         1
   Keepalives:         16        15
   Route Refresh:       0         0
Route Refresh:      0         0
   Capability:          0         0
   Total:              18        16
Minimum time between advertisement runs is 30 seconds.
....................................................................................................
......................................................................
```

Related Commands

router

show bridge

Syntax Description	**show bridge**
{**[spanning-tree active | bridge | detail | interface ethernet** *<1-x>. <1-4000>* **| [sfp** *<1-x>*] **| [mst** *<WORD>* **configuration | detail | interface ethernet** *<1-x>. <1-4000>*| **[sfp** *<1-x>*] **| root] |**	Shows list of bridges and spanning-tree information. <1-x> = maximum number of ethernet ports, (depends on the model) SFP values 1-x (depends on the model)
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show bridge

Usage Guidelines

Use this command to list bridge and spanning tree information.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays bridge information.

```
Perle##show bridge
```

Related Commands

bridge

show cellular

Syntax Description	show cellular
[cellular interface *<0-0>* **all] |**	Displays all information.
[connection] |	Displays current active connections
[hardware] |	Displays cellular modem information.
[network] |	Displays cellular network information
[profile *<NAME>* |	Displays profile information about the modem.
[radio] |	Displays cellular modem radio information
[security] |	Displays modem security status
[sms-log |	Displays SMS log.
[*<filter/redirection options>***]**}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle>show cellular

Usage Guidelines

Displays information about your cellular connection.
Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified

Examples

This example displays the version of SSL installed on the IOLAN.

```
Perle>show cellular security
Modem Security Information
===========================
Active SIM Slot:    1
SIM Locked:         No
PIN Retry:        0
PUK Retry:          0
SCRC440#
```

Related Commands

crypto

show clock

See ***show clock***

show container (OCI)

Syntax Description	**show container**
{**[<*WORD*>] |**	Show container instance name.
[images] |	Show container image information.
[log <*WORD*>] |	Show container log.
[network <*WORD*>] |	Show network container information.
[name] |	Show name of container.
[stats] |	Show running container status.
[storage-info] |	Displays container storage information.
{**[<*filter/redirection options*>]**}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show container

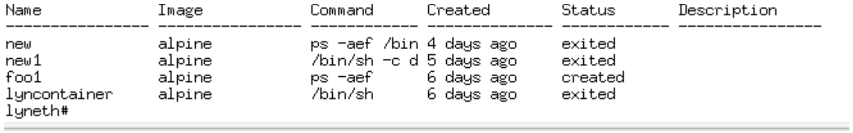
Usage Guidelines

Use this command to display OCI container information.

Examples

This example displays container information.

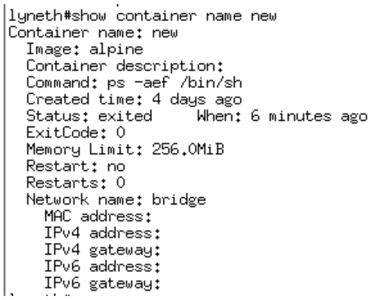
```
Perle#show container <cr>
```



```
Name             Image            Command      Created        Status       Description
---------------- ---------------- ------------ -------------- ------------ ----------------

new              alpine           ps -aef /bin 4 days ago     exited
new1             alpine           /bin/sh -c d 5 days ago     exited
foo1             alpine           ps -aef      6 days ago     created
lyncontainer     alpine           /bin/sh      6 days ago     exited
lyneth#
```

#show container name new <cr>



```
lyneth#show container name new
Container name: new
  Image: alpine
  Container description:
  Command: ps -aef /bin/sh
  Created time: 4 days ago
  Status: exited     When: 6 minutes ago
  ExitCode: 0
  Memory Limit: 256.0MiB
  Restart: no
  Restarts: 0
  Network name: bridge
    MAC address:
    IPv4 address:
    IPv4 gateway:
    IPv6 address:
    IPv6 gateway:
```

Related Commands

show container-management (OCI)

show container-management (OCI)

Syntax Description	**show container**
{[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show container-management

Usage Guidelines

Use this command to display the status of container management.

Examples

This example displays the status of container management.

Perle#show container-management <cr>

Container Management is currently active

Related Commands

show container (OCI)

show debugging

Syntax Description	show debugging
{**[debugging] |**	Displays processes that are in debugging mode.
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show debugging

Usage Guidelines

Use this command to show which functions or commands have debug enabled.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays which processes are set to debug.

```
Perle#show debugging
BGP events debugging is on
```

show crypto

See ***show crypto***

show dhcp

Syntax Description	show dhcp
{**[lease] |**	Displays current devices with leases.
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show dhcp lease

Usage Guidelines

Use this command to display all client dhcp leases with configured options.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays all dhcp leases.

```
Perle#show dhcp lease
dhcp-assigned-address 172.17.121.182
option subnet mask 255.255.0.0
option dhcp-lease time 86400 seconds
option dhcp-server-identifier 172.17.3.13
renew Mon Jan 01 08:44:00 EST 2021
rebind Mon Jan 01 19:02:16 EST 2021
expire Mon Jan 01 22:02:16 EST 2021
```

Related Commands

show ip dhcp

show dot1x

See ***show dot1x***

show eap

See ***show eap***

show eee

Syntax Description	**show eee**
{**[eee capabilities interface ethernet** *<1-x>* **.** *<1-4000>* **| [sfp** *<1-x>***] |**	Displays whether the remote Ethernet interface is capable of Energy Efficient Ethernet (EEE).
[status interface ethernet *<1-x>* **.** *<1-4000>* **| [sfp** *<1-x>***] |**	Displays the current status. • Disagree—the remote interface cannot negotiate EEE • Link down—the remote interface is not connected • Operational—both sides have agreed on EEE capabilities • Disabled—EEE is disabled on this Ethernet interface <1-x> = maximum number of ethernet ports, (depends on the model) SFP values 1-x (depends on the model)
[*<filter/redirection options>***]**}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show eee

Usage Guidelines

Use this command to display Ethernet EEE port capabilities.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays EEE capabilities on the Ethernet ports.

```
Perle#show eee capabilities
```

show email

Syntax Description	show email
{**[email] |**	Displays email configuration.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show email

Usage Guidelines

Use this command to display configured email parameters.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays email configuration.

```
Perle#show email
Email: Enabled
SMTP Server: 172.217.214.109:587
From: tfelton@gmail.com
Encryption: tls
Username: tfelton@gmail.com
Password: OHJJdoll564ggbTzMI
Validate Certificate: Disabled
Email Notifications:
Recipient                Notifications
Subject
tfelton@perle.com            alarms authentication entity envmon snmp ipsec
Tom’s events from IOLAN
```

Related Commands

email

show environment

See *show environment*

show facility-alarm

See *show facility-alarm*

show flash:

See *show flash:*

show format

Syntax Description	show format
[<*filter/redirection options*>]}	Output modifiers see *Show Command Filtering and Redirection*
Command Modes	Perle#show format

Usage Guidelines

Use this command to list supported CLI show format commands.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays the supported CLI show format commands.

```
Perle#show format
show aaa local user lockout
show alarm profile
show alarm profile %s
show alarm settings
show alarm settings enabled
show archive
show archive config rollback timer
show archive update-sw
show arps
show bgp memory
..........
```

show hosts

See *show hosts*

show interfaces

Syntax Description	show interfaces
{[bvi <*1-9999*>] |	Displays Bridge-Group Virtual interfaces.
[dialer <*0-15*>] |	Displays Dialer interfaces.

[dot11radio *<0-4>* | counters | descriptions | stats | summary] |	Displays IEEE 802.3z interfaces.
[ethernet *<1-x>* | [vrrp *<1-255>*] [description *<WORD>*] |	Displays Ethernet interfaces. <1-x> = maximum number of ethernet ports, (depends on the model)
[loopback counters | description | stats | summary] |	Displays loopback interface.
[openvpn-tunnel *<0-999>*] |	Displays OpenVPN interfaces.
[sfp *<1-x>*] |	Displays IEEE 802.3z SFP interfaces. SFP values 1-x (depends on the model)
[tunnel *<0-999*] |	Displays tunnels.
[counters] |	Displays counters for all interfaces.
[description] |	Displays descriptions for all interfaces.
[stats] |	Displays stats for all interfaces.
[summary] |	Displays summary for all interfaces.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show interfaces

Usage Guidelines

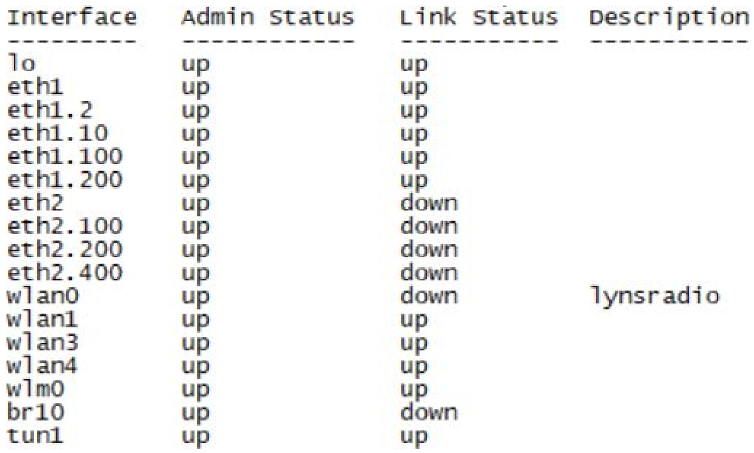
Use this command to display interface details, including admin statuses, and link statuses.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example shows interface descriptions.

Perle#show interfaces description



```
Interface     Admin Status     Link Status    Description
---------     ------------     -----------    -----------
lo            up               up
eth1          up               up
eth1.2        up               up
eth1.10       up               up
eth1.100      up               up
eth1.200      up               up
eth2          up               down
eth2.100      up               down
eth2.200      up               down
eth2.400      up               down
wlan0         up               down           lynsradio
wlan1         up               up
wlan3         up               up
wlan4         up               up
wlm0          up               up
br10          up               down
tun1          up               up
```

Related Commands

(config-if)#

(config-if)#cellular

(config-if-ethernet)#

(config-if)#tunnel

(config-if)#openvpn-tunnel

show ip access-lists

Syntax Description	**show ip access-lists**
{**[extended** *<100-199> <2000-2699>* **| standard** *<1-99> <2000-2699>*] |	Displays Extended and standard IP access lists.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show ip access-lists

Usage Guidelines

Use this command to display configured access lists.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

Perle#show ip access-lists
Extended IP access list 100
10 permit any any

Related Commands

ip **access-list**

show ip alg

Syntax Description	**show ip alg**
{**[table]** |	Displays ALG entries.
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show ip alg table

Usage Guidelines

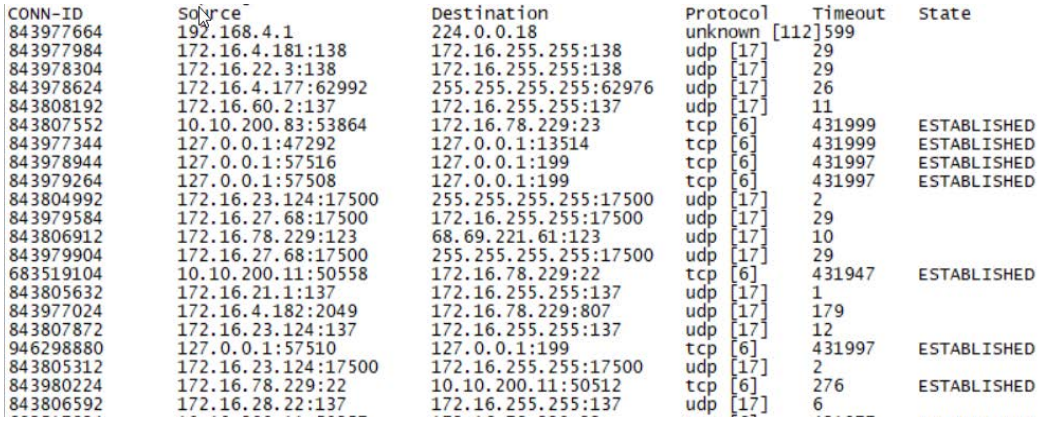
Use this command to display Application Level Gateway (ALG) entries.

Output modifiers (Pipe redirect)—allows you to pipe the output to the redirect options as specified.

Examples

This example displays ip alg table information.

Perle#show ip alg table



```
CONN-ID        Source           Destination            Protocol    Timeout   State
843977664      192.168.4.1      224.0.0.18             unknown [112]599
843977984      172.16.4.181:138     172.16.255.255:138     udp [17]     29
843978304      172.16.22.3:138      172.16.255.255:138     udp [17]     29
843978624      172.16.4.177:62992   255.255.255.255:62976  udp [17]     26
843808192      172.16.60.2:137      172.16.255.255:137     udp [17]     11
843807552      10.10.200.83:53864   172.16.78.229:23       tcp [6]      431999    ESTABLISHED
843977344      127.0.0.1:47292      127.0.0.1:13514        tcp [6]      431999    ESTABLISHED
843978944      127.0.0.1:57516      127.0.0.1:199          tcp [6]      431997    ESTABLISHED
843979264      127.0.0.1:57508      127.0.0.1:199          tcp [6]      431997    ESTABLISHED
843804992      172.16.23.124:17500  255.255.255.255:17500  udp [17]     2
843979584      172.16.27.68:17500   172.16.255.255:17500   udp [17]     29
843806912      172.16.78.229:123    68.69.221.61:123       udp [17]     10
843979904      172.16.27.68:17500   255.255.255.255:17500  udp [17]     29
683519104      10.10.200.11:50558   172.16.78.229:22       tcp [6]      431947    ESTABLISHED
843805632      172.16.21.1:137      172.16.255.255:137     udp [17]     1
843977024      172.16.4.182:2049    172.16.78.229:807      udp [17]     179
843807872      172.16.23.124:137    172.16.255.255:137     udp [17]     12
946298880      127.0.0.1:57510      127.0.0.1:199          tcp [6]      431997    ESTABLISHED
843805312      172.16.23.124:17500  172.16.255.255:17500   udp [17]     2
843980224      172.16.78.229:22     10.10.200.11:50512     tcp [6]      276       ESTABLISHED
843806592      172.16.28.22:137     172.16.255.255:137     udp [17]     6
```

show ip arp

Syntax Description	**show ip arp**
{**[<*A.B.C.D*>]** |	Displays the ARP entry for the specified IPv4 address.
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show ip arp

Usage Guidelines

Use this command to display ARP table details.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

```
Perle#show ip arp
Address             HWtype         HWaddress          Flags Mask     Iface
172.16.113.20        ether        78:2B:cb:a5:b4:0c   CM              eth1
```

show ip as-path-access-list

Syntax Description	show ip as-path-access-list
{[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show ip as-path-access-list

Usage Guidelines

Use this command to show as-path access list.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays as-path access list.BGP neighbors.

```
Perle#show as-path-access-list
AS path access JoeAS-Path
permit def
deny abc
```

Related Commands

ip as-path

show ip bgp

Syntax Description	show ip bgp
{[*<A.B.C.D>/nn <A.B.C.D>]* |	Displays BGP network routing table.
[cidr-only] |	Displays only routes with non-natural netmasks.
[community] |	Displays routes matching the communities.
[community-info] |	Displays all BGP community information.

[community-list *<1-500>* | *<WORD>* exact-match] |	Displays routes matching the community list.
[dampened-paths] |	Displays paths suppressed due to dampening.
[filter-list *<WORD>*] |	Displays routes conforming to the filter list.
[flap-statistics] |	Displays flap statistics of routes.
[ipv4 unicast] |	Displays address family.
[neighbours *<A.B.C.D>* *<X:X:X:X::X>* | advertised-routes | dampened-routes | flap-statistics | prefix-count | [received prefix-filter] | received-routers | routes] |	Displays detailed information on TCP and BGP neighbor connections.
[paths] |	Displays path information.
[prefix-list *<WORD>*] |	Displays routes matching the prefix list.
[regexp *<LINE>*] |	Displays routes matching the AS path regular expression.
[route-map *<WORD>*] |	Displays routes matching the route map.
[summary] |	Displays the summary of BGP neighbor statuses.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show ip bgp

Usage Guidelines

Use this command to display BGP information.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays BGP information.

```
Perle#show ip bgp
BGP table version is 0, local router ID is 172.16.113.215
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric          LocPrf             Weight Path
*> 172.16.0.0       0.0.0.0                  1                         32768              i

Total number of prefixes 1
```

Related Commands

clear ip

show ip community-list

Syntax Description	show ip community-list
{[*<filter/redirection options>*]}	Output modifiers see *Show Command Filtering and Redirection*
Command Modes	Perle#show ip community-list

Usage Guidelines

Use this command to display IP community list information.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays the community lists.

```
Perle#show ip community-list
Community (expanded) access list 100
permit 50
```

Related Commands

ip community-list

show ip ddns

See *show ip ddns*

show ip dhcp

See *show ip dhcp*

show ip dns

Syntax Description	show ip dns
[*<filter/redirection options>*]}	Output modifiers see *Show Command Filtering and Redirection*
Command Modes	Perle#show ip dns

Usage Guidelines

Use this command to display IP DNS configuration and information.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays all DNS settings.

```
Perle# show ip dns
IP DNS
======
DNS Lookup Enabled
Listen Addresses:
192.168.0.1
Cache Size          10000
Ignore Host File     Off
Negative TTL         3600
No Name Servers Configured
```

Related Commands

ip dns

show ip extcommunity-list

Syntax Description	show ip extcommunity-list
[*<filter/redirection options>*]}	Output modifiers see *Show Command Filtering and Redirection*
Command Modes	Perle#show ip extcommunity-list

Usage Guidelines

Use this command to display configured ip extcommunity lists.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays extcommunity lists.

```
Perle#show ip extcommunity-list
Extended community standard list 99
denyso0:0:1:30
```

Related Commands

ip community-list

show ip firewall

Syntax Description	show ip firewall
{[*<NAME>*]}	Displays firewall name.

[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show ip firewall

Usage Guidelines

Use this command to display IP firewall configuration.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays active firewalls.

```
Perle#show ip firewall
Active on
Rule  Packets Bytes  Action   Proto   Source      Destination  Rule Specs
-----  -------  -------  -------  -------  -----------     -----------------  ---------------
10     0      0      accept    ip        0.0.0.0/0        0.0.0.0/0
/* firewall1-10 */
10000  0      0      drop      ip        0.0.0.0/0        0.0.0.0/0
/* firewall1-10000 default-action drop */
```

Related Commands

ip firewall

clear ip

show ip health

Syntax Description	show ip health
{[interfaces | profiles | status] |	Displays health profile configuration.
[profiles] |	Displays health profile configuration.
[status] |	Displays health interfaces runtime status.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show ip health

Usage Guidelines

Use this command to display health status for interfaces.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays health information for configured interfaces.

```
Perle#show ip health
IP Health Profiles and Tests Configuration:
==========================================
Profile Name   : health-pro
  Failure-count: 5
  Success-count: 5
    Test 10: Type: PING       Response Timeout:   1
Target: 8.8.8.8

Profile Name   : labhealth
  Failure-count: 1
  Success-count: 1

Profile Name   : testit
  Failure-count: 1
  Success-count: 1
IP Interface Health-Profile Configuration:
=========================================
eth1              health-pro

IP Interfaces Health Status:
===========================

Interface:  eth1
  Status:  failed
  Last Status Change:  Sat Feb 20 08:05:12 2021
  -Test:  ping Target: 8.8.8.8
    Last Interface Success:  n/a
    Last Interface Failure:  0s
    # Interface Failure(s):  20178
```

Related Commands

(config-if)#cellular

(config-if)#

(config-if-ethernet)#

(config-if)#openvpn-tunnel

(config-if)#tunnel

show ip host-group

Syntax Description	**show ip host-group**
{[<*WORD*>] |	Displays IP host groups.

[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show ip host-group

Usage Guidelines

Use this command to display IP host groups.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays host group tables.

```
Perle#show ip host-group test
Host list:
  172.16.77.88
  1:2:3:4::5
```

Related Commands

ip host-group

show ip http

Syntax Description	**show ip http**
{**[server status]** |	Displays HTTP server status.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show ip http

Usage Guidelines

Use this command to show status of HTTP server.

Output modifiers (Pipe redirect)—allows you to pipe the output to the redirect options as specified.

Examples

Shows status of HTTP server.

```
Perle#show ip http
Http server status: Enabled
HTTP server port : 80
User session idle timeout: 1440 seconds
HTTP secure server status: Enabled
HTTP secure server port: 443
```

Related Commands

ip http

show ip interface

See ***show ip interface***

show ip nat

Syntax Description	**show ip nat**
{**[statistics] |**	Displays the Network Address Translation (NAT) source statistics table.
[translations] |	Displays the pre-nat and post-nat translations. table.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***

Command Modes	Perle#show ip nat

Usage Guidelines

Use this command to display the IOLAN's Network Address Translation Table (NAT) statistics and translations.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Example

This example displays IP NAT translations.

Perle#show ip nat translations

```
NAT Source Translations
Pre-NAT              Post-NAT             Prot     Timeout
192.168.30.1         10.10.200.229        tcp      431936
192.168.30.1         10.10.200.229        tcp      431936
192.168.30.1         10.10.200.229        tcp      431936
192.168.30.1         10.10.200.229        tcp      431935
192.168.30.1         10.10.200.229        tcp      431935
192.168.30.1         10.10.200.229        tcp      62
192.168.30.1         10.10.200.229        tcp      61
192.168.30.1         10.10.200.229        tcp      431995
192.168.30.1         10.10.200.229        tcp      431995
192.168.30.1         10.10.200.229        tcp      431995

NAT Destination Translations
Pre-NAT              Post-NAT             Prot     Timeout
10.10.200.229:2222   192.168.20.2:22      tcp      431825
```

Related Commands

ip nat

show ip ospf

Syntax Description	show ip ospf
{**[border-routers] |**	Displays border and boundary router information.
[database] |	Displays database summary.
[interface] |	Displays interface information.
[neighbor] |	Displays neighbor list.
[neighbor] |	Displays OSFP routing table.
[<*filter/redirection options*>]}	Output modifiers see *Show Command Filtering and Redirection*
Command Modes	Perle#show ip ospf

Usage Guidelines

Use this command to show the IOLAN‘s OSPF routing processes.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

```
Perle#show ip ospf
OSPF Routing Process, Router ID: 172.16.39.2
Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is disabled
Opaque Capability flag is disabled
Initial SPF scheduling delay 200 millisec(s)
Minimum hold time between consecutive SPFs 1000 millisec(s)
Maximum hold time between consecutive SPFs 10000 millisec(s)
Hold time multiplier is currently 1
SPF algorithm last executed 7m53s ago
SPF timer is inactive
Refresh timer 10 secs
Number of external LSA 0. Checksum Sum 0x00000000
Number of opaque AS LSA 0. Checksum Sum 0x00000000
Number of areas attached to this router: 1
Area ID: 0.0.0.0 (Backbone)
  Number of interfaces in this area: Total: 1, Active: 1
  Number of fully adjacent neighbors in this area: 0
  Area has no authentication
  SPF algorithm executed 1 times
  Number of LSA 1
  Number of router LSA 1. Checksum Sum 0x00001e7a
  Number of network LSA 0. Checksum Sum 0x00000000
  Number of summary LSA 0. Checksum Sum 0x00000000
  Number of ASBR summary LSA 0. Checksum Sum 0x00000000
Number of NSSA LSA 0. Checksum Sum 0x00000000
  Number of opaque link LSA 0. Checksum Sum 0x00000000
  Number of opaque area LSA 0. Checksum Sum 0x00000000
```

Related Commands

router

show ip prefix-list

Syntax Description	**show ip prefix-list**
{[*WORD*] |	Displays prefix list name.
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show ip prefix-list

Usage Guidelines

Use this command to display prefix list table.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example shows the ip prefix list.

```
Perle#show ip prefix-list
ip prefix-list prefix-lab (for lab users)
seq 10 permit 172.17.0.0/16
```

Related Commands

ip prefix-list

show ip rip

Syntax Description	**show ip rip status**
{**[status] |**	Displays RIP information.
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show ip rip status

Usage Guidelines

Use this command to display rip status information.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example shows rip status information.

```
Perle#show ip rip
Routing Protocol is "rip"
Sending updates every 30 seconds with +/-50%, next due in 30 seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribution metric is 1
```

```
Redistributing:
Default version control: send version 2, receive any version
Interface       Send Recv   Key-chain
Routing for Networks:
Routing Information Sources:
Gateway         BadPackets BadRoutes Distance Last Update
Distance: (default is 120)
```

show ip route

Syntax Description	show ip route
{[table *<1-200>*] |	Displays ip routes or route table. Tables must be pre-defined by the user.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show ip route

Usage Guidelines

Use this command to show configured tables for ip routing.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

Shows ip route table entries.

Perle#show ip route

```
table:200
```

Related Commands

ip route

show ip route-policy

Syntax Description	show ip route-policy
{[*<NAME>*] |	Show ip routes or route table. Tables must be pre-defined by the user.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show ip route-policy

Usage Guidelines

Use this command to display configured routing policies.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

Shows ip route policies table.

```
Perle#show ip route-policy
IPv4 Route-policy route1
Active on
Rule   Packets Bytes  Action    Proto     Source          Destination             Rule
                                Specs
-----   ------- ------- -------    -------    --------------       --------------    ---------------
20      0       0       rtable-254 ip         0.0.0.0/0      0.0.0.0/0
                                /* route1-9999 */
10000   0       0        accept     ip         0.0.0.0/0      0.0.0.0/0
                                /* route1-10000 default-action accept */
```

Related Commands

ip route-policy

show ip ssh

Syntax Description	**show ip ssh**
[<*filter/redirection options*>]}	Output modifiers see *Show Command Filtering and Redirection*
Command Modes	Perle#show ip ssh

Usage Guidelines

Shows configuration for ssh.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example shows ip ssh configuration.

```
Perle#show ip ssh
SSH version: 2
SSH server: Enabled
Authentication timeout: 120 seconds
Authentication retries: 3
```

```
SSH public key:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCgAtvWaaM0CeMWoZV1H00sni2J8T
alvSyysQGyBDIOAydaaKv1+s1Imj00FL2Boi3ke/SoKhvuLJQ+bMVFXD7kXw2fk7
Mo8f8Dd/rOuuF4kE6hKV+LLI44kJKwCUC2w2m4L1IH8Zn8HuX89Qcv2oqPUdkBf
1neIU3gc6gN4v1ckC069Tgg9hrhghCiBECCCYxmAJUhIy4dQcPwO1DQ6Acp2p3
W2RYdgUvRAIr8oLiVdrEvT7zZECpYgCMYWmfsTtUhvv8yZpvNAhV9nRm5E93YI
V2J15qImIISGKn0iiLRW42xjQ4MT5XmWdIXj+NpuMIQRtFzyYPkR2H
```

Related Commands

ip ssh

show ipv6

See ***show ipv6***

show ldap

See ***show ldap***

show license

Syntax Description	**show license**
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show license

Usage Guidelines

Use this command to display the GNU license information.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

show line

Syntax Description	**show line**
{**[console *<0-0>*] |**	Only available on models with console ports. Displays configured console parameters.
[tty *<1-x>* [modbus statistics master-tcp | master-udp | slave-tcp | slave-udp] | multihost | packet-forwarding | ppp | rlogin-client | settings | slip | ssh-client | ssl | statistics | telnet-client | udp | vmodem] |	Displays statistics for tty lines. <1-x> = maximum number of tty ports, (depends on the model)

[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	#show line

Usage Guidelines

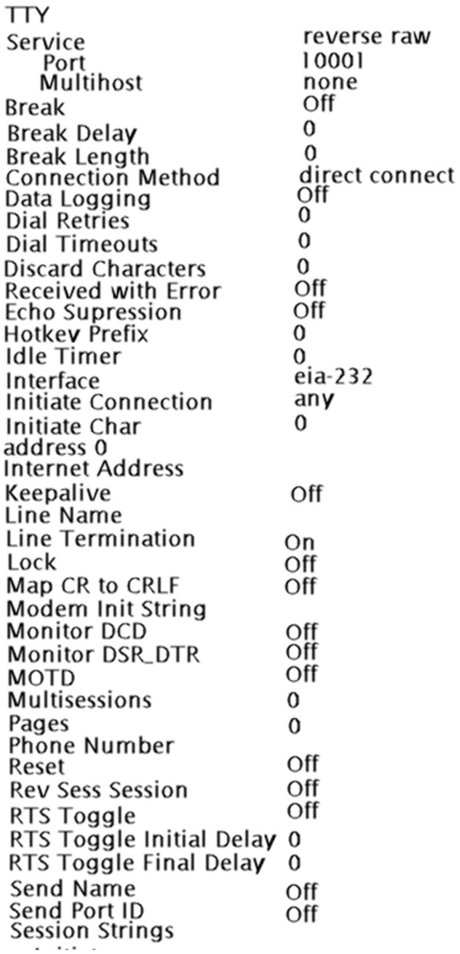
Use this command to display various line related configurations.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

Show line parameters for tty1.

Perle#show line tty 1



```
TTY
Service                      reverse raw
    Port                     10001
    Multihost                none
Break                        Off
Break Delay                  0
Break Length                 0
Connection Method            direct connect
Data Logging                 Off
Dial Retries                 0
Dial Timeouts                0
Discard Characters           0
Received with Error          Off
Echo Supression              Off
Hotkev Prefix                0
Idle Timer                   0
Interface                    eia-232
Initiate Connection          any
Initiate Char                0
address 0
Internet Address
Keepalive                    Off
Line Name
Line Termination             On
Lock                         Off
Map CR to CRLF               Off
Modem Init String
Monitor DCD                  Off
Monitor DSR_DTR              Off
MOTD                         Off
Multisessions                0
Pages                        0
Phone Number
Reset                        Off
Rev Sess Session             Off
RTS Toggle                   Off
RTS Toggle Initial Delay     0
RTS Toggle Final Delay       0
Send Name                    Off
Send Port ID                 Off
Session Strings
```

show lldp

See ***show lldp***

show logging

Syntax Description	**show logging**

[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show logging

Usage Guidelines

Use this command to display the logging buffer. Logging buffer output may be different on some models.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example shows the logging buffer.

```
Perle#show logging
Syslog logging: enabled (764643 messages processed, 0 messages rate-limited, 0
                                    overruns)
   Console logging: level debugging, 71 messages logged
   Monitor logging: level debugging, 71 messages logged
      Logging to:
   Buffer logging: level debugging, 1344 messages logged
   File logging: disabled
   Trap logging: level informational
      Logging Source-Interface:
 Log Buffer (16384 bytes):
 Sep 26 20:51:57 %REQHANDLERD-6: CONSOLE: initializing usb serial console
                                    mode
 Sep 26 20:52:02 %IPSEC_STARTER-6: Starting strongSwan 5.6.2 IPsec [starter]...
 Sep 26 20:52:02 %IPSEC_STARTER-6: charon is already running (/var/run/
                                    charon.pid exists) -- skipping daemon start
```

Related Commands

logging

show mab

See

show mac

See ***show mac***

show management-access

Syntax Description	**show management-access**
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show management-access

Usage Guidelines

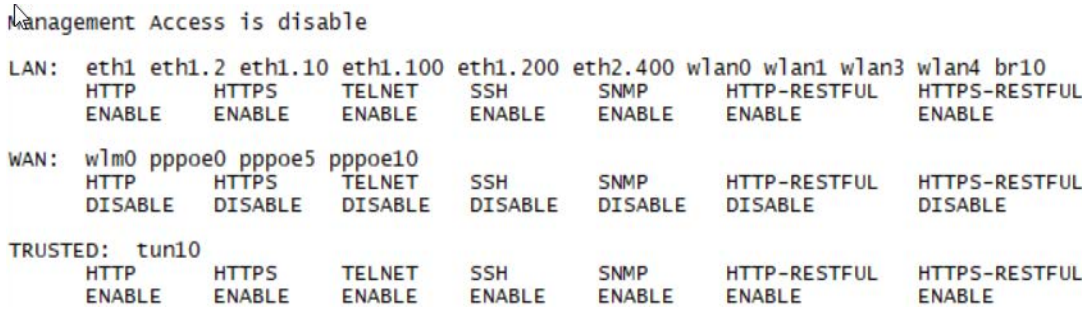
Use this command to display management access and access restrictions from the LAN and WAN side.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example shows management access methods for LAN/WAN and TRUSTED interfaces.

Perle#show management-access



```
Management Access is disable

LAN:  eth1 eth1.2 eth1.10 eth1.100 eth1.200 eth2.400 wlan0 wlan1 wlan3 wlan4 br10
      HTTP      HTTPS     TELNET    SSH       SNMP      HTTP-RESTFUL   HTTPS-RESTFUL
      ENABLE    ENABLE    ENABLE    ENABLE    ENABLE    ENABLE         ENABLE

WAN:  wlm0 pppoe0 pppoe5 pppoe10
      HTTP      HTTPS     TELNET    SSH       SNMP      HTTP-RESTFUL   HTTPS-RESTFUL
      DISABLE   DISABLE   DISABLE   DISABLE   DISABLE   DISABLE        DISABLE

TRUSTED:  tun10
      HTTP      HTTPS     TELNET    SSH       SNMP      HTTP-RESTFUL   HTTPS-RESTFUL
      ENABLE    ENABLE    ENABLE    ENABLE    ENABLE    ENABLE         ENABLE
```

Related Commands

(management-access-LAN)

(management-access-WAN)

show nat66

Syntax Description	**show nat66**
{**[prefix] |**	Display NAT66 prefixes.
[statistics] |	Display NAT66 statistics.
[<*filter/redirection options*>]}	Output modifiers see *Show Command Filtering and Redirection*
Command Modes	Perle#show nat66

Usage Guidelines

Use this command to display Network Address Translations (NAT) for IPv6 networks.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example shows NAT66 statistics

```
Perle#show nat66 statistics
Global Stats:
      ID:0
      Packets translated In -> Out
       1290003
      Packets translate Out -> In
       1290003
```

show network-watchdog

Syntax Description	show network-watchdog
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show network-watchdog

Usage Guidelines

Use this command to display network watchdog status and configuration.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example shows network-watchdog.

```
Perle#show network-watchdog
Network Watchdog Configuration/Status:
==============================================
Network-watchdog Router
       Configuration:
         Watchdog: Enable
         Target: 172.16.23.100
         Interface: eth1
         Interval: 1m
         Threshold: 2
```

```
Ping Count: 1
         Ping Timeout: 2s
         Fail Action: notification-only
        Test Status:
Total Success Count: 10 Since last reset Success Count: 9
         Total Failed Count: 1 Failed Tests 1/2 Next Test 0:0 (Min:sec)
         Reset Count: 1
```

Related Commands

network-watchdog

show ntp

See *show ntp*

show nvram:

See *show nvram:*

show policy-map

Syntax Description	show policy-map
{**[incoming] |**	Displays input-policy information.
[queueing] |	Displays queuing information.
[*<filter/redirection options>*]}	Output modifiers see *Show Command Filtering and Redirection*
Command Modes	Perle#show policy-map

Usage Guidelines

Use this command to display configured policy maps.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

```
Perle#show policy-map incoming
Interface action Received Dropped Overlimit
eth0 limiter 32 10 0
eth2 redirect 64 0 0
```

Related Commands

policy-map

show port-channel

Syntax Description	show port-channel
{**[member] |**	Displays port channel interface membership.
[status] |	Displays port channel interface details.
[*<filter/redirection options>*]}	Output modifiers see *Show Command Filtering and Redirection*
Command Modes	Perle#show port-channel

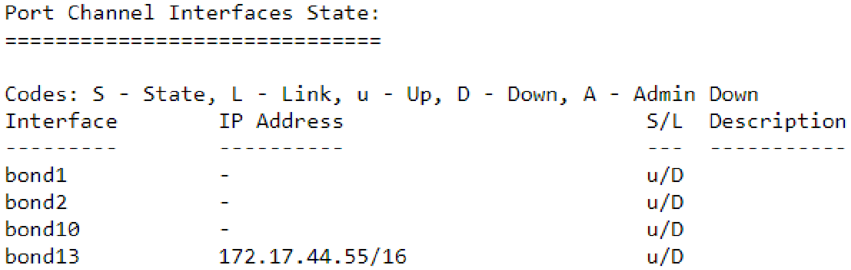
Usage Guidelines

Use this command to display port channel status and membership.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

Perle#show port-channel status



```
Port Channel Interfaces State:
==============================

Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
bond1            -                                 u/D
bond2            -                                 u/D
bond10           -                                 u/D
bond13           172.17.44.55/16                   u/D
```

Related Commands

(config-if-port-channel)#

show processes

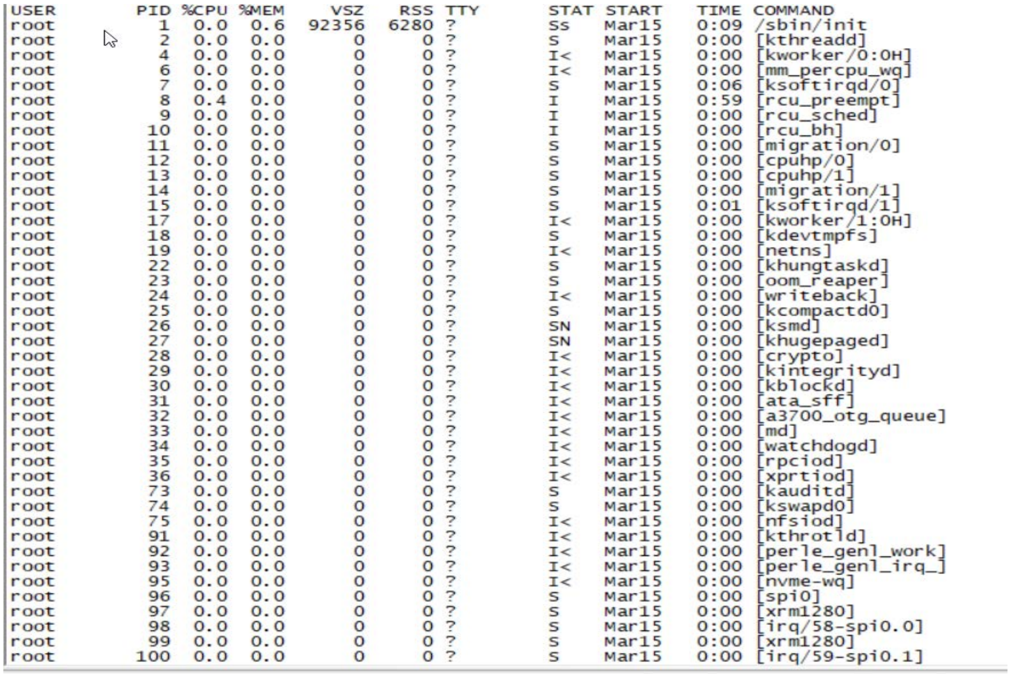
Syntax Description	show processes
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show processes

Usage Guidelines

Use this command to display processes running on your IOLAN.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Perle#show processes



```
USER          PID %CPU %MEM    VSZ    RSS TTY       STAT START   TIME COMMAND
root            1  0.0  0.6  92356   6280 ?         Ss   Mar15   0:09 /sbin/init
root            2  0.0  0.0      0      0 ?         S    Mar15   0:00 [kthreadd]
root            4  0.0  0.0      0      0 ?         I<   Mar15   0:00 [kworker/0:0H]
root            6  0.0  0.0      0      0 ?         I<   Mar15   0:00 [mm_percpu_wq]
root            7  0.0  0.0      0      0 ?         S    Mar15   0:06 [ksoftirqd/0]
root            8  0.4  0.0      0      0 ?         I    Mar15   0:59 [rcu_preempt]
root            9  0.0  0.0      0      0 ?         I    Mar15   0:00 [rcu_sched]
root           10  0.0  0.0      0      0 ?         I    Mar15   0:00 [rcu_bh]
root           11  0.0  0.0      0      0 ?         S    Mar15   0:00 [migration/0]
root           12  0.0  0.0      0      0 ?         S    Mar15   0:00 [cpuhp/0]
root           13  0.0  0.0      0      0 ?         S    Mar15   0:00 [cpuhp/1]
root           14  0.0  0.0      0      0 ?         S    Mar15   0:00 [migration/1]
root           15  0.0  0.0      0      0 ?         S    Mar15   0:01 [ksoftirqd/1]
root           17  0.0  0.0      0      0 ?         I<   Mar15   0:00 [kworker/1:0H]
root           18  0.0  0.0      0      0 ?         S    Mar15   0:00 [kdevtmpfs]
root           19  0.0  0.0      0      0 ?         I<   Mar15   0:00 [netns]
root           22  0.0  0.0      0      0 ?         S    Mar15   0:00 [khungtaskd]
root           23  0.0  0.0      0      0 ?         S    Mar15   0:00 [oom_reaper]
root           24  0.0  0.0      0      0 ?         I<   Mar15   0:00 [writeback]
root           25  0.0  0.0      0      0 ?         S    Mar15   0:00 [kcompactd0]
root           26  0.0  0.0      0      0 ?         SN   Mar15   0:00 [ksmd]
root           27  0.0  0.0      0      0 ?         SN   Mar15   0:00 [khugepaged]
root           28  0.0  0.0      0      0 ?         I<   Mar15   0:00 [crypto]
root           29  0.0  0.0      0      0 ?         I<   Mar15   0:00 [kintegrityd]
root           30  0.0  0.0      0      0 ?         I<   Mar15   0:00 [kblockd]
root           31  0.0  0.0      0      0 ?         I<   Mar15   0:00 [ata_sff]
root           32  0.0  0.0      0      0 ?         I<   Mar15   0:00 [a3700_otg_queue]
root           33  0.0  0.0      0      0 ?         I<   Mar15   0:00 [md]
root           34  0.0  0.0      0      0 ?         I<   Mar15   0:00 [watchdogd]
root           35  0.0  0.0      0      0 ?         I<   Mar15   0:00 [rpciod]
root           36  0.0  0.0      0      0 ?         I<   Mar15   0:00 [xprtiod]
root           73  0.0  0.0      0      0 ?         S    Mar15   0:00 [kauditd]
root           74  0.0  0.0      0      0 ?         S    Mar15   0:00 [kswapd0]
root           75  0.0  0.0      0      0 ?         I<   Mar15   0:00 [nfsiod]
root           91  0.0  0.0      0      0 ?         I<   Mar15   0:00 [kthrotld]
root           92  0.0  0.0      0      0 ?         I<   Mar15   0:00 [perle_genl_work]
root           93  0.0  0.0      0      0 ?         I<   Mar15   0:00 [perle_genl_irq_]
root           95  0.0  0.0      0      0 ?         I<   Mar15   0:00 [nvme-wq]
root           96  0.0  0.0      0      0 ?         S    Mar15   0:00 [spi0]
root           97  0.0  0.0      0      0 ?         S    Mar15   0:00 [xrm1280]
root           98  0.0  0.0      0      0 ?         S    Mar15   0:00 [irq/58-spi0.0]
root           99  0.0  0.0      0      0 ?         S    Mar15   0:00 [xrm1280]
root          100  0.0  0.0      0      0 ?         S    Mar15   0:00 [irq/59-spi0.1]
```

....

show radius

See ***show radius***

show reload

Syntax Description	**show reload**
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show reload

Usage Guidelines

Use this command to display scheduled IOLAN   reloads or reboots.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example show configured reloads.

```
Perle#show reload
Reload scheduled for 18:00:00 EDT Oct 17 2019 (in 59 minutes)
```

Related Commands

reload

show rest-api

Syntax Description	**show rest-api**
{**[jwt | server status] |**	Show RESTful API information.
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show rest-api

Usage Guidelines

Use this command to display RESTful API information.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays RESTful API information.

```
Perle#show rest-api server status
RESTful API HTTP server status: Disabled
RESTful API HTTP server port: 8080
Cookie maximum age timeout: 1440 seconds
RESTful API HTTPS server status: Disabled
RESTful API HTTPS server port: 8443
```

Related Commands

remote-management

show route-map

Syntax Description	**show route-map**
{**[<*WORD*>] |**	Displays specified route map.
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show route-map

Usage Guidelines

Use this command to display route map information.

Output modifiers (Pipe redirect)—allows you to pipe the output to the redirect options as specified.

Example

Shows route map details.

```
Perle#show route-map route1
RIB:
route-map route1, permit, sequence 2
  Match clauses:
  Set clauses:
  Call clause:
  Action:
    Exit routemap
RIP:
route-map route1, permit, sequence 2
Match clauses:
  Set clauses:
  Call clause:
  Action:
    Exit routemap
RIPV6:
route-map route1, permit, sequence 2
  Match clauses:
  Set clauses:
  Call clause:
  Action:
    Exit routemap
OSPF:
route-map route1, permit, sequence 2
  Match clauses:
  Set clauses:
  Call clause:
  Action:
    Exit routemap
```

```
BGP:
route-map route1, permit, since
  Match clauses:
  Set clauses:
  Call clause:
  Action: Exit routemap
```

Related Commands

router

show running-config

Syntax Description	show running-config
{[all] |	Displays all config including defaults.

[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show running-config

Usage Guidelines

Use this command to display the IOLAN's current running config. To make this configuration permanent you must copy running config to startup config.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Related Commands

show startup-config

show sdm

Syntax Description	**show sdm**
{**prefer** |	Displays the value for sdm.
[<*filter/redirection options*>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Default	Both IPv4 and IPv6
Command Modes	Perle#show sdm

Usage Guidelines

Use this command to display IPv4/IPv6 protocols running on your IOLAN.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays the current value for sdm.

```
Perle#show sdm prefer
The current template is ‘dual-ipv4-and-ipv6 default template
```

Related Command

sdm

show serial

Syntax Description	**show serial**
{**[advanced] |**	Displays advanced configuration.

[modbus gateway] |	Displays modbus configuration.
[port-buffering] |	Displays port buffering information.
[trueport remap] |	Displays Trueport configuration.
[username *<WORD>*] |	Displays user configuration for serial port.
[vmodem | vmodem-phone] |	Displays virtual modem phone number.
[*<filter/redirection options>*]}	Output modifiers see *Show Command Filtering and Redirection*
Command Modes	Perle#show serial

Usage Guidelines

Use this command to view serial configuration.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays the advanced configuration for serial.

```
Perle#show serial advanced
Process Break Signals            off
Flush on Close                off
Single Telnet                off
Data Logging Buffer Size          4K
Monitor Connection Interval         180 Seconds
Monitor Connection Number of Retries 5
Monitor Connection Retry Timeout     5 Seconds
```

Related Command

serial

show snmp

Syntax Description	**show snmp**
{**community** |	Displays community name.
[contact] |	Displays contact information
[engine-id] |	Displays SNMP engine-id.
[group] |	Displays SNMP groups.
[host] |	Displays host information
[location] |	Displays location information.

[mib ifmib ifindex] |	Displays SNMP ifmib information.
[user] |	Displays SNMP users.
[view] |	Displays SNMP views.
[<***filter/redirection options***>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show snmp

Usage Guidelines

Use this command to display SNMP configured options.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example show the configured options for SNMP.

```
Perle#show snmp view
View name: IOLAN-view
  include: iso, exclude
```

Related Commands

snmp-server

show ssh

See ***show ssh***

show startup-config

Syntax Description	**show startup-config**
{[<***filter/redirection options***>]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show startup-config

Usage Guidelines

Use this command to display the IOLAN‘s startup configuration. This is the configuration which is used when the device is first powered up or re-booted.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Related Commands

show running-config

show system

Syntax Description	show system
{[hardware] |	Displays hardware details.
[statuses] |	Displays system statuses for alarms, memory, flash etc:
[uptime] |	Displays IOLAN’s uptime.
[versions verbose] |	Displays IOLAN’s software versions.
[<*filter/redirection options*>]}	Output modifiers see *Show Command Filtering and Redirection*
Command Modes	Perle#show system

Usage Guidelines

Use this command to displays information about software versions.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

This is a sample of the type of information presented. The specific information displayed on your system is model Dependant.

```
Perle#show system statuses

System Statuses:
 System Up Time............................... 7
hours 26 minutes 4 seconds
 System Date and Time (local time
zone)........ 2019-12-10 18:02:18

Startup-Configuration state.................. In
Sync with
Running-configuration
System Statuses:
 System Up Time............................... 7 hours 26 minutes 4 seconds
 System Date and Time (local time zone)........ 2019-12-10 18:02:18
Startup-Configuration state.................. In Sync with
Running-configuration
CPU Utilization.............................. 4.55
 Memory (kBytes free)......................... 55420
  Flashdisk (Mbytes free)...................... 1008
```

show tacacs

See *show tacacs*

show task-status

Syntax Description	**show task-status**
{[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show task-status

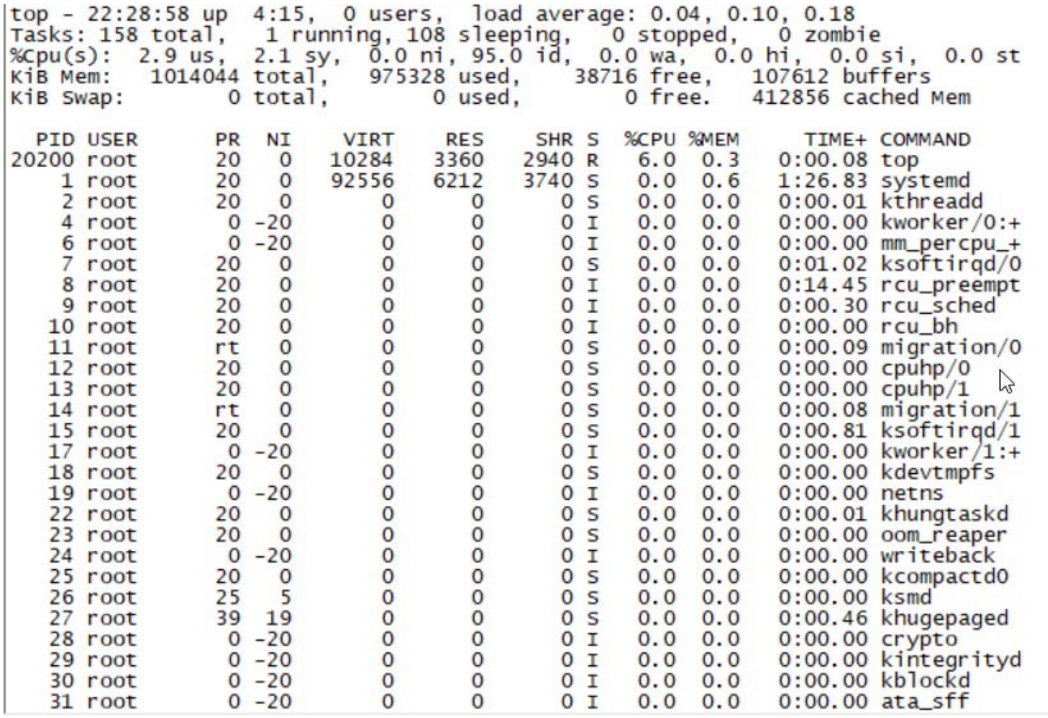
Usage Guidelines

Use this command to display system running tasks.

Output modifiers (Pipe redirect)—allows you to pipe the output to the redirect options as specified.

Examples

Perle#show task-status



```
top - 22:28:58 up  4:15,  0 users,  load average: 0.04, 0.10, 0.18
Tasks: 158 total,   1 running, 108 sleeping,   0 stopped,   0 zombie
%Cpu(s):  2.9 us,  2.1 sy,  0.0 ni, 95.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem:   1014044 total,   975328 used,    38716 free,   107612 buffers
KiB Swap:        0 total,        0 used,        0 free.   412856 cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
20200 root      20   0   10284   3360   2940 R   6.0  0.3   0:00.08 top
    1 root      20   0   92556   6212   3740 S   0.0  0.6   1:26.83 systemd
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.01 kthreadd
    4 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 kworker/0:+
    6 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 mm_percpu_+
    7 root      20   0       0      0      0 S   0.0  0.0   0:01.02 ksoftirqd/0
    8 root      20   0       0      0      0 I   0.0  0.0   0:14.45 rcu_preempt
    9 root      20   0       0      0      0 I   0.0  0.0   0:00.30 rcu_sched
   10 root      20   0       0      0      0 I   0.0  0.0   0:00.00 rcu_bh
   11 root      rt   0       0      0      0 S   0.0  0.0   0:00.09 migration/0
   12 root      20   0       0      0      0 S   0.0  0.0   0:00.00 cpuhp/0
   13 root      20   0       0      0      0 S   0.0  0.0   0:00.00 cpuhp/1
   14 root      rt   0       0      0      0 S   0.0  0.0   0:00.08 migration/1
   15 root      20   0       0      0      0 S   0.0  0.0   0:00.81 ksoftirqd/1
   17 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 kworker/1:+
   18 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kdevtmpfs
   19 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 netns
   22 root      20   0       0      0      0 S   0.0  0.0   0:00.01 khungtaskd
   23 root      20   0       0      0      0 S   0.0  0.0   0:00.00 oom_reaper
   24 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 writeback
   25 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kcompactd0
   26 root      25   5       0      0      0 S   0.0  0.0   0:00.00 ksmd
   27 root      39  19       0      0      0 S   0.0  0.0   0:00.46 khugepaged
   28 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 crypto
   29 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 kintegrityd
   30 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 kblockd
   31 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 ata_sff
```

....

show tech-support

Syntax Description	**show tech-support**
{[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show tech-support

Usage Guidelines

Use this command to capture internal IOLAN information. It will capture a large range of information which you could send to Perle technical support to assist in resolving issues.

Output modifiers (Pipe redirect)—allows you to pipe the output to the redirect options as specified.

show terminal

See ***show terminal***

show username

Syntax Description	**show username**
{[*<WORD>*] |	Type the username to display.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show username

Usage Guidelines

Use this command to display information about a user.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

```
Perle#show username lyn
username       lyn
   privilegeLevel 15
   Password:      ********
   password created: Fri Sep 18 21:18:27 testtime zone 2020
   Two Factor     Disabled
```

Related Commands

show users

show users

See ***show users***

show version

See ***show version***

show virtual-machine

Syntax Description	**show virtual-machine**

{**[active] |**	Displays the active virtual machine. Only one virtual machine can be active at a time.
[name:] |	Displays installed virtual machine names.
[storage-info] |	Displays VM storage information.
[*<filter/redirection options>*]}	Output modifiers see ***Show Command Filtering and Redirection***
Command Modes	Perle#show virtual-machine

Usage Guidelines

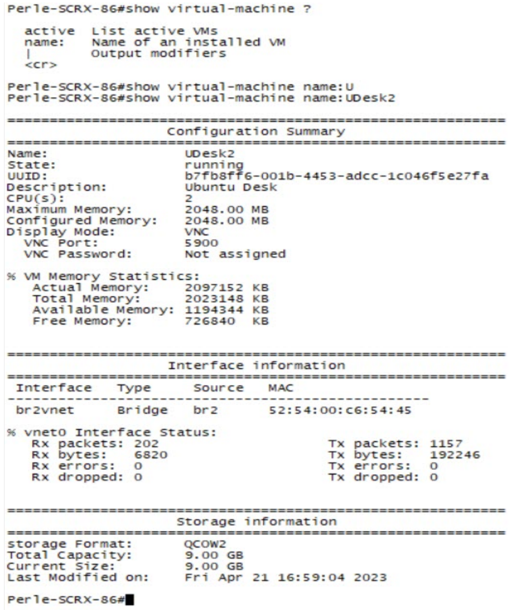
Use this command to display the active virtual machine or a configuration summary for a selected virtual machine.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays a configuration summary for the selected virtual machine.

Perle#show virtual machine name:Udesk2



```
Perle-SCRX-86#show virtual-machine ?

  active  List active VMs
  name:   Name of an installed VM
  |       Output modifiers
  <cr>

Perle-SCRX-86#show virtual-machine name:U
Perle-SCRX-86#show virtual-machine name:UDesk2

============================================================
                   Configuration Summary
============================================================
Name:                    UDesk2
State:                   running
UUID:                    b7fb8ff6-001b-4453-adcc-1c046f5e27fa
Description:             Ubuntu Desk
CPU(s):                  2
Maximum Memory:          2048.00 MB
Configured Memory:       2048.00 MB
Display Mode:            VNC
  VNC Port:              5900
  VNC Password:          Not assigned

% VM Memory Statistics:
   Actual Memory:        2097152 KB
   Total Memory:         2023148 KB
   Available Memory:     1194344 KB
   Free Memory:          726840  KB


============================================================
                   Interface information
============================================================
 Interface   Type     Source   MAC
------------------------------------------------------
 br2vnet     Bridge   br2      52:54:00:c6:54:45

% vnet0 Interface Status:
   Rx packets: 202                    Tx packets: 1157
   Rx bytes:   6820                   Tx bytes:   192246
   Rx errors:  0                      Tx errors:  0
   Rx dropped: 0                      Tx dropped: 0


============================================================
                    Storage information
============================================================
storage Format:          QCOW2
Total Capacity:          9.00 GB
Current Size:            9.00 GB
Last Modified on:        Fri Apr 21 16:59:04 2023

Perle-SCRX-86#
```

show vrrp

Syntax Description	**show vrrp**
{**[interface] |**	Displays VRRP information for specified interface.
[status] |	Displays VRRP statistics.
[*<filter/redirection options>*]}	See ***Show Command Filtering and Redirection***
Command Modes	Perle#show vrrp

Usage Guidelines

Use this command to display VVRP interface information and statistics.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Examples

This example displays VRRP information on Ethernet interface 1.

```
Perle#show vrrp interface 1
Interface: eth1
--------------
  Group: 10
  ----------
  State:     FAULT
  Last transition:  12m23s

  Priority:   100
  Advertisement interval: 1000 milli-sec
  Preempt:   enabled

  VIP count:   1
    172.16.44.55/16
```

Related Commands

vrrp

show zone-policy

<table>
<tr><th>Syntax Description</th><th>show zone-policy</th></tr>
<tr><td>{[zone <<i>WORD</i>>] |</td><td>Displays specified zone policy.</td></tr>
<tr><td>[<<i>filter/redirection options</i>>]}</td><td>Output modifiers see
<i>Show Command Filtering and Redirection</i></td></tr>
<tr><td><b>Command Modes</b></td><td>Perle#show zone-policy</td></tr>
</table>

Usage Guidelines

Use this command to show zone policy for the specified zone.

Output modifiers (Pipe redirect)—allows you to redirect the output to the options as specified.

Related Commands

zone-pair

shutdown

Syntax Description	shutdown
{**shutdown**}	Shutdown the IOLAN. The Reset button brings system backup.
Command Modes	Perle#shutdown

Usage Guidelines

Use this command to shutdown the IOLAN.

ssh

See ***ssh***

telnet

See ***telnet***

terminal

See ***terminal***

testemail

See ***testemail***

traceroute

See ***traceroute***

undebug

Syntax Description	undebug
{[**alarmgr] |**	Turns off alarmgr debug.
[all] |	Turns all debug off.
[bgp] |	Turns off BGP debug.
[bridge spanning-tree packet[|	Turns off bridge spanning-tree debug.
[clpd] |	Turns off clpd debug.
[dialer] |	Turns off dialer debug.
[dot1x-authenticator] |	Turns off dot1x authenticator debug.
[dot11-supplicant] |	Turns off dot1x debug.
[drmgrd] |	Turns off drmgrd debug.
[email] |	Turns off email debug.
[init] |	Turns off init process debug.

[ip] |	Turns off ip process debug.
[ipsec] |	Turns off IPsec debug.
[kernel] |	Turns off kernel debug.
[lldp] |	Turns off LLDP debug.
[logging] |	Turns off logging debug.
[ntp] |	Turns off NTP debug.
[rest-api] |	Turns off RESTful API debug.
[snmp] |	Turns off SNMP debug.
[trapmgr] |	Turns off trapmgr debug.
[tty] |	Turns off tty debug.
[vrrp] |	Turns off VRRP debug.
[vty] |	Turns off vty debug.
[wan-highavail] |	Turns off wan-highavail debug.
[wanifmgr]}	Turns off wanifmgr debug.
Command Modes	Perle#undebug

Usage Guidelines

Use this command to turn debugging mode off for a process.

Examples

This example turns off debugging for alarmmgr.

```
Perle#undebug alarmgr
Alarm Manager debugging is off
```

Related Commands

copy

password

traceroute

virtual-machine

Syntax Description	virtual-machine
{**[install local *<NAME>*]**	Enter the name of the local ISO image to be loaded into this virtual machine.

{**[export remote-system ftp: | http: | https: | scp: sftp: | usb-flash |**	Export disk image to a remote server or to usb flash.
[force-off] |	Forcefully shutdown an active VM.
[power-on]	Power on an inactive VM.
[reboot] |	Reboot the VM.
[resume] |	Resume a suspended VM.
[shutdown]	Gratefully shutdown the VM
[suspend] |	Suspend an active VM.
[uninstall] |	Uninstall the VM.
[blklist] |	Remove a disk image from the blacklist to allow it to be re-imported.
[install resume]}	Resume the installation of the VM
Command Modes	Perle#virtual-machine

Usage Guidelines

Use this command to create a virtual machine space in which to load a virtual machine ISO image.

Examples

This example specifies a virtual machine named LinuxVM.

```
Perle#virtual-machine install local LinuxVM
Perle(install-local)#
```

Related Commands

virtual-machine

(config-install-local)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-install-local)#
{**[cpu-cores** ***<WORD>*****] |**	Enter the number of CPU cores. At lease one core must be specified, Default is 1. Values are 1–3.
[description ***<LINE>*****] |**	Specify a description for this virtual machine.

[display [console | vnc authentication 0 | 7 | *<WORD>* | none] [port *<5900-5950* | auto] |	Display device at which you log into z/VM. Specify the authentication (if needed) and the port for the VNC server to connect to. Default is none for authentication Default is VNC for display
[install] |	Install the VM to the IOLAN. All mandatory fields must be entered. ● iso-file ● name of VM ● network settings <bvi 1-9999> ● operating system (os) to be used.
[iso-file usb-flash] |	Specify the iso file image from the usb flash drive.
[memory *<1024-5358>*] |	Specify the MB needed for this VM installation. Values are 1024-5358 MB Default is 1024 MB
[network bvi *<1-9999>*] |	Specify the bvi to be used with this VM. Values are 1–9999
[os generic | variant :***<WORD>*] |**	Use this o/s or variant when creating the VM.
[seed-file remote-system ftp: | http: | https: | scp | sftp | usb-flash] |	Specify the path to the remote file system or use the usb flash drive.
[storage *<WORD>*]}	Enter the MB size requirements of your installation
Command Modes	Perle(config-install-local)#

Usage Guidelines

Configure parameter for this Virtual Machine.

Examples

In this example the cpu cores is set to 3.

```
Perle(install-local)#cpu-cores 3
```

Related Commands

show virtual-machine

virtual-machine

vrrp

Syntax Description	**vrrp**

{**restart**}	Restart VRRP process.
Command Modes	Perle#vrrp

Usage Guidelines

Use this command to restart VRRP.

Examples

This example restarts VRRP.

```
Perle#restart vrrp
```

Related Commands

show virtual-machine

vrrp

wireguard

Syntax Description	**wireguard**
{export public-key | url [flash: | ftp: | http: | https: | scp: | sftp: | tftp:] *<filename>*] |	Export public and private keys.
[generate key default-keypair] |	Generates a new default key pair to be used for encryption.
[import private-key [terminal *<TEXT>*] | url [flash: | ftp: | http: | https: | scp: | sftp: | tftp:] *<filename>*] | [public-key *<TEXT>*] |	Import public and private keys.
[remove key default-keypair]}	Removes default key pair.
Command Modes	Perle#wireguard

Usage Guidelines

Use this command to copy a file from one location to another.

Examples

This example removes the default key pair.

```
Perle#wireguard remove key default-keypair
```

Related Commands

crypto

4 Global Configuration Mode

This chapter defines all the CLI commands in Global Configuration Mode. Some CLI commands may not be applicable to your model or running software.

aaa

Use the no form of this command to negate a command or set to defaults.

Syntax Description	aaa
{[**accounting dot1x default start-stop group** *<WORD>* **radius | tacacs] | [exec** *<WORD>* **| default none | start-stop broadcast | group |radius | tacacs | stop-only broadcast | group |radius | tacacs] | [system default none | start-stop] |**	When AAA accounting is enabled, the IOLAN reports user activity to the TACACS+ or RADIUS security server (depending on which security method is selected) in the form of accounting records. This allows the AAA accounting feature to track the services that users are accessing and the amount of network resources that users are consuming. Each accounting record contains accounting attributes that are stored on the security server. This data can then be analyzed for network management, client billing, and auditing. If using groups a pre-defined group must have been previously created.
[authentication attempts login *<1-25>* **| [dot1x default group** *<WORD>* **| radius] | [login** *<WORD>* **group** *<WORD>* **| ldap | local | none | radius | tacacs | default |**	Configure authentication parameters. Authentication verifies users before they are allowed access to the network and network services (which are verified with authorization).
[group *<WORD>* **| group | ldap local | none | radius | tacacs] | [two-factor pin-attempts** *<1-10>* **| pin-size** *<4-6>* **| pi n-tries** *<1-10>* **| [wan-only off | on] |**	The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.The first listed method is used. If it fails to respond, the second one is used, and so on. **Two factor** authentication parameters for pin attempts, size, and retries. **WAN-only** **Off**—all admin users, (privilege 15), require two factor authentication. **On**—admin users (privilege 15), require two factor authentication only for remote network connections.
[authorization [console] | [exec *<WORD>* **| group** *<WORD>* **if-authenticated | local | none | radius | tacacs] |**	Configure parameters for the authorization EXEC command. This determines if the user is allowed to run in EXEC mode. EXEC authorization applies to vty and tty lines.The first listed method is used. If it fails to respond, the second one is used, and so on. "If-authenticated" is configured for authorization and the user is authenticated, no authorization is needed, and the user gets full admin privileges.

[group server [ldap *<WORD>*] | [radius *<WORD>*] | [tacacs *<WORD>*] |	Configure a group server for LDAP, RADIUS or TACACS+.
[local [authentication attempts max-fail *<1-65535>*] | [username min-len *<1-32>*] | [lockout-time *<30-65535>*] |	Configure local user failed authentication attempts. Value is 1–65535 attempts Default is never lock the user out. Configure the minimum length for user names. Values are 1 to 32 Default is minimum length of 1. Lock out time is 30 to 65535 in minutes.
[password expiry *<1-999>* | pbkdf2 rounds *<1000-100000000>* | restriction enable | group [lower-case *<1-5>* | numeric *<1-5>* | special | upper-case *<1-5>* | max-len *<1-128>* | min-len *<1-64>* | reuse *<1-32>*]}	Configure password restrictions. • Password cannot be the same as User name • Cannot have 3 consecutive characters in the same password • No password is not allowed • Special character are any non alphanumeric character • Minimum number of lowercase characters is 1–5 • Minimum number of lowercase numeric numbers is 1–5 • Minimum number of special characters is 1–5 • Minimum number of uppercase characters is 1–5 • Number of times a password can be changed before it can be reused. Value is 1–32 times pbkdf2 round default is 100000 The larger number of rounds, the more secure password hashing, however slower logins will occurs.
Command Modes	Perle(config)#aaa

Usage Guidelines

Configure Authentication, Authorization, and Accounting parameters.

Examples

This example generates start and stop accounting records.

```
Perle(config)#aaa accounting network default start-stop group radius
```

This example configures authentication and authorization to RADIUS as the first method to authenticate/authorize, then local database as the second method for all users.

```
Perle(config)#aaa authentication login default group radius local
Perle(config)#aaa authorization exec default group radius local
```

This example sets two-factor authentication attempts to 2.

```
Perle(config)#aaa authentication two-factor pin-attempt 2
```

Related Commands

clear aaa

(config-ldap-server)

clear ldap

(config-sg-radius)

clear radius

(config-sg-tacacs)

clear tacacs

(config-user-2factor)

(config-sg-ldap)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-sg-ldap)#**
{**[server name** ***<WORD>*****]**}	Configure LDAP server name.
Command Modes	Perle(config-sg-ldap)#

Usage Guidelines

Use this command to configure LDAP server name.

Examples

This example configures the LDAP server name to LDAP1.

```
Perle(config-sg-ldap)#server name ldap1
```

Related Commands

clear ldap

ldap

show ldap

(config-sg-radius)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-sg-radius)#
{server name <WORD>}	Configure RADIUS server name.
Command Modes	Perle(config-sg-radius)#

Usage Guidelines

Use this command to configure the RADIUS server name.

Examples

This example configures the RADIUS server name to RADIUS1.

```
Perle(config-sg-radius)#server name radius1
```

Related Commands

clear radius

ip radius

show radius

(config-radius-server)

(config-sg-tacacs)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-sg-tacacs)#
{server name <WORD>}	Configure TACACS+ server name.
Command Modes	Perle(config-sg-tacacs)#

Usage Guidelines

Use this command to configure the TACACS+ server name.

Examples

This example configures the TACACS+ server name to TACACS1.

```
Perle(config-sg-radius)#server name tacacs1
```

Related Commands

ip tacacs

tacacs

clear tacacs

show tacacs

alarm

Use the no form of this command to negate a command or set to defaults.

Syntax Description	alarm

{profile *<WORD>*}	See ***(config-alarm-profile)#*** for configuring parameters.
Command Modes	Perle(config)#alarm

Usage Guidelines

Use this command to configure parameters for alarms.

Examples

This example configures creates a profile called test1.

Perle(alarm)#profile test1

Related Commands

show alarm

(config-alarm-profile)#

(config-alarm-profile)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-alarm-profile)#**
{[alarm | link-fault | not-forwarding | not operating] |	Monitors for alarm type. ● link-fault ● port-not-forwarding ● port-not-operating
[notifies | link-fault | not forwarding | not operating] |	Sends a trap/notification to the configured SNMP host trap receivers on the triggering and clearing of the alarms. ● link-fault ● port-not-forwarding ● port-not-operating
[syslog link-fault | not-forwarding | not operating] |	Sends a syslog message to the configured syslog host on the triggering and clearing of these alarms. ● link-fault ● port-not-forwarding ● port-not-operating
Command Modes	Perle(config-alarm-profile)#

Usage Guidelines

Use this command to configure alarm profile parameters.

Examples

This example configures an alarm profile to monitor for link fault and send a syslog message to the configured server.

```
Perle(config))#alarm profile test-alarm
Perle(config-alarm-profile)#alarm link-fault
Perle(config-alarm-profile)#syslog link-fault
```

Related Commands

show alarm

archive

(config-archive)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-archive)#
{**[maximum *1-14*] |**	Configure the number of configuration archives to keep in the archive list. Archive list can contain between 1–14 configurations.
[path flash: | ftp: | http: | https: | scp: | sftp | tftp: | usb:<1-8>] |	Configure the file system path for archived configurations. The path must exist.
[time-period *<0-525600>*] |	Configure the time period to automatically save the running configuration to an archive file.
[update-sw check | auto-download] |	Enables update-software check. Check default is Disabled Auto-download is enabled for FN models
[write-memory]}	Enables—saves the configuration to an archive file each time you copy running-config to start-up config.

Command Default	no path maximum 10 no time-period no write-memory
Command Modes	Perle(config-archive)#archive

Usage Guidelines

Use this command to configure the full path to store archive configuration files.

flash:*perle-image-name.img*

ftp:*[[//username[:password]@location]/directory]/perle-image-name.img*

http://*[[username:password]@][hostname* | *host-ip [directory] /perle-image-name.img*

https://*[[username:password]@][hostname* | *host-ip [directory] /perle-image-name.img* |

scp:*[[username@location]/directory]/perle-image-name.img* |

sftp:*[[//username[:password]@location]/directory]/perle-image-name.img* |

tftp:*[[//location]/directory]/perle-image-name.img*

usb:*<1-8>*

Examples

This example sets up an archive path for the write-memory command.

```
Perle(config-archive)#path flash:
Perle(config-archive)#write-memory
Perle(config-archive)#exit
Perle(config)#exit
```

If you do not supply a filename, then your running config is named with the current date and time. See below.

```
Perle#show flash:
Directory of flash:
78      -rw-      10764  Sep 22 2020 11:30 -06:00 -Sep-22-11-30-29-0130322   -rw-
5643 Perle
```

Related Commands

show archive

(config-archive)#

archive

arp

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**arp**
{*<A.B.C.D> <H.H.H>* **bvi** *<1-9999>*] | [**ethernet** *<1-x>*. *<1-4000>*]}	Add static ARP entry to the ARP table. <1-x> = maximum number of ethernet ports, (depends on the model)
Command Modes	Perle(config)#arp

Usage Guidelines

Use this command to add ARP entries to ARP table.

Examples

Add this ARP entry to the ARP table.

```
Perle(config)#arp 172.16.44.55 1234.1234.1234 bvi 2
```

Related Commands

show arp

banner

Use the no form of this command to negate a command or set to defaults.

Syntax Description	banner
{[<*LINE*>]	Configure a delimiting character to indicate the start and end of the message. It cannot be a character that you use in the message. Do not use " or % as a delimiting character. No white space characters are allowed.
[login <*LINE*>]	Configure the login banner.
[motd <*LINE*>]	Configure the message of the day (MOTD) on login.
[prompt-timeout <*LINE*>]}	Configure the message for login authentication timeout.
Command Modes	Perle(config)#banner

Usage Guidelines

Use this command to configure a banner or message of the day to display to users.

delimiter character—indicates the start and end of the message and is not a character that you use in the message. Do not use " or % as a delimiting character. White space characters do not work.

banner text—the text is alphanumeric, case sensitive, and can contain special characters. It cannot contain the delimiter character you have chosen. The text has a maximum length of 80 characters and a maximum of 40 lines.

The banner has special macros that are inserted into the banner.

They are:

$(hostname) which is the hostname you configured on the switch and **$(domain)** which is the domain name you configured on the IOLAN.

login—set login banner

motd—set message of the day (motd)

prompt-timeout—login authentication timeout

Banner applies to all consoles and vty sessions.

Examples

Displays a message of the day at login.

```
Perle(config)#banner motd line
Enter text message. End with the character ’l’
Good morning crew

Enter configuration commands, one per line. End with CNTL/Z
```

This example sets the domain name to be used in the banner, then set a banner of Good morning and Welcome to your domain. Domain is replaced with the domain name of MYTEST-DOMAIN.

```
Perle(config)# ip domain-name MYTEST-DOMAIN
Perle(config)#banner hGood morning and Welcome to your h
$(domain)
```

Related Commands

(config-line)#console

boot

Use the no form of this command to negate a command or set to defaults.

Syntax Description	boot
{[host dhcp | [retry timeout *<600-65535>*]}	Configure boot parameters. **host dhcp**—enables Zero Touch provisioning (ZTP). Download configuration via DHCP server. **host retry timeout**—sets the time in seconds to wait for ZTP to complete (including time to download config or software). **no boot host retry timeout**—waits indefinitely for ZTP to complete.
Command Modes	Perle(config)#boot

Usage Guidelines

Use this command to enable ZTP. This command allows you to download your config and firmware via your DHCP server.

Examples

This example configures ZTP so that configuration and firmware files are downloaded from your DHCP server.

```
Perle(config)#boot host dhcp
```

bridge

Use the no form of this command to negate a command or set to defaults.

Syntax Description	bridge

{[bridge *<1-4000>* | spanning-tree | protocol ieee] |	Configure the bridge range and spanning-tree. Values are 1 to 4000.
[spanning-tree logging]}	Configure spanning tree logging.
Command Modes	Perle(config)#spanning-tree bridge

Usage Guidelines

Use this command to configure a bridge range and enable spanning tree sub-menu. Spanning Tree Protocol (STP) is a loop free topology for an Ethernet local area network. If loops are detected, the protocol blocks one of the paths to eliminate the loop. STP prevents bridge loops and broadcast radiation. The spanning-tree protocol is applied to previously defined bridge interfaces.

Examples

This example configures bridge 10 with spanning-tree.

```
Perle(config)#bridge 10 spanning-tree
Perle(config-st-bridge)#
```

Related Commands

(config-st-bridge)#

(config-st-bridge)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-st-bridge)#**
{[aging -time *<10-1000000>*] |	Configure the timeout period in seconds, for aging out dynamically learned forwarding information. Values are 1 to 1000000 in seconds Default is 300 seconds
[forward-time *<4-30>*] |	Configure the forward delay timer. The forward delay timer is the time interval spent in the listening and learning state. Values are 4 to 30 seconds Default is 15 seconds.
[hello-timer *<1-10>*] |	Configure the hello timer. The hello timer is the time between each bridge protocol data unit (BPDU) sent on a port. Values are 1 to 10 seconds Default is 2 seconds.

[loopguard default] |	Configure the Spanning Tree Protocol (STP) loop guard feature which provides additional protection against Layer 2 forwarding loops (STP loops). An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the forwarding state. Default is Disabled
[max-age *<10-1000000>*] |	Configure the max age timer to control the maximum length of time that passes before a bridge port saves its configuration BPDU information. Value are 10 to 100000 seconds Default is 20 seconds
[max-hops *<6-40>*] |	Configure the number of possible hops in the region before a bridge protocol data unit (BPDU) is discarded. Value are 6 to 40 Default is 20
[mode mstp | rstp | stp] |	Set the spanning tree mode. ● Spanning Tree Protocol (STP) ● Rapid Spanning Tree Protocol (RSTP) ● Multiple Spanning Tree Protocol (MSTP) Default is RSTP
[mst instance *<0-4000>* | name *<WORD>* revision *<0-65535>*] |	Configure MST instances for the region. Each region can have multiple instances. Map VLANs to an MST instance (0-63). Instance 0 cannot be deleted and is used to map/unmapped VLANs to instance 0. Each instance has a VLAN or range of VLANs which is associated with it. Name—define the name of the region. Revision—This setting must be the same for all MSTP switches in the same MST region

[port-fast disable | edge | network] |	A spanning tree normal port is one that functions in the default manner for spanning tree. Under normal circumstances it will transition from the Listening, Learning, Forwarding stages based on the default timers. PortFast causes a port to enter the spanning tree forwarding state immediately, bypassing the listening and learning states. STP enabled ports that are connected to devices such as a single switch, workstation, or a server can access the network only after passing all these STP states. Some applications need to connect to the network immediately, else they will timeout. **Disable**—go through normal learning/forwarding and blocking states.
[port-fast edge |	**Edge**—is used to configure a port on which an end device is connected such as a PC. All ports directly connected to end devices cannot create bridging loops in the network. Therefore, the edge port directly transitions to the forwarding state, and skips the listening and learning stages. However, the specific command configures a port such that if it receives a BPDU, it immediately loses its edge port status and becomes a normal spanning-tree port.
[port-fast network] |	**Network**—Interface goes into forward state immediately. Portfast network protects against loops by detecting unidirectional links in the STP topology.
[priority *<0-61440>*] |	Every IOLAN participating in a Spanning Tree Protocol (STP) network is assigned with a numerical number called a bridge priority value. Priority values decide who will be elected as root. You can set the bridge priority in increments of 4096 only. When you set the priority, valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. You set the priority value argument to 0 to make the IOLAN root. Default is 32768
[root] |	Configure the root bridge.The root bridge is the bridge with the smallest (lowest) bridge ID.
[transmit hold-count *<1-10>*]}	Controls the number of BPDUs sent before pausing for 1 second. Range is 1 to 10 seconds Default is 6 seconds
Command Modes	Perle(config-st-bridge)#

Usage Guidelines

Configures the parameters for Spanning Tree Protocol.

Examples

This example sets mode to MSTP.

```
Perle(config-st-bridge)#spanning-tree mode mstp
```

Related Commands

(config-st-bridge)#

cellular

Use the no form of this command to negate a command or set to defaults.

Syntax Description	cellular
sms authentication method both | none | password | phone | user *<WORD>* enable | password 0 *<WORD>* | 7 *<WORD>* | *<WORD>* | phone *<LINE>* | privilege admin | none | restricted}	Configure SMS authentication parameters.
{profile *<WORD>* [5gband <auto> | 1 | 2 | 3 | 5 | 28 | 41 | 48 | 66 | 71 |77 |78] | authentication chap | pap | none | [band 1 | 2 | 3 | 4 | 5 | 7 | 8 | 9 | 12 | 13 | 14 | 18 | 19 | 20 | 26 | 28 | 29 | 30 | 32 | 41 | 42 | 43 | 46 | 48 | 66 | auto] |data-apn access-point-name *<WORD>* | cid *<1-16>* | pdp-type ipv4 | ipv4ipv6 | ipv6 | data-limit action-on limit disable-lte | none | alert-on-limit off |on | alert-percentage *<0-99>* | bill-day *<1-31>* | mb-size *<0-100000>* | firmware att | generic | other | sim-select | verizon | [password 0 *<LINE>* | 7 *<LINE>* | *<LINE>* | 0 *<LINE>* | 7 *<LINE>* | *<LINE>*] | roaming on | off | sim-slot 1 | 2 | technology 5g | auto | lte | umts | username *<WORD>* |	Configure cellular profile parameters. Some bands may not be available on all models. Depending on the product model you may have either 1 or 2 SIM slots.

sms authentication method both | none | password | phone | user *<WORD>* enable | password 0 *<WORD>* | 7 *<WORD>* | *<WORD>* | phone *<LINE>* | privilege admin | none | restricted}	Configure SMS authentication parameters.
Command Default	SMS authentication default method is both.
Command Modes	Perle(config)#cellular

Usage Guidelines

Use this command to configure cellular profiles.

Examples

This example sets up a cellular connection using a profile test to browse the Internet.

```
Perle(config)#cellular profile test data-apn access-point-name ssid90 cid 10
```

Related Commands

(config-st-bridge)#

show bridge

(config-st-bridge-mst-instance)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-st-bridge-mst-instance)#**
{**[priority *0-61440>*] |**	Every IOLAN participating in a Spanning Tree Protocol (STP) network is assigned with a numerical number called a bridge priority value. Priority values decide who will be elected as root. You can set the bridge priority in increments of 4096 only. When you set the priority, valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. You set the priority value argument to 0 to make the IOLAN. Default is 32768
[vlan *<1-4000>*]}	Configure the range of VLANs to add this instance mapping
Command Modes	Perle(config-st-bridge-mst)#

Usage Guidelines

Configures the priority parameters for Multiple Spanning Tree Protocol (MST).

Examples

This example sets the bridge priority to 28672.

```
Perle(config-st-bridge-mst)#priority 28672
```

Related Commands

(config-st-bridge)#

(config-if-ethernet)#

class-map

Use the no form of this command to negate a command or set to defaults.

Syntax Description	class-map
{*<1-4094>*}	Configure a class-map number. Priority queues can only use class 1–7.
Command Modes	Perle(config)#class-map

Usage Guidelines

Use this command to classify inbound network traffic destined to, or passing through, the IOLAN based on a series of flow match criteria.The class map classifies network traffic based on various match criteria configured within a class map. In other words, it defines traffic classes. A class map can reference an ACL to be used as the criteria or specific criteria is applied to the class map. Class maps in turn are referenced by policy maps.

Examples

This example creates class map 1.

```
Perle(config)#class-map 1
```

Related Commands

policy-map

(config-cmap)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-cmap)#
{**[description *<LINE>*] |**	Configure a class-map match-name description.
[match-name *<NAME>*]}	Configure a name for this classification.
Command Modes	Perle(config-cmap)#

Usage Guidelines

Use this command to create a classification. Classifications are separation of packets into traffic classes. Configure the device to take a specific action on the specified classified traffic, such as policing or marking down, or other actions.

Examples

In this example the name specified for this classification is match-icmp.

```
Perle(config-cmap)#match-name match-icmp
```

Related Commands

(config-cmap-match)#

policy-map

(config-cmap-match)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-cmap-match)#
{**description** *<LINE>* |	Description of class-map match-name.
[match ethernet destination *<H.H.H>* **source type | type** *<0-65535>***] |**	Match Ethernet header.
[interface [bvi *<1-9999>***] | [dialer** *<0-15>***] | [ethernet** *<1-x>* **| [openvpn-tunnel** *<0-999>***] | [tunnel** *<0-999>***] |**	Match interface.
[ip [destination address *<A.B.C.D> <A.B.C.D>***] |**	Destination IP address or prefix.
[ip destination port *<0-65535>***] |**	Destination port number to match.
[dscp *<0-63>* **| af11 | af12 | af13 | af21 | af22 | af23 | 31 | af32 | af33 | af41 | af42 | af43 |cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef] |**	Match IP DSCP (DiffServ Codepoints)
[max-length *<0-65535>***] |**	Maximum packet length.

[protocol *<0-255>* **| ah | dccp | dsr | egp | eigrp | encap | esp |etherip | ggp | gre | hmp | icmp | odpr | igmp | igp | ip | ipip | ipv6 | ipv6-frag | ipv6-icmp | ipv6-nonxt | opts | ipv6-route | isis | l2tp | manet | mpls-in-ip | narp | osfo | pim | rdp | roch | rsvp | sctp | sdrp | shim6 | skip | tcp | udp | udplite | vrrp | xns-idp] |**	Protocol to match.
[source address *<A,B.C.D> <A,B.C.D>***] | [port** *<1-65535>***] |**	Match values for source.
[tcp-flags ack | syn] |	TCP flags to match.
ipv6 [destination *<X:X:X:X::X>/<0-128>***] |**	Destination IPv6 address or prefix.
[ip destination port *<0-65535>***] |**	Destination port number to match.
[ipv6 dscp *<0-63>* **| af11 | af12 | af13 | af21 | af22 | af23 | 31 | af32 | af33 | af41 | af42 | af43 |cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef] |**	Match IP DSCP (DiffServ Codepoints)
[ipv6 max-length *<0-65535>***] |**	Maximum packet length.
[ipv6 protocol *<0-255>* **| ah | dccp | dsr | egp | eigrp | encap | esp |etherip | ggp | gre | hmp | icmp | odpr | igmp | igp | ip | ipip | ipv6 | ipv6-frag | ipv6-icmp | ipv6-nonxt | opts | ipv6-route | isis | l2tp | manet | mpls-in-ip | narp | osfo | pim | rdp | roch | rsvp | sctp | sdrp | shim6 | skip | tcp | udp | udplite | vrrp | xns-idp] | [tcp-flags ack | syn] | udplite | vrrp | xns-idp] |**	Protocol to match.
[ipv6 source address *<X:X:X:X::X/<0-128>* **| port** *<1-65535>***] |**	Match values for source.

[ipv6 tcp-flags ack | syn] |	TCP flags to match.
[mark ***<1-214748748364>*****] |**	Match on mark applied by policing routing.
[vlan ***<1-4000>*****]**}	Match on VLAN ID
Command Modes	Perle(config-cmap-match)#

Usage Guidelines

Use the match command to configure "rules" or matches to apply to the class-map. If the packet matches any of the criteria configured for this class map, then this class map is applied to the packet.

Examples

This example I have specified the name bridge-50-match and matched on ip source address of 172.16.88.88.

```
Perle(config-cmap)#match-name bridge50-map
Perle(config-cmap-match))#match ip source address 172.16.88.88 icmp
```

Related Commands

(config-cmap)#

policy-map

clock

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**clock**
{**[summer-time** ***<WORD >*** **date** ***<1-31> <MONTH > <hh:mm> <1-31> <MONTH > < hh:mm >*** **[*****<1-1440-in-minutes>*****] | [*****recurring <1-4 >*****] [*****<FIRST >*****] [*****<LAST>*****] |**	Configure the name of the summer time zone followed by start/end dates. **Configure start time:** ● numeric value for the day of the month to start summer timezone 1–31 ● numeric value for the day of the month to start summer timezone 1–31 ● name of the month to start January, February, March, April, May, June, July, August, September, October, November, December ● time to start in hours (24 hour clock) and minutes **Configure end time:** ● numeric value for the day of the month to end summer timezone 1–31 ● name of the month to end (January, February, March, April, May, June, July, August, September, October, November, December) ● time to end in hours (24 hour clock) offset in minutes 1–1440

[timezone *<WORD>* *<-23 - 23>* | *<0-59>*}	Configure the timezone as hours/minutes offset from Universal Time Clock (UTC).
Command Modes	Perle(config)#clock

Usage Guidelines

Use this command to configure the clock.

Examples

This example configures the clock 6 hours off from UTC.

```
Perle(config)#clock timezone ont-time-zone -6
```

Related Commands

show clock

container (OCI)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**container**
{[name *<LINE >*] |	Create container with this name.
[network *<WORD>*] |	Create container with this network name.
registry - | hostname:port username *<WORD>* secret *<WORD>*]}	Registry ● - (use default docker registry) ● - hostname:port Username–specify the user Secret–specify a password for this user
Command Modes	Perle(config)#container

Usage Guidelines

Use this command to configure container parameters.

Examples

This example creates container network new-container.

Perle(config)#container network new-container <cr>

Perle(config-container-net)#

This example show you how to supply registry credentials to add images from repositories that require a CA certificate, cert, and key file.

First add the host to the router host table
Perle(config)#ip host lab-debian 172.16.48.20

Second upload the registry keys that are need for this host.
Perle(config)#crypto pki import container-registry lab-debian:443 ca url http://lab-debian/certs/ca.crt

Perle(config)#crypto pki import container-registry lab-debian:443 cert url http://lab-debian/certs/myrouter.cert

Perle(config)#crypto pki import container-registry lab-debian:443 key url http://lab-debian/certs/myrouter.key

Perle(config)#container registry lab-debian:443 username admin secret perle1

Perle#container image add lab-debian:443/myimage

Related Commands

container (OCI)

show container (OCI)

(config-container)#

(config-container)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-container)#
[arguments *<1-40> <LINE>* |	Arguments to be supplied to the container when it starts.
[clean-restart] |	On bootup or restart container, container will be removed first before restarting.
[description *<LINE>*] |	**Description**–container description. Max is 32 characters.
[disable] |	**Disable**–disable container instance.
[environment *<WORD>* *<LINE>*] |	**WORD**–add a custom environment variable. **LINE**–set environment variable.
[image *<WORD>* image *<WORD>* *<WORD>* [autoadd] |	**WORD**–image name. **WORD**–container image tag or digest **Autoadd**–automatically download image if required.
[import-changes] |	Run the image modified with the supplied file from an earlier export-changes.

[log max-size *<100-10000>* no-compress] |	Specify the size of the log file. Maximum size of the log file is in KiB. Turn compress of the rotating log files off.
[memory *<6-512>*] |	**Memory**–container memory in megabytes (MB).
[network *<WORD>* ip address *<A.B.C.D>* | ipv6 address *<X:X:X:X::X>*] |	**WORD**–creates a container with the given name **ip/ipv6**–assigns static ip or ipv6 address.
[restart-policy always | no | on-failure [*<0-9999>*]}	**Restart–policy** **Always**–restart containers when they exit, regardless of status exit code, retrying indefinitely. **no**–do not restart containers on exit. **on-failure**–restart containers when they exit with a non-zero exit code, retrying <0-9999> times. Default is: on failure 100 retries, 0 for infinite.
Command Modes	(config-container)#

Usage Guidelines

Use this command to configure container parameters.

Examples

This example creates a container called test-container1 with a static IP address of 172.16.88.88.

```
(config-container)#network-container test ip address 172.16.88.88 <cr>
```

This example adds argument ps -aef to container test. On connect to the container this argument will be run on the container and output will be redirected to your CLI prompt.

```
(config)#container name test <cr>
(config-container)#image alpine <cr>
(config-container)#argument 1 ps <cr>
(config-container)#argument 2 -eaf <cr>
(config-container)#no disable <cr>

#show container test log <cr>
#   PID USER  TIME .....COMMAND
    1 root      0:00     ps-aef
```

Related Commands

(config-container)#

container (OCI)

(config-container-net)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-container-net)#**

{**[description** ***<LINE>*** **| network-interface bvi** ***<1-9999>*** **dhcp | dhcpv6]**}	Description–container network description. Network-interface–select bridge interface 1-9999.
Command Modes	(config-container-net)#

Usage Guidelines

Use this command to configure container network parameters. Any changes to this setting requires a reboot to take effect.

Examples

This example creates BVI (Bridge-Group Virtual Interface) 10.

```
(config-container-net)#network-interface bvi 10 <cr>
```

Related Commands

(config-container)#

container (OCI)

container-management (OCI)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**container-management**
{**enable**}	Starts container management services.
Command Modes	Perle(config)#container-management

Usage Guidelines

Use this command to enable container management.

Examples

This example enables container management process.

```
Perle(config)#container-management
```

Related Commands

(config-container)#

(config-container-net)#

container (OCI)

controller

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**controller**
{**[cellular** ***<0-0>*****]**}	Enter sub-menu cellular mode.
Command Modes	Perle(config)#controller

Usage Guidelines

Use this command to enter the sub-menu cellular mode.

Examples

This example to enter the sub-menu cellular mode.

```
Perle(config)#controller cellular 0
```

Related Commands

show crypto

cellular

(config-controller)#

(config-controller)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-controller)#
[lte alternative-profile *<WORD>* **| diversity | enable | [failover | connect-retires** *<1-100>* **| enable | revert-timer** *<1-1500>* **signal-loss-timer** *<1-60>* **| signal threshold** *<-150-0>*] **| primary-profile** *<WORD>*	Enable, configure and disable features on the LTE (cellular) interface.
[power-down]}	Power down cellular module
Command Modes	Perle(config-controller)#

Usage Guidelines

Use this command to configure LTE parameters found under the config-controller sub-menu.

Examples

In this example we are going to activate the use of the diversity antenna.

```
Perle(config-controller)#lte diversity
```

Related Commands

(config-st-bridge-mst-instance)#

(config-cmap-match)#

policy-map

crypto

Use the no form of this command to negate a command or set to defaults

Syntax Description	crypto

<table>
<tr><td>{[<b>ipsec client</b> <i>&lt;WORD&gt;</i> | <b>enable</b> | <b>esp-group</b> <i>&lt;WORD&gt;</i> | <b>ike-group</b> <i>&lt;WORD&gt;</i> | <b>import ipsec.conf terminal</b>] |</td><td>See <i>(config-client)</i> to configure parameters.
Enables or restarts IPsec.
See <i>(config-esp)#</i> to configure parameters.
See <i>(config-ike)#</i> to configure parameters.
Specify where to import the ipcsec.conf file.</td></tr>
<tr><td colspan="2"><b>flash:</b><i>filename</i> |
<b>ftp:</b><i>[[//username[:password]@location]/directory]/filename</i> |
<b>http://</b><i>[[username:password]@][hostname | host-ip [directory] /filename</i> |
<b>https://</b><i>[[username:password]@][hostname | host-ip [directory] /filename</i> |
<b>scp:</b><i>[[username@location]/directory]/filename</i> |
<b>sftp:</b><i>[[//username[:password]@location]/directory]/filename</i> |
<b>tftp:</b><i>[[//location]/directory]/filename</i> |</td></tr>
<tr><td><b>l2tp</b> |
<b>nat-network</b> <i>&lt;A&gt;B&gt;C&gt;D/N&gt;</i> |
<b>nat-transversal</b> |
<b>l2tp</b> |
<b>nat-network</b> <i>&lt;A&gt;B&gt;C&gt;D/N&gt;</i> |
<b>nat-transversal</b> |</td><td>See <i>(config-12tp)</i> to configure parameters.
Configure a permitted IPsec Network Address Translation (NAT) network/mask.
Enables Network Address Translation (NAT) Transversal. NAT Transversal allows traffic to get to the specified destination when a device does not have a public IP address.
This is usually the case if your ISP is doing NAT, or the external interface of your firewall is connected to a device that has NAT enabled.</td></tr>
<tr><td>[<b>key</b> [<b>export password-cryptkey terminal</b>] | [<b>rsa public</b> | <b>terminal 3des</b> <i>&lt;LINE&gt;</i> | <b>generate</b> [<b>password-cryptkey</b>] | <b>rsa modulus</b> <i>&lt;1024-4096></i> |
[<b>import</b> [<b>client rsa pem</b> | <b>pkcs12 terminal password</b> <i>&lt;LINE&gt;</i>] |</td><td>Configure long term key operations.</td></tr>
<tr><td colspan="2">[<b>flash:</b><i>filename</i>] |
<b>ftp:</b><i>[[//username[:password]@location]/directory]/filename</i> |
<b>http://</b><i>[[username:password]@][hostname | host-ip [directory] /filename</i> |
<b>https://</b><i>[[username:password]@][hostname | host-ip [directory] /filename</i> |
<b>scp:</b><i>[[username@location]/directory]/filename</i> |
<b>sftp:</b><i>[[//username[:password]@location]/directory]/filename</i> |
<b>tftp:</b><i>[[//location]/directory]/filename</i>] |</td></tr>
</table>

[zeroize password-cryptkey | rsa openvpn connection <WORD> | enable | generate secret <NAME> | import ca <NAME> | cert <NAME> | {dh <WORD> | key <NAME> | secret <NAME> |template <NAME>] |	Remove crypto keys.
[terminal | url flash:filename] | ftp:[[//username[:password]@location]/directory]/filename | http://[[username:password]@][hostname | host-ip [directory] /filename | https://[[username:password]@][hostname | host-ip [directory] /filename | scp:[[username@location]/directory]/filename | sftp:[[//username[:password]@location]/directory]/filename | tftp:[[//location]/directory]/filename]|	
[zeroize ca <NAME> | cert <NAME> | key <NAME> | pki import client | https pem | pkcs12} | {openvpn ca <NAME> | cert <NAME> | key <NAME>} | {server test pem | pkcs12] |	Remove crypto keys.
[terminal | url flash:filename | ftp:[[//username[:password]@location]/directory]/filename | http://[[username:password]@][hostname | host-ip [directory] /filename | https://[[username:password]@][hostname | host-ip [directory] /filename | scp:[[username@location]/directory]/filename | sftp:[[//username[:password]@location]/directory]/filename | tftp:[[//location]/directory]/filename] |	
[zeroize [container-registry <WORD> ca cert key | [https] | [openvpn ca <NAME> | cert <NAME> | key <NAME>] | [server <WORD>] |	
radsec ca import <NAME> | cert <NAME> | key <NAME> |	Import or remove Radsec key.
[ssl algorithm encryption any | suite-b-tls | tls-1.2 | tls1.3}	Configure the SSL encryption method.
enable |	Enable Wireguard
[wireguard interface <0-9>] |	Select Wireguard interface ID.

[wireguard private-key 0 ***<WORD>*** **| 7** ***<WORD>*** **|** ***<TEXT>*** **|**	Specify private key value.
[wireguard public-key 0 ***<WORD>*** **| 7** ***<WORD>*** **|** ***<TEXT>***}	Specify public key value.
Command Modes	Perle(config)#crypto

Usage Guidelines

Use this command to configure parameters for IPsec configuration, key, OpenVPN configuration, PKI, and SSL parameters.

Examples

This example exports the public key from the IOLAN to the terminal session.

```
Perle(config)# crypto key export rsa public terminal
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDReknFjyYmPYATixxn1nGVe3xyncwkhA
bKO3JFUI5Vvnd50wT5gYNxd4vP4dJe4J5/mvzG7rcbZ4uCz/
dX8xMs18xUzpoqHbjOF5EUfBtPZzgI/IsDkwzfIaWj/
Qznau6TemWnR72RpzKaDRdFy0j4ghzvfUdXWz/EKPq/
5EJ97sdU97RzURfL8j4IwThanpLVi8kP8guNioYJdFgdrgcerKg6aUTehU7C2X9sai08e
1WNcGA6UrmIzj4rtUsV0Enu+Tx47WM6kcPij423QIM0abnn4RWwRPnU4qINKTvWR
4gKZQUpYEFPvwtJgtpLGDOIYikMvZrc09X1D68Ttbx7
```

Related Commands

show crypto

(config-client)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-client)**
{**[authentication identify** ***<WORD>*** **[pre-shared-key** ***<WORD>*****] | [remote-identity** ***<WORD>*****] | [x509** ***<LINE>*** **| trustpoint** ***<CA-FILE>*****] |**	Configure the local authentication identity.
[connection-type disable | initiate | respond] |	Sets the connection type: ● initiate ● respond ● disable
[ike-group ***<WORD>*****] |**	Configure IPsec IKE configuration.
[local-address [***<A.B.C.D>*** **|** ***<X:X:X:X::X:X>*** **| any] |**	Configure the local address interface.

[tunnel <1-429467295> [esp-group <WORD>] | [local-address <A.B.C.D/N | X:X:X:X::X/N>] | protocol <0-255> | [ah | all | ax.25 | dccp | ddp | egp | eigrp | encap | exp | etherip | fc | ggp | gre | hip | hmp | hopopt | icmp | igp | ip | ipcomp | ipencap | ipip isis | iso--tp4 | l2tp | manet | mobility-header | mpls-in-ip | ospf | pim | pup | rdp | rohc | rspf | rsvp | sctp | skip | st | tcp | tcp -udp | udp | udplite | vmtp | wesp | xns-idp |xtp] | | [remote-address <A.B.C.D/N | X:X:X:X::X/N>]}	Configure the client tunnel parameters.
Command Modes	Perle(config-client)#

Usage Guidelines

Use this command to configure IPSEC parameters.

Examples

This example sets client connection to initiate.

```
Perle(config-client)#connection-type initiate
```

This example sets up the responder side of the connection.

```
Perle(config)#crypto ipsec client @myx509
Perle(config-client)#authentication x509 "C=CA, O=orgxdeb, CN=boxxdeb"
Perle(config-client)#authentication x509 trustpoint "CACert.pem"
Perle(config-client)# connection-type respond
Perle(config-client)# tunnel 0 local-address 192.168.51.111/32
Perle(config-client)# tunnel 0 remote-address 0.0.0.0/0crypto ipsec clinet @myx509
```

Related Commands

show crypto

(config-connection)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-connection)**
{[ca <WORD>] |	Configure the PKI CA trustpoint name.
[cert <NAME>] |	Configure the PKI certificate name.

[cipher aes-128-cbc | aes-128-gcm | aes-192-cbc | aes-192-gcm | aes-256-cbc | aes-256-gcm | bf-cbc | camellia-128-cbc | camellia-192-cbc | camellia-256-cbc | cast5-cbc | des-cbc | des-ede-cbc | des-ede3-cbc | des-cbc | rc2-40-cbc | rc2-64-cbc | rc2-cbc | seed-cbc] |	Configure the cipher for this connection.
[client] |	Enables client mode if TCP mode is used with the remote command or if you receive the OpenVPN message "Options error: --proto tcp is ambiguous in this context. Please specify --proto tcp-server or --proto tcp-client
[client-to-client] |	Sets client to client mode for the connection. This lets connected clients see each other, not just the server.
[comp-lzo [adaptive | no | yes] |	Configure compression. In cases where the OpenVPN server pushes the request "comp-lzo no" to connecting clients, the client side breaks with repeated "write to TUN/TAP : Invalid argument (code=22)" errors unless it too has already specified "comp-lzo no. **Note:** the "no comp-lzo" (the default) turns off the entire compression subsystem which is required for connections not using compression.
[dev *<0-999>*] |	Configure the OpenVPN interface number.
[dh *<WORD>*] |	Configure Diffie-Hellman parameters.
[ifconfig *<A.B.C.D> <WORD> <A.B.C.D> <WORD>*] |	Configure the local and the remote IP addresses for each side of the connection. Reverse the ip addresses when configuring "the other end".
[keepalive *<1-65535> <1-65535>*] |	Configure the keepalive interval (in seconds) and the keepalive timeout (in seconds).
[key *<WORD>*] |	Configure the PKI private key.
[lport *<1-65535>*] |	Configure the port on the local side. Default is 1194
[persist-tun] |	Keeps tun device between restarts.
[port *<1-65535>*] |	Configure the port on both sides of the connection.
[pull] |	Downloads the configuration from the server.

[remote [*<A.B.C.D>* **|** *<WORD>* **|** *<X:X:X:X::X> <1-65535>***] | [tcp | udp] |**	Configure the remote host for connection.
[remote-cert-tls client | server] |	Configure peer certificate checking as client or server. When this is used with a TLS connection, the peer's certificate credentials are validated using the CA certificate referred to by the "ca" command. This is recommended to mitigate man-in-the-middle attacks but can be left off if the signing CA certificate is not currently available.
[rport *<1-65535>***] |**	Configure the port on the remote side.
[secret *<NAME>***] |**	Configure the Pre-Shared secret key.
[server *<A.B.C.D> <A.B.C.D>* **[no pool] |**	Configure OpenVPN IPv4 server parameters.
[server-bridge *<A.B.C.D> <A.B.C.D> <A.B.C.D> <A.B.C.D>***] |**	Configure the gateway and IP pool addressing.
[server-ipv6 *<X:X:X:X::X>***] |**	Configure OpenVPN IPv6 server parameters.
[template *<WORD>***] |**	Configure the connection template.
[tls-auth] |	Sets a PSK to use for TLS authentication. The PSK previously defined via crypto openvpn generate secret name will be used. This can be used to add authentication to the TLS control channel to help reduce the chances of a DoS attack.
[tls-client] |	Sets the IOLAN to act as a TLS client.
[tls-server] |	Sets the IOLAN to act as a TLS server.
[user-pass *<WORD> <WORD>* **0 | 7] |**	Configure the remote user name and password.
[user-pass -verify] |	Enables or disables server username and password verification.
[verb *<0-11>***]**}	Configure the verbosity level. (debug)
Command Modes	Perle(config-connection)#

Usage Guidelines

Use this command to configure parameters for OpenVPN connections.

Examples

Configure OpenVPN remote port to 1050.

```
Perle(config-connection)#rport 1050
```

Related Commands

show crypto

(config-esp)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-esp) #**
{[compression] |	Configure compression for the IPsec connection.
[lifetime *<30-86400>*] |	Configure tunnel expire timer after no activity. Range is 30 to 86400 Default is 1800 seconds
[mode transport | tunnel] |	Configure the tunnel mode. **Transport mode**—payload encrypted; headers clear **Transport mode**—both headers and payload encrypted.
[pfs] |	Configure PFS On to improve security by 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 has performance impact but provides further security.
[proposal *<1-65535>* [encryption 3des | aes128 | aes128gcm182 | aes256 | aes256gcm128 | ch]}	Configure the IKE/ESP proposal.
Command Modes	Perle(config-esp)#

Usage Guidelines

Use this command to configure IPsec parameters.

Examples

Configure esp group mode to transport.

```
Perle(config-esp)# mode transport
```

Related Commands

show crypto

(config-ike)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-ike) #
{[aggressive-mode] |	Enables or disables aggressive mode. Aggressive mode uses fewer packet exchanges, therefore it is faster then main mode. However, 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). You must use aggressive mode if one or both peers have dynamic external IP addresses or if you use Network Address Translation Traversal (NAT-T) Default is Off
[close-action] |	Configure the action to take if an unexpected peer connection is closed. ● **Clear**—terminate the VPN connection. You must manually re-initiate the VPN connection. We recommend that you use Clear when the remote peer uses dynamic IP address ● **Hold**—traffic from your local network to the remote network can trigger the IOLAN to re-initiate the VPN connection. We recommend that you use Hold when the remote peer uses a static IP address ● **Restart**—re-initiate the VPN connection ● **None**—Do not take any action
[dpd action clear] |	Configure Dead Peer Detection (DPD). This 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. ● **Clear**—terminate the VPN connection over the detection timeout. You must manually re-initiate the VPN connection. We recommend that you use Clear when the remote peer uses dynamic IP address ● **Hold**—traffic from your local network to the remote network can trigger the 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

[dpd action restart] |	- **Restart**—re-initiate the VPN connection. Default Action is Hold Interval is 30 seconds Timeout is 120 seconds
[interval *<2-86400>*] |	Dpd interval.
[timeout *<10-86400>*] |	Dpd timeout.
[ike-version ike | ikev1 | ikev2] |	Configure the IKE version. IKE uses IKEv2 but switches to IKEv1 depending on the peer. Default is IKEv2
[lifetime *<30-86400>*] |	Configure the connection keep alive timer. Range is 30 to 86400 Default is 3600 seconds
[proposal [dh-group 2 | 5 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26] | [encryption 3des | aes128 | aes128gcm128 | aes256 | aes256gcm256]}	Configure the IKE/ESP proposal. Dh-default is 2 Encryption default is aes256 Hash default is SHA1
Command Modes	Perle(config-ike)#

Usage Guidelines

Use this command to configure IKE parameters.

Examples

Configures dead peer detection to restart.

```
Perle(config-ike)# dpd action restart
```

Related Commands

show crypto

(config-12tp)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-l2tp)
{client-ip-pool *<A.B.C.D> <A.B.C.D>* |	Configure L2TP client IP pool addresses to be used by the clients.
dns-server *<1-2> <A.B.C.D>* |	Configure L2TP DNS servers.
outside-address *<A.B.C.D>* |	Configure the IP address to bind to.
pre-shared-key *<WORD>* |	Configure the given pre-shared secret.

username ***<WORD>*** **password** ***<WORD>***}	Configure L2TP user name and password for this connection.
Command Modes	Perle(config-l2tp)#

Usage Guidelines

Use this command to configure L2TP connection parameters.

Examples

Configure user name and password for L2TP connection.

Perle(config-l2tp)#username lyn password test

Related Commands

show crypto

(config-wg0)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-wg0)**
[address ipv4 ***<A.B.C.D> <A.B.C.D>*** **| ipv6** ***<X:X:X:X::X/2-128>*** **|**	Configure the IPv4 or IPv6 address for the Wireguard interface.
[crypto wireguard interface ***<0-9>*****] |**	Change Wireguard interface.
[description ***<TEXT>*****] |**	Configure the description for this Wireguard interface.
[peer ***<TEXT>*****] |**	Specify a Wireguard peer name.
[port ***<1-65535>*** **|**	The Wireguard VPN will use this port for communication. Default UDP port is 51820
Command Modes	Perle(config-wg0)#

Usage Guidelines

Use this command to configure Wireguard parameters.

Examples

This example sets address of 172.16.77.55 to this Wireguard interface.

Perle(config-wg0)#address 172.16.77.55 255.255.0.0

Related Commands

show crypto

(config-wg0-test)

(config-wg0-test)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-wg0-test)
[address ipv4 ***<A.B.C.D>*** **|** ***<Host and Domain-name>*** **| ipv6** ***<Host and Domain-name>*** **|** ***<X:X:X:X::X/2-128>*** **|**	Configure Wireguard peer address.
[allowed-ips [*<A.B.C.D>* | *all*] | ipv6 [*<X:X:X:X::X.* | *all>*] |	Add the address/s of the peers that can use this Wireguard interface or select all.
[crypto wireguard interface ***<0-9>*** **] |**	Change Wireguard interface.
persistent-keepalive ***<1-65535>*** **|**	Persistent keepalive–in seconds (between 1-65535). How often to send an authenticated empty packet to the peer for the purpose of keeping a state full firewall or NAT mapping valid persistently. If the interface rarely sends traffic, but at anytime at anytime recieve traffic from a peer, and it is behind NAT, the interface might benefit from having a persistent keepalive interval of 25 seconds. Default 0 - this option is disabled
[port ***<1-65535>*** **|**	The Wireguard VPN will use this port for communication.
Command Modes	Perle(config-wg0-test)#

Usage Guidelines

Use this command to configure Wireguard parameters.

Examples

This example adds peer IPv4 address 172.16.88.99 to the Wireguard interface for communications.

```
Perle(config-wg0-test)#allowed-ips  172.16.88.99
```

Related Commands

show crypto

(config-wg0)

dot1x

Use the no form of this command to negate a command or set to defaults.

Syntax Description	dot1x
{**[credential** ***<WORD>*** **] |**	Configure a dot1x credential profile.
[logging] |	Logs dot1x messages

[system-auth-control] |	Enables dot1x system-auth-control fort 802.1x access control on any port on the IOLAN. Set the port control command on each specific port you want 802.1x access control.
[test timeout *<1-65535>*}	Use the readiness check before 802.1x is enabled on the IOLAN. Configure the EAPOL device timeout for the specified time frame.
Command Modes	Perle(config)#dot1x

Usage Guidelines

Use this feature to determine if connected devices are 802.1x-capable.

Examples:

This example creates a credential profile testcrd, Enable dotx1 authentication on Ethernet interfaces for multihost.

Note: You must enable system -auth-control if you want to authenticate dot1x devices.

```
Perle(config)#dot1x credential testcred
Perle(config)#interface ethernet 1
Perle(config-if)#authentication mult-auth
```

Related Commands

(config-dot1x-creden)

show eee

(config-dot1x-creden)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-dot1x-creden)**
{**password** < *0* > *<LINE>* | *<7>* *<LINE>* |	Configure a password. 0–specifies that an unencrypted password follows. 7–specifies that an hidden password follows.
username *<WORD>*}	Configure a user name.
Command Modes	Perle(config-dot1x-creden)#

Usage Guidelines

Use this command to configure dot1x credentials.

Examples

This example configures the password "testing" to an encrypted password.

```
Perle(config)#dot1x credential testing
Perle(config-dot1x-creden)# password 7 DB0UeI1lynwOKW/j1
```

Related Commands

show eee

eap

Use the no form of this command to negate a command or set to defaults.

Syntax Description	eap
{**profile** *<WORD>*}	Configure EAP profiles.
Command Modes	Perle(config)#eap

Usage Guidelines

Use this command to create EAP profiles.

Related Commands

show eap

(config-eap-profile)

(config-eap-profile)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-eap-profile)
{**method gtc | leap | md5 | mschapv2 | peap | tls | [ttls chap | eap-gtc | eap-md5 | eap-mschapv2 | mschap | mschapv2 | pap] |**	Configure the method of encapsulating sensitive information such as passwords to be authenticated from the IOLAN. The certificate authority you must trust. This is a self-signed certificate that you create here *eap*
pki-trustpoint *<WORD>*}	Configure the default pki trustpoint.
Command Modes	Perle(config-eap-profiles)#

Usage Guidelines

Use this command to configure parameters for EAP profiles.

EAP defines the transport and usage of identity credentials. EAP encapsulates the user names, passwords, certificates, and tokens for client authentication.

A trustpoint is a certificate authority you trust. Your IOLAN automatically trusts any other certificates signed with that trusted certificate

Create an eap profile before setting these parameters.

Examples

This example sets the method to gtc.

```
Perle(config-eap-profiles)#method gtc
```

Related Commands

show eap

email

Use the no form of this command to negate a command or set to defaults.

Syntax Description	email
{**enabled**] |	Enables the email feature.
[encryption none | ssl | tls] |	Configure encryption. - none - ssl - tls
[from *<WORD>*] |	Configure from parameter. Format is user@company.com
[recipient *<WORD>* | **enable notifications-subject** *<LINE>* | **notifications alarms | authentication | bgp | bridge | entity | envmon | interface-ip | ipsec | lldp | network-watchdog | openvpn | osfp | smnp | software-update] |**	Configure the recipient and receive notifications Format is: user@company.com Specify the email notifications. - alarms, authentication, bgp, bridge, dot11, entity, envmon, interface-ip, ipsec, lldp, network-watchdog, openvpn, ospf, snmp, software-update
[smtp-server *<WORD>* | *<A.B.C.D>* | *<X:X:X:X::X:X>*] |	Configure the SMNP server for mail requests.
[username *<WORD>* | **password 0** *<LINE>* | **7** *<WORD>* | *<LINE>*] |	Configure the username for server authentication.
[validate-certificate}	Configure the validation email certificate.
Command Modes	Perle(config)#email

Usage Guidelines

Use this command to configure email notification parameters.

Examples

This example enables the email feature and configures the smnp server for email requests.

```
Perle(config)#email enabled
Perle(config)#email snmp-server 172.16.55.77
```

Related Commands

show email

enable

Use the no form of this command to negate enable secret.

Syntax Description	enable
{secret 0 *<LINE>* | 5 *<LINE>* | *<LINE>*}	Configure the enable password. 0—Specifies an unencrypted password to follow 5—Specifies a encrypted password to follow LINE—the unencrypted (cleartext) secret
Command Modes	Perle(config)#enable

Usage Guidelines

Use this command to configure the password to be used to enable privilege mode.

Examples

This example configures a password for enable mode.

```
Perle(config)#enable secret testsecret
```

hostname

Use the no form of this command to negate a command or set to defaults.

Syntax Description	hostname
{*<WORD>*}	Configure the IOLAN name.
Command Modes	Perle(config)#hostname

Usage Guidelines

Use this command to configure the IOLAN's hostname.

Examples

This example configures the IOLAN's name to TestHost.

```
Perle(config)#hostname TestHost
TestHost(config)#
```

interface

Use the no form of this command to negate a command or set to defaults.

Syntax Description	interface
{[bvi *<1-9999>*] |	Configure the bridge interface. See *(config-if)#*

[dialer *<0-15>*] |	Configure the dialer interface. See ***(config-if)#cellular***
[ethernet *<1-x>.<1-4000>*] |	Configure the Ethernet interface. See ***(config-if-ethernet)#*** <1-x> = maximum number of ethernet ports, (depends on the model)
[openvpn-tunnel *<0-999>* tap | tun] |	Configure an OpenVPN tunnel. See ***(config-if)#openvpn-tunnel***
[tunnel *<0-999>*] |	Configure the tunnel. See ***(config-if)#tunnel***
[range ethernet *<1-x>*}	Configure an Ethernet range. See ***(config-if-range)#*** <1-x> = maximum number of ethernet ports, (depends on the model) SFP values 1-x (depends on the model)
Command Modes	Perle(config)#interface ethernet 1 Perle(config-if)#

Usage Guidelines

Use this command to configure an interface.

Examples

This example configures parameters for Ethernet interface 1.

```
Perle(config)#interface ethernet 1
```

Related Commands

(config-if)#

(config-if)#cellular

(config-if)#openvpn-tunnel

(config-if)#tunnel

(config-if-range)#

(config-subif)#

(config-if-vrrp)#

ip access-list

Use the no form of this command to negate enable.

Syntax Description	**ip access-list**
{**[extended *<100-199>* | *<2000-2699>*] |**	Configure an IP access list number. See ***(config-ext-nacl)***

[resequence extended ***<100-199><1-65535>* | *<2000-2699> <1-65535>*] |** **standard** ***<1-99> <1-65535> <1300-1999> <1-65535>*] |**	Configure resequence IP Access list. Entries are numbered sequentially, starting from 10 and in intervals of 10.
[standard ***<1-99>* | *<1300-1999>*}**	Configure an IP access list number. See ***(config-std-nacl)***
Command Modes	Perle(config)#ip access-list

Usage Guidelines

Use IP Access Control Lists (ACLs) to define rules for controlling the network traffic and reducing network attacks. You can filter traffic based on sets of rules defined for the incoming traffic or outgoing traffic. Access lists look from the top list entry to bottom list entry.. Be sure when creating access lists that the most important entries are at the top of the list.

Examples

Displays ACL definitions. You will note that there is no available space to add an entry within this list. Using the resequence command you can resequence these ACL entries.

```
Standard IP access list Moo.
10 deny host 1.1.1.1
20 deny host 2.2.2.2
30 permit 3.3.3.3
40 permit 4.4.4.4
```

To resequence this ACL list to start at 20 and then resequence each entry by 20's use:

```
Perle(config)#ip access-list resequence Moo 20 20
Standard IP access list Moo.
   20 deny host 1.1.1.1
   40 deny host 2.2.2.2
   60 permit 3.3.3.3
   80 permit 4.4.4.4
```

You now have space between the entries to add entries.

Note: Resequence numbering is lost on a reboot, therefore you must copy running-config to startup-config for these changes to be permanently saved.

Related Commands

(config-std-nacl)

(config-ext-nacl)

(config-std-nacl)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-std-nacl)**

{***<1-2147483647>*** **deny | permit** ***<A.B.C.D>/hostname> <A.B.C.D>/ hostname>*** **| any | host*****<A.B.C.D>/ hostname>***}	Configure standard access lists.
Command Modes	Perle(config-std-nacl)#

Usage Guidelines

Configure packets to reject or accept.

Examples

This example permits packets from this host.

```
Perle(config-std-nacl)#permit host 172.16.77.88
```

(config-ext-nacl)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-ext-nacl)**
{***<1-65535>*** **|** {**deny ip | permit ip** ***<A.B.C.D>/ hostname> <A.B.C.D>/ hostname>*** **| any | host** ***<A.B.C.D>/hostname>***}	Configure sequence numbers and permits or denies packets.
Command Modes	Perle(config-ext-nacl)#

Usage Guidelines

Configure sequence number and define packets to permit or deny.

Examples

This example permits packets from source host 172.16.77.88 and destination host any (host).

```
Perle(config-ext-nacl)#permit ip host 172.16.77.88 any
```

ip alg

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**ip alg**
{**alg modules ftp | gre | h323 | nfs | pptp | sip | sqlnet | tftp | disable**}	Configure Application Level Gateway (ALG) modules. **Some parameters may not be available on some firmware versions or models.**
Command Modes	Perle(config)#ip alg

Usage Guidelines

Use this command to configure client applications to communicate with known ports used by server applications. ALG allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for protocols such as FTP, BitTorrent, SIP, RTSP, and file transfer etc. In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (firewall pinhole) dynamically as required. Application data is passed through the security checks of the firewall or NAT that would have otherwise been restricted. Without an ALG, the ports would either get blocked, or the network administrator would need to open up a large number of ports in the firewall, weakening the network and allowing potential attacks on those ports.

By default all alg modules are enabled.

Examples

This example disables ALG module ftp.

```
Perle(config)#no ip alg modules ftp disable
```

ip as-path

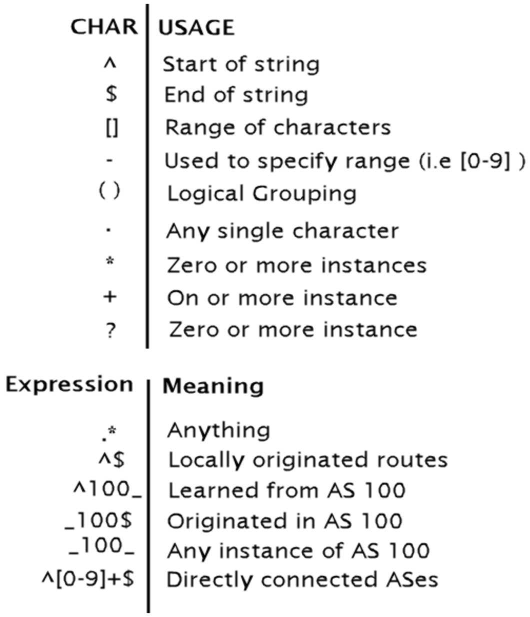
Use the no form of this command to negate a command or set to defaults.

Syntax Description	**ip as-path**
{**as-path access-list** ***<WORD>*** ***<1-65535>*** **deny | permit** ***<LINE>***}	Configure access list parameters.
Command Modes	Perle(config)#ip as-path

Usage Guidelines

Use this command to configure an access-list filters for Border Gateway Protocol (BGP) autonomous system (AS) numbers. You can use AS Path filters, either inbound or outbound, to filter either the routes you send or the routes you receive, respectively. You must apply these filters to each peer separately. Regular expressions are strings of special characters used to search and find character patterns.

Regular expression for *<LINE>* include:



CHAR	USAGE
^	Start of string
$	End of string
[]	Range of characters
-	Used to specify range (i.e [0-9])
( )	Logical Grouping
.	Any single character
*	Zero or more instances
+	On or more instance
?	Zero or more instance

Expression	Meaning
.*	Anything
^$	Locally originated routes
^100_	Learned from AS 100
_100$	Originated in AS 100
_100_	Any instance of AS 100
^[0-9]+$	Directly connected ASes

Examples

This example accepts prefixes that originated in AS 3299, all other prefixes won't be permitted.

Perle(config)#ip as-path access-list 1 permit ^3299$

Related Commands

(config-remote-mgmt)

show ip as-path-access-list

ip community-list

Use the no form of this command to negate a command or set to defaults.

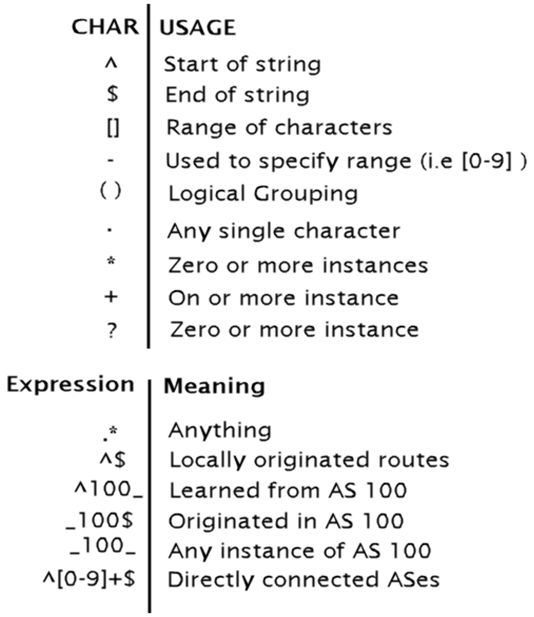
Syntax Description	ip community-list
{**expanded** *<100-500> <1-65535>* **deny** *<LINE>* | **permit** *<LINE>*] |	Configure an extended community list.You can configure up to 32 communities.
[standard *<1-99> <1-65535>* **deny** *<1-4294967295>* | **internet** | **local-as** |**no-advertise** | **no-export** | **permit** *<1-4294967295>* | **internet** | **local-as** | **no-advertise** | **no-export** | **permit** *<LINE>*]}	Configure a standard community list. You can configure up to 16 communities.
Command Modes	Perle(config)#ip community-list

Usage Guidelines

Use this command to configure a BGP community list and to control which routes are permitted or denied based on their community values.

Standard community lists are used to configure well-known communities and specific community numbers. You can pick more than one of the optional community keywords.

Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes



CHAR	USAGE
^	Start of string
$	End of string
[]	Range of characters
-	Used to specify range (i.e [0-9])
( )	Logical Grouping
.	Any single character
*	Zero or more instances
+	On or more instance
?	Zero or more instance

Expression	Meaning
.*	Anything
^$	Locally originated routes
^100_	Learned from AS 100
_100$	Originated in AS 100
_100_	Any instance of AS 100
^[0-9]+$	Directly connected ASes

Examples

This example configures a standard community list that denies routes that carry communities from network 40 in autonomous system 65540 and from network 60 in autonomous system 65550. This example shows a logical AND condition; all community values must match in order for the list to be processed.

Perle(config)#ip community-list standard test1 deny 65540:40 65550:60

Related Commands

router

ip default-gateway

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**ip default-gateway**
{**default-gateway** ***<A.B.C.D>***}	Configure the IP address of the default gateway.
Command Modes	Perle(config)#ip default-gateway

Usage Guidelines

Use this command to configure a default gateway.

Examples

This example configures a gateway address of 172.16.1.1.

```
Perle(config)#ip default-gateway 172.16.1.1
```

ip dhcp

Use the no form of this command to negate a command or set to defaults.

Syntax Description	ip dhcp
{[**dhcp excluded-address** *<A.B.C.D>* | **pool** *<NAME>*] |	Configure Dynamic Host Configuration Protocol (DHCP) to exclude an address range. Configure DHCP pools.
[**relay information hop-count** *<1-255>* | **packet-size** *<64-1400>* | **policy drop** | **encapsulate** | **keep** | **replace** | **port** *<1-655535>* | **server** *<A.B.C.D>*]}	Configure Relay Agent parameters. **Some parameters may not be available on some firmware versions or models.**
Command Modes	Perle(config)#ip dhcp

Usage Guidelines

Use this command to have the DHCP server automatically assign an IP address and other IP parameters to devices on your network.

Examples

This example excludes ip address 172.16.55.99 from the DHCP pool.

```
Perle(config)#ip dhcp exclude address 172.16.55.99
```

Related Commands

(config-dhcp)

(config-dhcp)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-dhcp)
{[**address** *<A.B.C.D>* **hardware-address** *<H.H.H>*] |	Configure the IP address to reserve for this client. This IP address is only assigned to the client with this hardware address.

[authoritative enable] |	Configure the authoritative parameter. This parameter must be set to enable if this is the only DHCP server on your network. Authoritative mode allows roaming clients to get a new DHCP address even if their lease has been assigned from another network and is still valid (lease has not expired) This prevents a client lock out situation.
[bootfile *<FILENAME>*] |	Configure the IP address or name of a TFTP server and boot file name to allow client auto-configuration.
[default-router *<A.B.C.D>*] |	Configure the default router to use after a DHCP client has booted. The IP address of the default router should be on the same subnet as the client.
[description *<POOL_NAME>*] |	Configure DHCP pool name description.
[dns-server *<A.B.C.D>*] |	Configure a DNS server for use by clients using this DHCP pool. A DNS server needs to be specified if you want to browse the Internet.
[domain-name *<A.B.C.D>*] |	Configure a domain name.
[enable] |	Enables this dhcp pool.
[lease *<0-365> <0-23> <0-59>* | infinite] |	Configure a lease time for client connecting using this DHCP pool. Typically 24 lease times are suitable, however if your situation is a public hotspot then shorter time be warranted.
[network *</nn | A.B.C.D>* start *<A.B.C.D>* stop *<A.B.C.D>*] |	Configure the network, start and stop IP addresses for DHCP lease ranges.
[option ascii *<string>* | hex *<hex-string>* | ip *<A.B.C.D>*] |	Configure DHCP options to send to the client.
[static-route *<A.B.C.D> <A.B.C.D> <A.B.C.D>*]}	Configure a static route.
Command Modes	Perle(config-dhcp)#

Usage Guidelines

Use this command to configure DHCP parameters.

Examples

This example sets authoritative mode to enable.

```
Perle(config-dhcp)#ip authoritative enable
```

Related Commands

ip dhcp

ip dns

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**ip dns**
{**[dns cache-size** *<1-10000>***] |**	Configure the size of the DNS cache. Values are 1 to 10000 Default is 10000
[domain *<NAME>* **server** *<A.B.C.D> <X:X:X:X::X>***] |**	Configure the domain name to forward to a custom DNS server.
[ignore-hosts-file] |	Configure the parameter—Do not use the local /etc/hosts file for name resolution.
[listen-address *<A.B.C.D> <X:X:X:X::X>***] |**	Configure the parameter to listen for DNS addresses on the following IP addresses.
[negative-ttl *<0-7200>***]**}	Configure the seconds to cache NXDOMAIN entries. Values are 0–7200 seconds Default is 3600 seconds
Command Modes	Perle(config)#ip dns

Usage Guidelines

Use this command to configure parameters for DNS.

Examples

This example sets listen address to 172.16.77.88.

```
Perle(config)#ip dns listen-address 172.16.77.88
```

Related Commands

ip domain

ip domain-name

ip domain

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**ip domain**
{**domain lookup**}	Enables DNS host name to IP address translation.
Command Modes	Perle(config)#ip domain

Usage Guidelines

Use the ip domain-lookup command to enable DNS host name-to-IP address translation on the IOLAN.

Examples

This example enables DNS host to IP address translation.

```
Perle(config)#ip domain
```

Related Commands

ip domain-name

ip domain-name

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**ip domain-name**
{**domain-name** *<WORD>*}	Configure the domain name.
Command Modes	Perle(config)#ip domain-name

Usage Guidelines

Use this command to configure the default domain name.

Examples

This example sets domain name to testlab.

```
Perle(config)#ip domain-name testlab
```

Related Commands

ip domain

ip drmgrd

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**ip drmgrd**
{**[drmgrd server]**}	Enable or disable drmgrd (PerleView daemon).
Command Modes	Perle(config)#ip drmgrd

Usage Guidelines

Use this command to enable or disable the PerleView daemon.

Default is PerleView daemon is enabled

Examples

This example disables the PerleView daemon.

```
Perle(config)#no ip drmgrd server
```

ip extcommunity-list

Use the no form of this command to negate a command or set to defaults.

Syntax Description	ip extcommunity-list
{**[extcommunity-list expanded** *<100-500> <1-65535>* **deny** *<LINE>* **| permit** *<LINE>*] |	Configure an extended community list entry.
standard *<1-99> <1-65535>* **deny rt | soo asn:nn**}	Configure a standard community list entry. BGP uses the SoO value associated with a route to prevent routing loops. **rt**—The route target BGP Extended Community dictates the policies used by the Virtual routing and forwarding (VRF). The route target must be configured to specify the routes, which contain this specific route target value, that are imported into the VRF, and the route target that is added to the routes that are exported from the (VRF). **soo**—The site-of-origin (SoO) extended community is a BGP extended community attribute used to identify routes that have originated from a site so that the readvertisement of that prefix back to the source site is prevented.
Command Modes	Perle(config)#ip extcommunity-list

Usage Guidelines

This command defines a new standard extcommunity-list.

Examples

This example configures a standard community list where the routes with this community are advertised to all peers (internal and external).

```
Perle(config)#ip extcommunity-list
```

Related Commands

show ip extcommunity-list

ip firewall

Use the no form of this command to negate a command or set to defaults.

Syntax Description	ip firewall
{**[firewall** *<WORD>*] |	Creates a firewall set of rules. Firewall name cannot be the same as route-policy name.

[all-ping enable] |	Configure the handling of IPv4 ICMP Echo requests. **Enable**—system responses to IPv4 ICMP Echo requests. **Disable**—system does not respond to IPv4 ICMP Echo requests Default is Disabled
[broadcast-ping enable] |	Configure the handling of IPv4 ICMP echo and timestamps requests. **Enable**—system responses to broadcast IPv4 ICMP echo and timestamp requests **Disable**—system does not respond to IPv4 echo and timestamp requests Default is Disabled
[ip-src-route enable] |	Configure the handing of IPv4 packets with source route option. Default is Disabled
[ipv6-receive-redirects enable] |	Configure the handing of received IPv6 ICMP redirect messages. Default is Disabled
[ipv6-src-route] |	Configure the handling of IPv6 packets with routing extension header. Default is Disabled
[log-martians enable] |	Configure the handing of IPv6 packets with routing extension header. Default is Disabled
[receive-redirects enable] |	Configure the handing of received IPv4 ICMP redirect messages. Permits or denies IPv4 ICMP redirect messages. Default is Disabled
[send-redirects enable] |	Configure the sending of IPv4 only redirect messages. Default is enabled
[source-validation disable | loose | strict] |	Configure source validation (IPv4 only). **Disable**—no source validation is performed **Loose**—enable loose reverse path forwarding as defined by RFC3704 **Strict**—enable strict reverse path forwarding as defined in RFC3704 Default is Disabled

[state-policy established accept | drop | reject invalid accept | drop | reject |related action accept | drop | reject] |	Configure the global firewall state policy for both IPv4 and IPv6. By default, the firewall is stateless, configuring any of these options makes the firewall become stateful. ● a firewall state policy is configured
[state-policy established accept | drop | reject invalid accept | drop | reject |related action accept | drop | reject] |	● NAT is configured ● The transport web proxy service is enable ● A load-balancing configuration is enable Default is none (not set)
[syn-cookies enable] |	Configure the policy for using TCP SYN cookies with IPv4. Default is enabled
[twa-hazards-protection enable]}	Configure for TCP TIME_WAIT assassination hazards protection per RFC 1337.
Command Modes	Perle(config)#ip firewall

Usage Guidelines

Use this command to configure firewall global configuration parameters.

Examples

This example configures the IOLAN to answer all incoming ping requests.

```
Perle(config)#ip firewall all-ping enable
```

Related Commands

show ip firewall

clear ip

show ipv6

(config-fw)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-fw)**
{**[default-action accept | drop | reject] |**	Configure the default action for the entire firewall.
[description *<LINE>*] |	Configure firewall rule description.
[enable default-log] |	Enables log packets matching the default-action **Note:** To see logging, turn on kernel debug. <config># debug kernel
[rule *<1-9999>*]}	Configure the number for this rule, then enters sub-menu. (config-fw-rules).

Command Modes	Perle(config-fw)#

Usage Guidelines

Creates a firewall set of rules with the given name.

Examples

This example configures the default log action to enable. See show logging for output.

Perle(config-fw)#enable-default-action

This example create rule 1, then enters sub-menu mode (config-fw-rules).

Perle(config-fw)#rule 1

Perle(config-fw-rules)#

Related Commands

show ip firewall

clear ip

show ipv6

show lldp

(config-fw-rules)

ip firewall

(config-fw-rules)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-fw-rules)
{**[description *<LINE>*] |**	Configure a description for the policy rule.
[disable *<LINE>*] |	Disables policy rule.
[log enabled] |	Enables log packets matching the rule.

Configure firewall rules to match conditions for traffic and the action to be taken if the match conditions are satisfied. Traffic matches on a number of characteristics, including source IP address, destination IP address, source port, destination port, IP protocol, and ICMP type. Rules are executed in sequence, according to the rule number. If the traffic matches the characteristics specified by the rule, the rule's action is executed; if not, the system "falls through" to the next rule.

<table>
<tr><td colspan="2">[match destination address <A.B.C.D> <A.B.C.D> | not <A.B.C.D> <A.B.C.D> start <A.B.C.D> stop <A.B.C.D> port <A.B.C.D> <A.B.C.D> | not <A.B.C.D> <A.B.C.D> start <A.B.C.D> stop <A.B.C.D> | fragment | non-fragment | icmp type <0-255> code <0-255> | type-name tos-host-redirect | tos-network-redirect | address-mask-reply |address-mask-request | communication-prohibited | destination-unreachable | echo-reply | echo-request | fragmentation needed | host-precedence-violation | host-redirect | host-unknown | host-unreachable | network-redirect | network-unknown | parameter-problem | port-unreachable | protocol-unreachable | redirect | required-option-missing | router-advertisement | router-solicitation | source-quench | source-route-failed | time-exceeded | timestamp-reply | timestamp-request | ipsec | non-ipsec | protocol <0-255> | ah | dccp | dsr | egp | eigrp | encap | esp | etherip | ggp | gre | hmp | icmp | idpr | igmp | igp | ip | ipip | ipv6 | ipc6-frag | ipv6-icmp | ipv6-nonxt | ipv6-opts | ipv6-route | isis | l2tp | manet | mpls-in-ip | narp | pim | rdp | roch | rvsp | sctp | shim6 | skip | tcp | udp | udplite | vrrp | xns-idp || recent count <1-255> | time <1-4294967295> | source address <A.B.C.D> <A.B.C.D> not <A.B.C.D> <A.B.C.D> start <A.B.C.D> stop <A.B.C.D> | mac-address <H.H.H> not <H.H.H> | port <1-65535> not <1-65535> start <1-65535> stop <1-65535> | state estabished | invalid | new | related | tcp-flags ack | all | fin | sh | rst | syn | urg | not] |</td></tr>
<tr><td>[set action accept | drop | reject] |</td><td>Action for packets.
The action is one of the following:
• Accept—Traffic is allowed and forwarded.
• Drop—Traffic is silently discarded.
• Reject—Traffic is discarded with an ICMP “Port Unreachable” message.
• Inspect—Traffic is processed by the intrusion protection system (IPS).</td></tr>
<tr><td>[time monthdays <1-31> not <1-31> | startdate january | february | march | april | may | june | july | august | september | november | december day <1-31> year <2001-2037> | starttime <hh:mm:ss>| stopdate january | february | march | april | may | june | july | august | september ||november | december | stoptime <hh:mm:ss> | utc | weekdays monday | tuesday | wednesday | thursday | friday saturday | sunday | not monday | tuesday | wednesday | thursday | friday | saturday | sunday]}</td><td>Configure time schedule to match rules.</td></tr>
</table>

Command Modes	Perle(config-fw-rules)#

Usage Guidelines

Use this command to create firewalls filter packets on interfaces.

There are two steps to create a firewall.
1. You define a firewall instance and save it under a name. A firewall instance is also called a firewall rule set, where a rule set is just a series of firewall rules. You define the firewall instance and configure the rules for its rule set in the firewall configuration node.

2 After defining the instance and specifying the rules in the rule set, you apply the instance to an interface or a zone. You do this by configuring the interface configuration node for the interface or zone. Once the instance is applied to the interface or zone, the rules in the instance begin filtering packets.

Examples

The example below applies firewall name set test to the inbound traffic on BV1 (bridging eth1 and eth2). This firewall drops all ICMP traffic (generated by ping commands), but allows all other traffic such as TCP Web traffic) because the default action is accept.

```
Perle(config)#ip firewall test
Perle(config-fw)#default-action accept
Perle(config-fw)#rule 1
Perle(config-fw-rules)#set action drop
Perle(config-fw-rules)#match protocol icmp
Perle(config-fw)#rule 2
Perle(config-fw-rules)#set action accept
Perle(config-fw-rules)#match protocol tcp
Perle(config)#interface ethernet 1
```

```
Perle(config)#bridge-group 1
Perle(config)#interface ethernet 2
Perle(config)#bridge-group 1
```

Related Commands

show ip firewall

clear ip

show ipv6

(config-fw)

ip ftp

Use the no form of this command to negate a command or set to defaults.

Syntax Description	ip ftp
{**ftp passive | password 0** ***<LINE>*** **| 7** ***<WORD>*** **|** ***<LINE>*** **| username** ***<WORD>***}	Configure File Transfer Protocol (FTP) parameters. Passive—indicates to the server that the client is opening the file transfer session. This option is used if the client is behind a firewall.

Command Modes	Perle(config)#ip ftp

Usage Guidelines

Use this command to configure File Transfer Protocol (FTP) parameters.

Examples

This example set username to labuser.

```
Perle(config)#ip ftp username labuser
```

ip health

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**ip health**
{**profile** *<WORD>*}	Configure an IP Health Profile. See ***(config-health-prof)*** for more information.
Command Modes	Perle(config)#ip health

Usage Guidelines

Use this command to create a health profile. Health profiles are assigned to interfaces to monitor the heath of that interface.

Examples

This example creates a health profile called labhealth.

```
Perle(config)#ip health profile labhealth
```

Related Commands

(config-health-prof)

show ip health

(config-health-prof)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-health-prof)**
{**failure-count** *<1-10>* | **success-count** | **test target** *<hostname* | *<A.B.C.D>* | **type ping response-timeout** *<1-30>* | **traceroute limit** *<1-254>*}	Test *<1–100>*—Prioritize heath test 1=first. ● Failure test count before marking failed ● Count failure before marking as failed ● Count successes before marking as active ● Configure a health test
Command Modes	Perle(config-health-prof)#

Usage Guidelines

Use this command to configure health tests.

Examples

This example creates a health test to ping host 172.16.77.4 10 times

```
Perle(config-health-prof)#test target 10 172.16.77.4
```

ip host

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**ip host**
{**host** *<WORD> <A.B.C.D>*}	Configure a host to add to the host table.
Command Modes	Perle(config)#ip host

Usage Guidelines

Use this command to add a host to the IOLAN's internal host table.

Examples

This example adds host labhost with ip address of 172.16.99.10 to the host table.

```
Perle(config)#ip host labhost 172.16.99.10
```

Related Commands

show hosts

ip host-group

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**ip host-group**
{**host** *<WORD>*}	Configure the host group name.
Command Modes	Perle(config)#ip host

Usage Guidelines

Use this command to create a host group. A host group is a list of hosts.

Examples

This example creates host group hosts_for_labs.

```
Perle(config)#ip host-group hosts_for_labs
```

Related Commands

(config-host-group)

(config-host-group)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-host-group)
{**host** *<A.B.C.D>* | *<WORD>* | *<X:X:X:X::X>*}	Configure a host to add to the host group.

Command Modes	Perle(config-host-group)#

Usage Guidelines

Use this command to add a host to the host group.

Examples

This example adds host 172.17.55.90 to host group.

Perle(config-host-group)#host 172.17.55.90

Related Commands

ip host-group

ip http

Use the no form of this command to negate a command or set to defaults.

Syntax Description	ip http
{**accounting exec** *<WORD>* | **default]** |	Configure HTTP server accounting parameters.
[authentication aaa login-authentication *<WORD>* | **default]** |	Configure HTTP server authentication method.
[client password 0 *<LINE>* | **7** *<WORD>* | *<LINE>* **proxy-server** *<WORD>* **proxy-port** *<1-65535>* | **secure-trust-point** *<WORD>* | **username** *<WORD>* | **verify-server]** |	Configure HTTP client certificate secure trustpoint.
[local port *80* | *<1025-65535>***]** |	Configure a HTTP server local port number for listening. Values are 1025 to 65535 Default is 80
[secure-port *443* | *<1025-65535>***]** |	Configure a HTTPS server port for listening. Values are 1025 to 65535 Default is 4430
[secure-server] |	Enable HTTP secure server.

[server] |	Enable HTTP server.
[session-idle-timeout ***<1-1440>*****]**}	Configure a HTTP server session idle timeout. Default session idle timeout is 1440 seconds.
Command Modes	Perle(config)#ip http

Usage Guidelines

Use this command to configure HTTP/S server parameters.

Examples

This example enables HTTP secure server.

```
Perle(config)#ip http secure-server
```

Related Commands

show ip http

ip local-route

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**ip local-route**
{**rule** ***<1-32765>***}	Configure the rule number. Values 1-32765
Command Modes	Perle(config)#ip local-route

Usage Guidelines

Use this command to configure an ip local route policy.

Examples

This example creates a ip local route rule 3.

```
Perle(config)#ip local-route rule 3
```

(config-local-rules)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-local-rules)#**
{**[match destination address** ***<A.B.C.D> <A.B.C.D>*** **| [inbound-interface [bvi** ***<1–9999>*****] | [cellular** ***<0–0>>*****] | [dialer** ***<0–15>*****] | [ethernet** ***<1-x>*****] | [sfp** ***<1-x>*****] | [openvpn-tunnel** ***<0–999>*****] | [tunnel** ***<0–999>*****] [source address** ***<A.B.C.D> <A.B.C.D>*****]**}	Specify match values for destination, inbound interface and source.

[set table *<1-200>* | [main] |	Specify the routing table or main routing table.
Command Modes	Perle(config)#ip local-route

Usage Guidelines

Configure local route policy parameter.

Examples

Perle(config-local-rules)#lset table main

Related Commands

ip local-route

ip name-server

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**ip name-server**
{**name-server *<A.B.C.D>***}	Configure the address of the name server.
Command Modes	Perle(config)#ip name-server

Usage Guidelines

Use this command to configure the nameserver. Nameserver is a server that handles queries regarding the location of a domain name’s various services such as website, emails and so on. It is also a part of the Domain Name System (DNS) which maintains a directory of domain names and translate them to IP addresses. When you visit a domain, a DNS lookup first checks its name servers and reviews the DNS records for that domain accordingly.

Examples

This example set name-server to 172.16.44.55.

Perle(config)#ip name-server 172.16.44.55

ip nat

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**ip nat**
{**nat [inside source any | list *<1-199>* interface bvi *<1-9999>* | cellular *<0-0>* | dialer *<0-15>* | dot11radio *<0-4>* | ethernet *<1-5><1-24>* | openvpn *<0-999>* | tunnel *<0-999>*] |**	Configure Network Address Translation (NAT). Inside source address.
[over load | no-strict] |	

[pool *<WORD>* outbound bvi *<1-9999>* | cellular *<0-0>* | dialer *<0-15>* | dot11radio *<0-4>* | ethernet *<1-5><1-24>* | openvpn *<0-999>* | tunnel *<0-999>* no-strict] |	Specify the pool to use for this interface.
[outside destination static ip [*<A.B.C.D> <A.B.C.D>* inbound-interface bvi *<1-9999>* | cellular *<0-0>* | dialer *<0-15>* | dot11radio *<0-4>* | ethernet *<1-5><1-24>* | openvpn *<0-999>* | tunnel *<0-999>*] |	Outside destination address.
[local-pool *<WORD>*] |	**Local pool**–define the local pool
[global-pool *<WORD>*] |	**Global pool**–define the global pool **Note:** Global address pools cannot have overlapping addresses between multiple pools
[address-mapping [persistent | random] |	**Address mapping** • **Random mode**–translation address is computed based on source and destination addresses of incoming packets on every connection • **Persistent mode**–translation address is computed based on source address of incoming packets on the first connection, and will be persistent for each connection there after Default translation mode is random
[inbound-interface bvi *<1-9999>* | cellular *<0-0>* | dialer *<0-15>* | dot11radio *<0-4>* | ethernet *<1-5><1-24>* | openvpn *<0-999>* | tunnel *<0-999>*] |	
[tcp | tcp+udp | udp *<A.B.C.D> <1-65535>*] |	
[inbound-interface bvi *<A.B.C.D> <1-9999>* | cellular *<0-0>* | dialer *<0-15>* | dot11radio *<0-4>* | ethernet *<1-5><1-24>* | openvpn *<0-999>* | tunnel *<0-999>*] *<1-65535> <A.B.C.D> <A.B.C.D>*] |	

[pool <*WORD*> <*A.B.C.D*> <*A.B.C.D*> netmask <*A.B.C.D*>]}	Define DHCP address pool.
Command Modes	Perle(config)#ip nat

Usage Guidelines

One to One:

Use Source Network Address Translation (SNAT) to allow multiple host inside the network to reach a host outside the network.

One to Many:

Use Destination Address Translation (DNAT) to allow multiple hosts outside the network to reach a single host inside the network.

Examples

This example allows all local traffic to the Internet through ethernet port 1.

First you need to create an access-list, then you need to assign NAT.

Perle(config)#ip access-list standard 1

Perle(config-std-nacl)#permit any

Perle(config)#ip nat inside source list 1 interface ethernet 1 overload

Related Commands

show ip nat

ip prefix-list

Use the no form of this command to negate or set to defaults.

<table>
<tr><th>Syntax Description</th><th>ip prefix-list</th></tr>
<tr><td><b>{&lt;<i>WORD</i>&gt; deny &lt;<i>A.B.C.D</i>&gt; &lt;/<i>n</i> | <i>A.B.C.D</i>&gt; ge | le &lt;<i>1-32</i>&gt; | description &lt;<i>LINE</i>&gt; | permit &lt;<i>A.B.C.D</i>&gt; &lt;/<i>n</i> | <i>A.B.C.D</i>&gt; ge | le &lt;<i>1-32</i>&gt; | seq <1-65535> deny &lt;<i>A.B.C.D</i>&gt; &lt;/<i>n</i> | <i>A.B.C.D</i>&gt; ge | le &lt;<i>1-32</i>&gt; | permit &lt;<i>A.B.C.D</i>&gt; &lt;/<i>n</i> | <i>A.B.C.D</i>&gt; ge | le &lt;<i>1-32</i>&gt;}</b></td><td>Configure prefix-list filter.
<b>ge value</b> (optional) Specifies a prefix length greater than or equal to the value. It is the lowest value of a range of the length (the "from" portion of the length range)
<b>le value</b> (optional) Specifiers a prefix length less then or equal to the value. It is the highest value of a range of the length (the "to" portion of the length range.</td></tr>
<tr><td><b>Command Modes</b></td><td>Perle(config)#ip prefix-list</td></tr>
</table>

Usage Guidelines

Use this command to create prefix lists Prefix lists are used in route maps and route filtering operations.The can be used as an alternative to access lists in many routing filtering commands. The most important difference is that a prefix-list allows you to filter networks based on their subnet mask.

Examples

This example shows how to accept a mask length of up to 24 bits in routes with the prefix 172.20.10.171/16.

```
Perle(config)#ip prefix list1 permit 172.20.10.171 /16 le 24
```

This example shows how to permit the prefix 172.17.0.0/16.

```
Perle(config)#ip prefix list2 permit 172.17.0.0 255.255.0.0
```

Related Commands

show ip access-lists

ip radius

Use the no form of this command to negate or set to defaults.

Syntax Description	**ip radius**
{**[source-interface [bvi** *<1-9999>***] | | [dialer** *<0-15>***] | [ethernet** *<1-24>. <1-4000>***] | [openvpn-tunnel** *<0-999>***] | [tunnel** *<0-999>***]**}	Configure an interface as the source IP address from which the RADIUS client sends RADIUS requests or receives responses.
Command Modes	Perle(config)#ip radius

Usage Guidelines

Use this command to configure Remote Authentication Dial-In User Service (RADIUS) authentication. RADIUS authenticates local and remote users on a company network. RADIUS is a client/server system that keeps the authentication information for users, remote access servers, VPN gateways, and other resources in one central database.

Examples

This example configures the source-interface as ethernet 1

```
Perle(config)#ip radius source-interface ethernet 1
```

Related Commands

clear radius

show radius

ip route

Use the no form of this command to negate or set to defaults.

Syntax Description	**ip route**

<table>
<tr><td><b>[ethernet</b><i>&lt;1-24&gt; <1-255&gt;</i> <b>dhcp | vrrp</b> <i>&lt;1-255&gt;</i> <b>| null</b> <i>&lt;1-255&gt;</i><b>]</b> <i>&lt; A.B.C.D> <1-255&gt;</i> | <i>&lt; A.B.C.D> <A.B.C.D> <A.B.C.D> <1-255&gt;</i> |</td><td>Configure static routes.</td></tr>
<tr><td><b>[table</b> <i>&lt;1-200> <A.B.C.D> <A.B.C.D> < A.B.C.D&gt;</i><b>] |</b></td><td></td></tr>
<tr><td><b>[bvi</b> <i>&lt;1-9999&gt;</i><b>] | [dialer</b> <i>&lt;0-15&gt;</i><b>] | [ethernet</b> <i>&lt;1-24&gt;</i> <b>dhcp | vrrp</b> <i>&lt;1-255&gt;</i> <b>| null</b> <i>&lt;1-255&gt;</i><b>] | [openvpn</b> <i>&lt;0-999&gt;</i><b>] | [tunnel</b> <i>&lt;0-999&gt;</i> <b>|</b> <i>&lt;1-255&gt;</i> <b>| dhcp]</b>}</td><td>Apply this route to this interface</td></tr>
<tr><td><b>enable-default-log</b> |</td><td>Configure default log.</td></tr>
<tr><td><b>Command Modes</b></td><td>Perle(config)#ip route</td></tr>
</table>

Usage Guidelines

Use this command to configure a static route.

Examples

This example routes packets from network 172.16.1.7 to an IOLAN at 172.17.23.20.

```
Perle(config)#ip route 172.16.1.7 255.255.0.0 172.17.23.20
```

Related Commands

ip route-policy

ip route-policy

Use the no form of this command to negate or set to defaults.

Syntax Description	**ip route-policy**
{**route-policy** *<WORD>*}	Configure a route policy. See *(config-pbr-rules)* for more information.
Command Modes	Perle(config)#ip route-policy

Usage Guidelines

Use this command to create a route policy name.

Examples

This example creates route policy testlab.

```
Perle(config)#ip route-policy testlab
```

Related Commands

(config-pbr-rules)

(config-pbr)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-pbr)**
{**description** *<LINE>* |	Configure a policy rule.
enable-default-log |	Configure default log.
rule *<1-9998>*}	Configure rule number.
Command Modes	Perle(config-pbr)#

Usage Guidelines

Use this command to create a policy rule.

Examples

This example configures rule number 10, then enter sub menu mode.

```
Perle(config-pbr)#rule 10
Perle(config-pbr-rules)#
```

(config-pbr-rules)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-pbr-rules)**
{**description** *<LINE>* |	Configure policy rule description.
log-enable |	Logs packet matching the rule.

Configure match values as define to the routing table.

match [destination address *<A.B.C.D> <A.B.C.D>* **| not** *<A.B.C.D> <A.B.C.D>* **| start** *<A.B.C.D>* **stop** *<A.B.C.D>***] |**

[port *<1-65535>***| not** *<1-65535>* **| start** *<1-65535>* **stop** *<1-65535>***] | [fragment | fragment | non-fragment] | [icmp type** *<0-255>* **code** *<0-255>***] | [ipsec ipsec |non-ipsec] | [protocol <0-255> ah | dccp | dsr | egp | eigrp | encap | esp | esp | etherip | ggp | gre | hmp | icmp | idpr | igmp | igp | ip | ipip | ipv6 | ipv6-frag | ipc6-icmp | ipv6-nonxt | ipv6-opts |**

IPv6 policy rule

ipv6-route | isis | l2tp | manet | mpls-in-ip | narp | not | osfp | pim | rdp | rohc | rsvp | sctp | sdrp | shim6 | skip | tcp | udp | udplite | xns-idp] | [recent count *<1-255>* **| time** *<1-4294967295>***] | [source address** *<A.B.C.D> <A.B.C.D>* **| not** *<A.B.C.D>* **| start** *<A.B.C.D>* **stop** *<A.B.C.D>* **| mac-address** *<H.H.H>* **| not** *<A.B.C.D>* **| [state established disable | enable] | [invalid disable | enable] | [new disable | enable] | related tcp-flags ack | all | fin | psh | rst | syn | urg | not |**	
set action drop | [dscp af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 cs1 | cws2 | cs3 | cs4 | cs5 | cs6 | cs7 ef] | mark *<1-2147483647>* **| [routing-table** *<1-200>* **| main] | tcp-mss** *<500-1460>* **| pmtu |** *<500-1460>*|	Sets action for policy rules.
time monthdays *<1-31>* **| not** *<1-31>***] | startdate month** *<WORD> <1-31> <2001-2037>* **| [starttime** *<hh:mm:ss>***] | stopdate month** *<WORD> <1-31> <2001-2037>* **| stoptime** *<hh:mm:ss>* **| utc | weekedays** *<DAY>* **| not** *<DAY>*}	Configure the time to match the rules.
Command Modes	Perle(config-pbr-rules)#

Usage Guidelines

Use these commands to set policy rules.

Examples

This example sets the action for the packets that match defined rule.

```
Perle(config-prb-rules)# set action drop
```

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

```
Perle(config)# ip route  0.0.0.0 0.0.0.0 10.10.200.9
Perle(config)#i p route table 2 0.0.0.0 0.0.0.0 172.16.0.8

Perle(config-prb)# ip route-policy http-firewall
Perle(config-prb))# rule 2
Perle(config-prb-rules)# set routing-table 2
Perle(config-prb-rules)# match protocol tcp
Perle(config-prb-rules)# match destination port 80

Perle(config)# interface ethernet 1
Perle(config-if)# ip address 192.168.2.1 255.255.255.0
Perle(config-if)# ip policy route-policy http-firewall
```

ip scp

Use the no form of this command to negate or set to defaults.

Syntax Description	ip scp
{scp password 0 *<LINE>* | 7 *<WORD>* | *<LINE>* | username *<WORD>*}	Configure SCP password and username.
Command Modes	Perle(config)#ip scp

Usage Guidelines

Use this command to configure the username and password to enable the IOLAN to securely copy files from a remote workstation.

Examples

This example configures the username for a connection to a remote host.

```
Perle(config)#ip scp username lynlab
```

ip sftp

Use the no form of this command to negate or set to defaults.

Syntax Description	ip sftp
{username *<WORD>* | password <0 *<LINE>* | 7 *<LINE>* | *<LINE>*}	SFTP configuration commands.
Command Modes	Perle(config)#ip stfp

Usage Guidelines

Use this command to create a SFTP secure connection to a remote host.

Examples

This example configures a username fred.

```
Perle(config)#ip sftp username fred
```

ip ssh

Use the no form of this command to negate or set to defaults.

Syntax Description	ip ssh
{authentication-retries *<0-5>*] |	Configure ssh authentication retires. Values are 1 to 5 Default is 3

Configure the SSH client parameters.

<table>
<tr><td colspan="2"><b>[client algorithms mac hmac hmac-sha1 | hmac-sha1-etm@openssh.com | hmac-sha2-256 | hmac-sha2-256-etm@openssh.com | hmac-sha2-512 | hmac-sha2-512 -etm@openssh.com | umac-128-etm@openssh.com | umac-128@openssh.com | 64-etm@openssh.com | umac-64@openssh.com] |</b></td></tr>
<tr><td><b>[pubkey-chain] |</b></td><td>Configure to use a public key-chain.</td></tr>
<tr><td colspan="2">Configure server algorithm encryption.</td></tr>
<tr><td colspan="2"><b>[server algorithm encryption 3des-cbc | aes128-cbc | aes128-ctr | aes128-gcm@openshh.com | aes192-cbc | aes192-ctr | aes256-cbc | aes256-ctr | aes256-gmc@openssh.com | arcfour | arcfour128 | arcfour256 | blowfish-cbc | cast128-cbc | chacha2--poly1305@openssh.com | rijndael-cbc@lysator.liu.se | mac hamc-md5 | hmac-md5-96 | hmac-md5-96-etm@openssh.com | hmac-md5-etm@openssh.com | hmac-ripemd160 | hmac-ripemd160-etm@openssh.com | hmac-sha1 | hmac-sha2-256 | hmac-sha2-256-etm@openssh.com |hmac-sha2-512 | hmac2-512-etm@openssh.com | umac-128-etm@openssh.com | umac-128@openssh.com | umac-64-etm@openssh.com | umac-64@openssh.com] |</b></td></tr>
<tr><td colspan="2">Configure the SSH server parameters.</td></tr>
<tr><td colspan="2"><b>[etm@openssh.com | umac-128-etm@openssh.com | umac-128@openssh.com | umac-64-etm@openssh.com | umac-64@openssh.com] |</b></td></tr>
<tr><td colspan="2">Configure algorithms used for SSH server.
Specify the authentication method.</td></tr>
<tr><td colspan="2"><b>[server [algorithm encryption 3-des-cbc aes128-cbc aes128-ctr aes128-gcm@openssh.com aes192-cbc aes192-ctr aes256-cbc aes256-ctr aes256-gcm@openssh.com chacha20-poly1305@openssh.com rijndael-cbc@lysator.liu.se] | authentication-method keyboard-interactive | password | public-key] |</b></td></tr>
<tr><td><b>[stricthostkeycheck] |</b></td><td>Enables SSH server authentication.</td></tr>
<tr><td><b>[time-out</b> <i>&lt;120&gt;</i>}</td><td>Configure SSH login time out interval.
Values are 1 to 120 seconds.
Default is 20 seconds</td></tr>
<tr><td><b>Command Modes</b></td><td>Perle(config)#ip ssh</td></tr>
</table>

Usage Guidelines

The SSH protocol enables you to set up SSH connections. YourIOLAN supports both client and server modes.

Examples

This example sets server mode for encryption hmac-md5.

```
Perle(config)#ip ssh server algorithm mac hmac-md5
```

Related Commands

telnet

ip ssh

show ssh

ip tacacs

Use the no form of this command to negate or set to defaults.

Syntax Description	ip tacacs
{**tacacs source-interface bvi** *<1-9999>* | | **dialer** *<0-15>* | **ethernet** *<1-24>* . *<1-4000>* | **openvpn-tunnel** *<0-999>* | **tunnel** *<0-999>*}	Configure the source interface for TACACS+ requests.
Command Modes	Perle(config)#ip tacacs

Usage Guidelines

Use this command to configure for Terminal Access Controller Access Control System (TACACS+) authentication.

Examples

This example configures the source-interface as ethernet 1

```
Perle(config)#ip tacacs source-interface ethernet 1
```

Related Commands

clear tacacs

tacacs

ip telnet

Use the no form of this command to negate or set to defaults.

Syntax Description	ip telnet
{**server**}	Enables Telnet server.
Command Modes	Perle(config)#ip telnet

Usage Guidelines

Use this command to config Telnet as the protocol to use for connections to a host. Telnet allows a user at one site to establish a TCP connection to a login server at another site and then pass the keystrokes from one device to the other.

Examples

This example enables telnet server.

```
Perle(config)#ip telnet server
```

Related Commands

telnet

show management-access

(management-access-LAN)

(management-access-WAN)

ipv6

Use the no form of this command to negate a command or set to defaults.

Syntax Description	ipv6
{[access-list <WORD>] |	Configure access list name.
[dhcp pool <WORD>] |	Configure the dhcp pool name.
[dns domain <WORD> server <X:X:X:X::X> | listen-address <X:X:X:X::X>] |	Configure DNS domain parameters.
[firewall <WORD> | ipv6-receive-redirects enable | ipv6-src-route enable | state-policy [established action accept | drop | reject] | [invalid action accept | drop | reject] | [related accept | drop | reject] |	Configure firewall options.
[host <WORD> | <X:X:X:X::X>] |	Configure static host names.
[name-server <X:X:X:X::X>] |	Configure the address of the name server.
[prefix-list <WORD>] |	Configure a prefix-list filter.
[radius source-interface bvi <1-9999> | | dialer <0-15> | ethernet <1-24>. <1-4000> openvpn-tunnel <0-999> tunnel <0-999>] |	Configure RADIUS configuration parameters.
[route <A.B.C.D> <A.B.C.D> | bvi <1-9999> | dialer <0-15> | ethernet <1-24>. <1-4000> | open-vpn-tunnel <0-999> | tunnel <0-999> <X:X:x:X::X <1-255> | table <1-200>] |	Configure static routes.
[route-policy <WORD>] |	Configure IPv6 route policy name.
[router osfp | rip] |	Enablea IPv6 routing process.

[tacacs source-interface bvi *<1-9999>* | | dialer *<0-15>* | ethernet *<1-24>* . *<1-4000>* openvpn-tunnel *<0-999>* tunnel *<0-999>*] |	Configure TACACS+ configuration parameters.
[unicast-routing]}	Enables unicast routing.
Command Modes	Perle(config)#ipv6

Usage Guidelines

Use this command to configure IPv6 parameters.

Examples

This example configures the DHCP pool name.

```
Perle(config)#ipv6 dhcp pool ipv6pool1
```

Related Commands

show ipv6

(config-ipv6-acl)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-ipv6-acl)**
{[*<1-65535>*] |	Configure the sequence number.
[deny *<X:X:X:X::X/0-128 | any>* exact-match] |	Configure to deny specified packets.
[permit *<X:X:X:X::X/0-128 | any>* exact-match]}	Configure to permit specified packets.
Command Modes	Perle(config-ipv6-acl)#

Usage Guidelines

Use this command to configure network packets to deny or permit using Access Control Lists (ACLs).

Examples

This example denies packets from this network.

```
Perle(config-ipv6-acl)# deny 172.16.0.0/16 exact-match
```

Related Commands

show ipv6

(config-dhcpv6)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-dhcpv6)
{**address prefix** *<X:X:X:X::X/ 0-128* |	Configure the IPv6 address prefix.
dns-server *<X:X:X:X::X>* |	Configure a DNS server for use by clients using this DHCP pool. A DNS server needs to be specified if you want to browse the Internet.
domain-name *<WORD>* |	Configure a domain name.
host *<WORD>* |	Configure the host name.
lifetime default *<0-4294967294>* **maximum** *<0-4294967294>* **minimum** *<0-4294967294>*|	Configure IPv6 DHCP parameters. Value is 0 to 4294967294 Max value is 0 to 4294967294 Min value is 0 to 4294967294
nis address *<X:X:X:X::X>* | **domain-name** *<WORD>* |	Configure the address and domain name of your nis server.
nisp address *<X:X:X:X::X>* | **domain-name** *<WORD>* |	Configure the address and domain name of your nisp server.
sip address *<X:X:X:X::X>* | **domain-name** *<WORD>* |	Configure the address and domain name of your sip server.
sntp address *<X:X:X:X::X>* |	Configure the address of your SNTP server.
subnet *<X:X:X:X::X/<1-128>*}	Configure the subnet.
Command Modes	Perle(config)#

Usage Guidelines

Use this command to configure IPv6 DHCP parameters.

Examples

This example sets the dns-server address to 1:2:3:4:5::6.

```
Perle(dhcpv6-config)#dns-server 1:2:3:4:5::6
```

Related Commands

show ipv6

(config-fw6)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-fw6)
{**default-action accept | drop | reject** |	Configure default action for firewall rules.
description *<LINE>* |	Configure firewall rules description.
enable-default-logfile |	Logs packets matching default action.
rule *<1-9999>*}	Creates rule number, then goes into sub menu mode.
Command Modes	Perle(config-fw6)#

Usage Guidelines

Use this command to configure IPv6 firewall options.

Examples

This example sets the default action for firewall rules.

```
Perle(config-fw6)# default-action drop
```

Related Commands

show ipv6

(config-fw6-rules)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-fw6-rules)
{**[description** *<WORD>*] |	Configure a description for the policy rule.
[disable] |	Disables the policy rule.
[log-enable] |	Logs packet matching the rule.

[match destination [address *<X:X:X::X/0-128>* | not *<X:X:X::X/0-128>* | start *<X:X:X::X>* stop *<X:X:X::X>*] | port <1-65535> not *<X:X:X::X/0-128>* | start *<X:X:X::X>* stop *<X:X:X::X>*] | [fragment fragment | non-fragment] | icmp type *<0-255>* code *<0-255>* | typenane address-unreachable | bad-header | communication-prohibited | destination-unreachable | echo-reply | echo-request | neighbour-advertisement | neighbour-solicitation | no-route | packet-too-big | parameter-problem | port-unreachable | route-advertisement | router-solicitation | time-exceeded | ttl-zero-during-reassembly | ttl-zero-during-transit | unknown-header-type | unknown-option] | ipsec ipsec | non-ipsec | [protocol <0-255> | ah |dccp |dsr | egp | eigrp | encap | esp | etherip | ggp | gre | hmp | icmp | idpr | igmp | igp | p | ipip | ipv6 | ipv6-frag | ipv6-icmp | ipv6-nonxt | ipv6-opts | ipv6-route | isis | l2tp | manet | mpls-in-ip | narp | not | ospf pim | rdp | roho | rsvp | sctp | sdrp | shim6 | skip | tcp | udp | udplite | vrrp | xnc-idp] recent count *<1-255>* | time *<1-4294967295>*] | *source* address *<X:X:X::X/0-128>* | not *<X:X:X::X/0-128>* | start*<X:X:X::X>* stop *<X:X:X::X>*] | [mac-address *<H.H.H>* not *<H.H.H>*] | [port *<1-65535>* | not *<1-65535>* | start *<1-65535>* | *stop* *<1-65535>*] | state [established disable | enable] | [invalid disable | enable] | [new enable | disable] | [related disable | enable] | tcp-flags ack | all | fin | psh | rst | syn |urg | not ack | all | fin | psh | rst | syn | urg] |	
[set action drop | accept | reject] |	Configure packet modifications.
time monthdays *<1-31>* | not *<1-31>*] | startdate *<MONTH>* *<1-31>* *<2001-2037>* | stopdate *<MONTH>* *<1-31>* *<2001-2037>*| starttime *<hh:mm:ss>* | stoptime *<hh:mm:ss>* | utc | weekdays *<DAY>* | not *<DAY>*]}	Configure time parameters.
Command Modes	Perle(config-fw6-rules)#

Usage Guidelines

Use this command to configure firewall rules for IPv6.

Examples

This example sets the action for matched packets.

```
Perle(config-fw6-rules)# set action accept
```

Related Commands

show ipv6

(config-pbr6)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-pbr6)**

description *<LINE>* |	Configure firewall rules description.
enable-default-logfile |	Logs packets matching default action.
rule *<1-9998>*}	Creates rule number, then goes into sub menu mode.
Command Modes	Perle(config-pbr6)#

Usage Guidelines

Use this command to configure IPv6 firewall options.

Examples

This example sets the default action for firewall rules.

```
Perle(config-fw6)# default-action drop
```

Related Commands

show ipv6

(config-pbr6-rules)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-pbr6-rules)#**
{**description** *<LINE>* |	Configure policy rule description.
log-enable |	Logs packet matching the rule.
Configure match values as define to the routing table.	
[match [destination address *<A.B.C.D> <A.B.C.D>* **| not** *<A.B.C.D> <A.B.C.D>* **| start** *<A.B.C.D>* **stop** *<A.B.C.D>***] | [port** *<1-65535>***| not** *<1-65535>* **| start** *<1-65535>* **stop***<1-65535>***] | [fragment | fragment | non-fragment] | [icmp type** *<0-255>* **code** *<0-255>***] | [ipsec ipsec |non-ipsec] | [protocol** *<0-255>* **ah | dccp | dsr | egp | eigrp | encap | esp | esp | etherip | ggp | gre | hmp | icmp | idpr | igmp | igp | ip | ipip | ipv6 | ipv6-frag | ipc6-icmp | ipv6-nonxt | ipv6-opts | ipv6-route | isis | l2tp | manet | mpls-in-ip | narp | not | osfp | pim | rdp | rohc | rsvp | sctp | sdrp | shim6 | skip | tcp | udp | udplite | vrrp | xns-idp] | [recent count** *<1-255>* **| time** *<1-4294967295>***] | [source address** *<A.B.C.D> <A.B.C.D>* **| not** *<A.B.C.D>* **| start** *<A.B.C.D>* **stop** *<A.B.C.D>* **| mac-address** *<H.H.H>* **| not** *<A.B.C.D>* **| [state established disable | enable] | [invalid disable | enable] | [new disable | enable] | related tcp-flags ack | all | fin | psh | rst | syn | urg | not] |**	

[set action drop | [dscp af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 cs1 | cws2 | cs3 | cs4 | cs5 | cs6 | cs7 ef] | mark *<1-2147483647>* **| [routing-table** *<1-200>* **| main] | tcp-mss** *<500-1460>* **pmtu |** *<500-1460>***] |**	Sets action for policy rules.
[time monthdays *<1-31>* **| not** *<1-31>* **| startdate month** *<WORD> <1-31> <2001-2037>***| [starttime** *<hh:mm:ss>***] | stopdate month***<WORD> <1-31> <2001-2037>* **| stoptime** *<hh:mm:ss>* **| utc | weekedays** *<DAY>* **| not** *<DAY>***]**}	Configure the time to match the rules.
Command Modes	Perle(config-pbr-rules)#

Usage Guidelines

Use this command to set IPv6 routing rules.

Examples

This example sets rule to match icmp type 80 code 80.

```
Perle(config-prb-rules)#match icmp type 80 code 80.
```

Related Commands

show ipv6

(config-rtr)—OSPF

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-rtr)-OSPF

{**ospf [area** *<0-4294967295>* **|** *<A.B.C.D>* **| export-list** *<WORD>* **| import-list** *<WORD>* **| nssa [default-information-originate no summary] | range** *<X:X:X:X::X>/<0-128>* **| stub no-summary** |	Configure OSPF area parameters. **Area**—OSPF area ID in decimal format or IP address format **NSSA** ● default-information-originate–originate Type 7 default into NSSA area ● No summary—NSSA ABBRs, the origination of the default route is conditioned to the existence of a default route in the RIB that wasn't learned via the OSPF protocol. **Range**—Summarize routes matching address/mask (border routers only) **Stub**–no-summary–do not send summary LSA into stub area
interface bvi *<1-9999>* **| dialer** *<0-15>* **| ethernet** *<1-x>* **.** *<1-4000>* **| sfp** *<1-x>* **| tunnel** *<0-999>* |	Specify the interface to use with OSPF.
redistribute connected bgp route-map *<WORD>* **| connected route-map** *<WORD>* **kernel route-map** *<WORD>* **| rip route-map** *<WORD>* **| static route-map** *<WORD>* |	Redistribute information from other routing protocol.
router-id *<A.B.C.D>*}	
Command Modes	Perle(config-router)#

Usage Guidelines

Use this command to configure OSPF protocol parameters.

Examples

This example sets ethernet 1 to OSPF.

```
Perle(config-rtr)#interface ethernet 1
```

Related Commands

show ip ospf

(config-rtr)—RIP

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-rtr)-RIP**

{**[aggregate-address *<A.B.C.D> <A.B.C.D>* as-set summary-only] |**	Specifies the block of addresses to be aggregated. **as-set**—specifies that the routes resulting from the aggregation include the AS-set. **summary-only**—specifies that aggregated routes are summarized. These routes will not be advertised.
[exit-address-family] |	Exit family level menu.
maximum-path *<1-255>* | ibgp *<1-255>* |	Configure the maximum number of eBGP/iBGP paths to a destination. ebgp values are 1 to 255 Default is 1 ibgp values are 1 to 255 Default is 1
[neighbour *<A.B.C.D> <X:X:X:X::X>* |	Configure neighbor configuration. Specify an IPv4 or IPv6 address.
advertisement-interval *<0-600>* |	Configure the minimum interval between sending BGP routing updates. Values 0 to 600 Default eBGP is 30 secs Default iBGP peers is 5 seconds
allowas-in *<1-10>* |	Allows or disallows receiving BGP advertisements containing the AS path of the local router. Default readvertisement is disabled. Default is 3
[asoverride] |	Override ASN's in outbound updates if AS–path equals remote–AS. Only applies to eBGP neighbor. Default is disable
[attribute-unchanged as-path | med | next-hop] |	Allows the IOLAN to send updates to a neighbor with unchanged attributes. Value is on for all if no option provided Default is disabled
[capability dynamic |	Advertise dynamic capability to this neighbor. Default is session is brought up with minimal capability on both sides.
orf prefix-list both | receive | send] |	Advertises support for Outbound Route Filtering (OFR) for updating BGP capabilities advertised and received from this neighbor. Default is the session is brought up with minimal capability on both sides.
[default originate route-map *<NAME>*] |	Enables or disables forwarding of the default route to a BGP neighbor. Default is disabled

[description *<LINE>*] |	Provide a description for a BGP neighbor.
[disable-connected-check |	Enables a directly connected eBGP neighbor to peer using a loopback address without adjusting the default TTL of 1. Default is off
[distributed-list *<1-99>* in | out *<1300-2699>* in | out] |	Aapplies an access list to filter inbound/outbound routing updates from this neighbor. Default is none
[dont't-capability-negotiate] |	Disables BGP capability negotiation Default is capability negotiation is performed.
[ebgp-multihop *<1-255>*] |	Allows you to establish eBGP peer relationships between routers that aren't directly connected to one another. Default is only directly connected neighbors are allowed.
[filter-list *<WORD>*] |	Applies an AS–path list to routing updates to this neighbor Default is none
[local-as *<1-4294967295>* no-prepend] |	Defines a local autonomous system number for eBGP peering Default is none
[maximum-prefix *<1-4294967295>*] |	Configure the maximum number of prefixes to accept from this neighbor before that neighbor is taken down. Values are 1–4294967295 Default is none
[next-hop-self] |	Sets the local router as the next ho for this neighbor Default is disable
[override-capability] |	Overrides capability negotiation to allow a peering session to be established with a neighbor that does not support capabilities negotiation Default is a session cant be established if the neighbor does not support capability negotiation.
[passive] |	Directs the router not to initiate connections with this neighbor
[password *<LINE>* |	Configure a BGP MD5 password Default is none
[port *<1-65535>*] |	Specifies the port on which the neighbor is listening for BGP signals Values are 1 to 65535 Default port is 179

[prefix-list *<WORD>*] |	Applies this prefix list filter updates to/from this neighbor Default is none
[remote-as *<1-4294967295>*] |	Configure the autonomous system number of the neighbor. Default is none
remove-private-as |	Directs the IOLAN to remove private AS numbers from updates sent to this neighbor (eBGP only) Default is disable (do not remove)
[route-map *<WORD>* in | out] |	Applies a route map to filter updates to/from this neighbor Default is none
[route-reflector -client] |	Specify this neighbor as a route reflector client (iBGP only) Default is disabled
[route-server-client] |	Specify this neighbor as a route server client Default is disable
[send-community both | extended | standard] |	Enables or disables the sending of community attributes to the specified neighbor Value— no type specified send standard attributes Default is both
[shutdown]	Administratively shuts down a BGP neighbor Default is disabled
[soft-reconfiguration] |	Directs the IOLAN to store received routing updates.
[strict-capability-match] | **[timers *<0-65535> <0-65535>* |**	Directs the router to strictly match the capabilities of the neighbor Default is disable
[timers *<0-65535> <0-65535>* |	Keepalive interval Values are 0—65535 Default is 60 seconds
[holdtime] |	Value are 0-65535 Default is 180 seconds
connect *<0-65335>*] |	Values are 0-65535 Default is 120 seconds
[ttl-security] |	Configure the time-to-live (ttl) security hop count. This option and ebgp-multihop cannot be set at the same time Values are 1 to 254 hops Default is 1

[unsuppress-map *<WORD>*] |	Directs the IOLAN to selectively advertise routes suppressed by aggregating addresses, based on a route map Value specify a router map
[update-source] |	Specifies the source ip address or interface for routing updates Default is none
[weight] |	Defines a default weight for routes from this neighbor Values are 1-65335 Default is routes learned from a BGP neighbor have a weight of 0. Routes sourced by the local router have a weight of 32768
network *<A.B.C.D>* backdoor | mask *<A.B.C.D>* | route-map *<WORD>*}	Configure a network to be advertised by the BGP routing process. **Backdoor**—indicates that this network is reachable by a back door rote. A back door network is considered to be like a local network but is not advertised. **Route-map**—specifies a configured route map to be used when advertising the network Default is none

key

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**key**
{**chain *< WORD>***}	Configure keychain management.
Command Modes	Perle(config)#key

Usage Guidelines

Use this command to create a key chain. Key chain management allows you to create and maintain key chains, which are sequences of keys (sometimes called shared secrets). You can use key chains with features that secure communications with other devices by using key-based authentication.

Examples

This example create key chain 1, then go into sub menu key.

```
Perle(config)#key chain key1
```

Related Commands

(config-keychain-key)

(config-key)

{**key** *<1-2147483647>*}

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-key)**
{**key** *<1-2147483647>*}	Configure a number for this key.
Command Modes	Perle#(config-key)#

Usage Guidelines

Use this command in conjunction with (config-keychain-key) to set a key number.

Examples

Configures a key number.

```
Perle(config-key)# key 250
```

Related Commands

(config-pbr6-rules)#

(config-keychain-key)

(config-keychain-key)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-keychain-key)**
{**string 0** *<WORD>* | **7** *<WORD>* | *<WORD>*}	Configure the key chain. 0–specifies an unencrypted password 7–specifies a hidden password with follow WORD–the unencrypted (cleartext) user password.
Command Modes	Perle(config-keychain-key)

Usage Guidelines

Use this command to configure a password for key chain.

Examples

Configure a password for key chain.

```
Perle(config-keychain-key)# string password123
```

Related Commands

(config-pbr6-rules)#

ldap

Use the no form of this command to negate a command or set to defaults.

Syntax Description	ldap
{server <*WORD*>}	Configure LDAP server name.
Command Modes	Perle(config)#ldap

Usage Guidelines

Use this command configure an LDAP server.

Examples

This example configures a LDAP server name.

```
Perle(config)# ldap server testldap
```

Related Commands

(config-ldap-server)

clear ldap

show ldap

(config-ldap-server)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-ldap-server)
{**[base-dn** <***WORD***>**] |**	Configure the Base DN for LDAP. The Base DN is the starting point an LDAP server uses when searching for user authentication within your Directory.
[bind authenticate root-dn <***WORD***> **password 0** <***WORD***> **| 7**<***WORD***> **|** <***WORD***>**] |**	Configure ● An authenticated bind is performed when a root distinguished name (DN) and password are available ● In the absence of a root DN and password, an anonymous bind is performed
[ipv4 <***WORD***> **|** <***A.B.C.D***>**] |**	Configure the IPv4 address of LDAP server.
[ipv6 <***WORD***> **|** <***X:X:X:X::X***>**] |**	Configure the IPv6 address of LDAP server.
[mode secure] |	Set the server mode. ● secure – configures the LDAP to initiate the transport layer security (TLS) connection and specifies the secure mode ● non-secure Default is non-secure

[search-filter <*WORD*>] |	Configure a search filter The search filter operation must be supported on the LDAP server. Filters are to restrict the numbers of users or groups that are permitted to access an application. In essence, the filter limits what part of the LDAP tree the application syncs from. A filter can and should be written for both user and group membership. This ensures that you are not flooding your application with users and groups that do not need access.
[secure cipher | transport port <*1-65535*> | trustpoint <*WORD*>] |	Configure ● ciphers—adh, dh, dss, edh, high, medium, rsa, sslv3 ● transport—listening port for secure connections ● trustpoint Default listening port for secure transfer connections is 636
[timeout retransmission <*1-65535*>] |	Configure the timeout for retransmissions. Values are 1 to 65535 Default is 30 seconds
[transport port <*1-65535*>] |	Configure the listening port for unsecured connections. Default port is 389
[user-attribute other <*WORD*> | samaccountname | uid]}	Configure the user attribute. ● other—configure custom usr attibute ● sAMAccountName— Microsoft Active Directory ● uid—OpenLDAP
Command Modes	Perle(config-ldap-server)#

Usage Guidelines

Use this command to configure LDAP server parameters.

Examples

Search filter for LDAP

For example, if your users are distinguished by having two objectClass attributes (one equal to 'person' and another to 'user'), this is the command to match for it.

```
Perle(config-ldap-server) #search-filter (&(objectClass=person)(objectClass=user))
```

Search filter for Microsoft Active Directory

This only synchronize users in the 'Warehouse' group—this should be applied to the User Object Filter:

```
Perle(config-ldap-server) #search-filter
(&(objectCategory=Person)(sAMAccountName=*)(memberOf=cn=CaptainPlanet,ou=
users,dc=company,dc=com))
```

Related Commands

aaa

show ldap

clear ldap

ldap

(config-sg-ldap)

line

Use the no form of this command to negate a command or set to defaults.

Syntax Description	line
{[console *<0-0>*] |	Command for line console/tty only exist on models with serial ports. Primary terminal line. See *(config-line)#console*
[tty*<1-28>*] |	Terminal/serial. See *(config-line)#tty and #usb*
[vty *<0-15>*]}	Virtual terminal.
Command Modes	Perle(config)#line

Usage Guidelines

Use this command to change to line mode configuration.

Examples

Go into line configuration mode for tty 2.

```
Perle(config)# tty 2
```

Related Commands

(config-line)#console

(config-line)#tty and #usb

lldp

Syntax Description	lldp
{[hold-mult *<2-10>*] |	Configure a value for the LLDP hold multiplier. This is the time to cache learned LLDP information before discarding, measured in multiples of the timer parameter. For example, if the Timer is 30 seconds, and the Hold Multiplier is 4, then the LLDP packets are discarded after 120 seconds. Default is 4 Values are 2 to 10

[logging] |	Configure logging for LLDP neighbor discovery. Default is off.
[notification-interval] |	Configure the minimum interval between LLDP SNMP notifications. Default is 5 seconds Value is 5 to 3600 seconds
[optional-tlv port-info] |	Reverts to the previous setting of providing the interface name.
[reinit *<1-10>*] |	Configure the delay (in sec) for LLDP initializations on any interface. Default is 2 seconds Values are 1 to 10 seconds
[run] |	Enables LLDP. LLDP Disabled by default.
[timer] |	Configure the rate at which LLDP packets are sent. This parameter is used with the TX Hold multiplier parameter to determine when LLDP packets are discarded. Default is 30 seconds Values are 5 to 32768 seconds
[tvl-select mac-phy-cfg | managemnt-address *<A.B.C.D>* | *<X:X:X:X:X>* | max-frame-size | port-description | system capabilities | system description | system-name] |	Configure the LLDP TLVs to send. Default is all TLVs are sent. Maximum management addresses are 8. Default management addressees are automatically selected by LLDP.
[tx-delay]}	Configure the amount of time in seconds that passes between successive LLDP frame transmissions due to changes in the LLDP local systems MIB. Default is 30 seconds Values are 1 to 8192 seconds
Command Modes	Perle(config)#lldp

Usage Guidelines

Use this command to configure Link Layer Discovery Protocol (LLDP) parameters., LLDP allows network devices to advertise their identity and capabilities on a LAN. LLDP specifically defines a standard method for Ethernet network devices such as switches, routers, and wireless LAN access points to advertise information about themselves to other nodes on the network and store the information they discover. LLDP should be enabled in a multi-vendor network.

Examples

This example enables LLDP.

```
Perle(config)#lldp run
```

Related Commands

clear lldp

show lldp

logging

Use the no form of this command to negate a command or set to defaults.

Syntax Description	logging
{[*<hostname>* | *<A.B.C.D>*] |	Configure the address of the logging host.
[alarm *<2-3>* **| major | minor] |**	Sets the severity alarm level. **major**—immediate action needed (severity 2) **minor**—minor warning conditions (severity 3)
[buffered *<0-7>* **|** *<4096-32768>* **| alert | critical] | debugging | emergencies | errors | informational | notifications | warnings] |**	Configure buffered logging parameters.
[console *<0-7>* **|** *<4096-32768>* **| alert | critical] | debugging | emergencies | errors | informational | notifications | warnings] |**	Configure console logging parameters.
[delimiter tcp] |	Appends delimiter to syslog messages.
[facility auth | cron | daemon | kern | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | sys10 | sys11 | sys12 | sys13 | sys14 | sys9 | syslog | user | ucp] |	Configure facility parameter for syslog messages.
[file flash: *<filename> <0-7>* **|** *<4096-32768>* **| alert | critical | debugging | emergencies | errors | informational | notifications | warnings] |**	Configure file logging parameters.
[host *<A.B.C.D>* **transport tcp port <***1-65535>* **| udp port <***1-65535>***] |**	Configure the syslog server IP address and parameters.

[monitor *<0-7>* | *<4096-32768>* | alert | critical] | debugging | emergencies | errors | informational | notifications | warnings] |	Configure terminal line (monitor) logging parameters.
[on] |	Enables logging to all enabled destinations.
[origin-id hostname | ip | ipv6 | string] |	Adds origin ID to syslog messages.
[rate-limit *<1-10000>* except *<0-7>* | *<4096-32768>* | alert | critical] | debugging | emergencies | errors | informational | notifications | warnings] |	Configure message per second limit.
[source interface bvi *<1-9999>* | ethernet *<1-24>* | openvpn-tunnel *<0-999>* | tunnel *<0-999>*] |	Configure the interface for source address in logging transactions.
[trap *<0-7>* | *<4096-32768>* | alert | critical] | debugging | emergencies | errors | informational | notifications | warnings]}	Configure syslog server logging level.
Command Default	logging buffered 4096 debugging logging console debugging logging monitor debugging
Command Modes	Perle(config)#logging

Usage Guidelines

Use this command to enable logging settings.

Examples

This example enables logging to host 172.16.55.88.

```
Perle(config)#logging 172.16.55.88
```

Related Commands

show lldp

login

Syntax Description	**login**

{**[on-failure every *<1-65535>* | log every *<1-65535>*| trap every *<1-65535>*] |**	Configure options for failed login attempt.
[on-success every *<1-65535>* | log every *<1-65535>*| trap every *<1-65535>*]}	Configure options for successful login attempt.
Command Modes	Perle(config)#login

Usage Guidelines

Use this command to set parameters for users log in attempts.

Examples

This example logs failed login attempts.

```
Perle(config)#login on-failure
```

Related Commands

logging

mac

Use the no form of this command to negate a command or set to defaults.

Syntax Description	mac access-list
{**[access-list *<WORD>*] |**	Configure a MAC access list name.
[export *<WORD>* url flash: | ftp: | http: | https: | scp: | sftp: | tftp:] |	Exports MAC access list to a server.
[import *<WORD>* interface bvi *<1-9999>* | ethernet *<1-24>* . *<1-4000>* | url flash: | ftp: | http: | https: | scp: | stfp: | tftp:]}	Import formats are; ● xxxx.xxxx.xxxx—Cisco format where xxxx is 1-4 digits ● xx:xx:xx:xx:xx:xx—where xx is 1-2 digits ● aabbccddeeff ● Import from supported interface ● ethernet interfaces ● sub-ethernet (VLANs) interfaces ● bridge interfaces

Command Default

Notes:

- There are no defaults when configuring the MAC access-group and policy, but the no/ default policy after initial configuration, is Disabled
- No and default commands operate the same for all interface types
- If there is no MAC access-group specified, the no/default command REMOVES the MAC access-group and policy
- If a MAC access-group is specified the default policy: disabled is configured and applied

Command Modes

Perle(config)#mac

Usage Guidelines

Use this command to create a host MAC address list.

Policy descriptions

Permit—allow all MAC addresses in this MAC access list, deny all MAC addressees not in this list.

Deny—deny all MAC addresses in this MAC access list, allow all others not in the list

Disable—not active

MAC address list can also be created by importing CSV files.

Examples

This example assigns access-list eth1-macs to interface ethernet 1with all addresses within the eth1-macs policy to be accepted or permitted on this interface.

```
Perle(config)#interface ethernet 1
Perle(config)#mac-access-list eth1-macs-static
Perle(config-mac-acl)#
```

This example imports a <mac-list-csv.txt> file from host 172.16.4.182 using http protocol.

```
Perle(config)#mac access-list import <mac-list-csv.txt> url http://172.16.4.182/pub/
<mac-list-csv.txt>
Connected to 172.16.4.182.
59 bytes copied in 0.009 seconds (6319 bytes/sec)
Waiting for download to complete . . .
% Successfully processed 4 properly formatted MAC addresses
```

This example exports a <mac-list-csv.txt> file tot 172.16.4.182 using tftp protocol.

```
Perle(config)#mac access-list export <mac-list-csv.txt> url tftp://172.16.4.182/<mac-
list-csv.txt>
Accessing tftp://172.16.4.182//<macs-export-file>
60 bytes copied in 0.003 seconds (21030 bytes/sec)
```

This example imports and permits MAC addresses from BVI interface 10 into bridge-mac-list.

```
Perle(config)#mac access-list import bridge-mac-list interface bvi 10
Perle(config)#interface bvi 10
Perle(config-if)#mac access-group bridge-mac-list permit
```

Related Commands

show mac

(config-mac-acl)

(config-mac-acl)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-mac-acl)#
{[description <*LINE*>] |	Configure a MAC access-list description.
[host src-mac-address <*H.H.H*>]}	Configure the source address of the host you want to add to this list.
Command Modes	Perle(config-mac-acl)#

Usage Guidelines

Use this command to enter MAC address to this MAC address list.

Examples

This example adds hsot mac address aaaa.bbbb.cccc to the list.

```
Perle(config-mac-acl)#host src-mac-addr aaaa.bbbb.cccc
```

Related Commands

show mac

management-access

Syntax Description	management-access
{[enable] |	Enables management access. Default is enabled
[from-lan] |	Enters the configuration menu for defining management access from the LAN.
[from-wan]}	Enters the configuration menu for defining management access from the WAN.
Command Default	LAN—all protocols enabled WAN—all protocols are disabled.
Command Modes	Perle(config)#management-access

Usage Guidelines

Use this command to enter the configuration menu for the management access you wish to set.

With in the "from-LAN" and "from-WAN" sub menu, you will be able to enable/ disable the following management access methods.

Management Methods are:

- Enable—All management Access methods for this interface
- HTTP—Enable HTTP (Web) management Access for this interface
- HTTPS—Enable HTTPS (Web) management access for this interface
- Telnet—Enable Telnet management access for this interface
- SSH—Enable SSH management access for this interface
- SNMP—Enable SNMP management access for this interface

Related Commands

(management-access-LAN)

(management-access-WAN)

(management-access-LAN)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(management-access-LAN)
{**[http enable] |**	Enables devices connected from the LAN side with Role set to LAN to use HTTP to connect to the IOLAN.
[https enable] |	Enables devices connected from the LAN side with Role set to LAN to use HTTPS to connect to the IOLAN.
[snmp enable] |	Enables devices connected from the LAN side with Role set to LAN to use SNMP to connect to the IOLAN.
[ssh enable] |	Enables devices connected from the LAN side with Role set to LAN to use SSH to connect to the IOLAN.
[telnet enable]}	Enables devices connected from the LAN side with Role set to LAN to use Telnet to connect to the IOLAN.
Command Default	All methods are enabled on the LAN side. All methods are disabled on the WAN side.
Command Modes	Perle(config)#management-access-lan

Usage Guidelines

Use this comment to set protocols to allow entry from the LAN side to manage the IOLAN.

Examples

This example sets management access telnet for LAN devices.

```
Perle(config)#management-access from-LAN
Perle(management-access-lan)#telnet enable
```

Related Commands

(management-access-LAN)

(management-access-WAN)

(management-access-WAN)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(management-access-WAN)**
{**[http enable] |**	Enable devices connected from the WAN side with Role set to WAN to use HTTP to connect to the IOLAN.
[https enable] |	Enables devices connected from the WAN side with Role set to WAN to use HTTPS to connect to the IOLAN.
[snmp enable] |	Enables devices connected from the WAN side with Role set to WAN to use SNMP to connect to the IOLAN.
[ssh enable] |	Enables devices connected from the WAN side with Role set to WAN to use SSH to connect to the IOLAN.
[telnet enable]}	Enables devices connected from the WAN side with Role set to WAN to use Telnet to connect to the IOLAN.
Command Default	All protocols are disabled.
Command Modes	Perle(config)#management-access-from-lan

Usage Guide

Use this command to set protocols to allow entry from the WAN side to manage the IOLAN.

Examples

Configure management access for wan devices using ssh.

```
Perle(config)# management-access from-WAN
Perle(config-management-access-WAN)#ssh enable
```

Related Commands

(config-mac-acl)

network-watchdog

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**network-watchdog**
{**router**}	Configure the watchdog timer.
Command Modes	Perle(config)#network watchdog

Usage Guidelines

Use this command to enter sub-menu mode for watch dog timer.

Examples

This example takes you to sub-menu mode for watchdog timer feature.

Perle(config)#network-watchdog router

Related Commands

(config-network-watchdog)

(config-network-watchdog)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-network-watchdog)**
{**count** *<1-10>* | **enable** | **[fail-action notifications-only** | **notifications-reset]** |	**Fail-action** ● notify only ● notify and reboot
[interval *<1-180>*] |	**Interval** to wait between tests. Values are 1 to 180 minutes. Default IOLAN is 20 minutes.
[response *<1-3600>*] |	**Response**—Time to wait for a response to the ping request. Values are 1 to 3600 seconds. Default is 5 seconds.

[source-interface [bvi *<1-9999>*] | [dialer *<0-15>*] | ethernet *<1->*| [open-tunnel *<0-999>*] | [tunnel *<0-999>*] |	**Source-interface**—Specify the interface to send the ping request on (optional). Values are: ● BVI 1–9999 ● dialer 1–15 ● ethernet *<1-24>* ● openvpn 0–999 ● tunnel 0–999
[target *<A.B.C.D>* | *<WORD>* | *<X:X:X:X::X>*] |	**Target**—Enter the target host IPv4, IPv6 or hostname address.
[threshold-count *<1-30>*]}	**Threshold count**—The consecutive failed test count to trigger an Fail-action. Value is 1 to 30
Command Modes	Perle(config-network-watchdog)#

Usage Guidelines

Use this command to configure the Network Watchdog timeout action When configured, the watchdog feature runs continuous ping tests. Each ping test is be comprised of one or more ping attempts. If all of the pings in a test fail, the test has failed, if one ping test passes, the test is considered to have passed.

The watchdog feature is triggered after a successful connection, which is defined as one successful test. After which your tests will run as defined..

If any of the ping test fail, the IOLAN and modem notifies the user and/or can reset the IOLAN and modem.

Examples

This example configures the watchdog timer on Ethernet interface 2 to ping target host 172.16.1.1 with a count of 10.

```
Perle(config-network-watchdog)#count 10
Perle(config-network-watchdog)#target 172.16.1.1
Perle(config-network-watchdog)#source interface ethernet 2
```

Related Commands

show network-watchdog

ntp

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**ntp**
{**[authentication] |**	Configure authentication of time sources. The time sources must authenticate with each other before synchronizing clock time.

[authentication-key *<1-65534>* md5 | sha1 | sha256 | sha512 | *<WORD>* 0 | 7] |	Configure the authentication key to be exchanged between time sources before clock synchronizing begins. 0—unencrypted key 7—encrypted key
[broadcastdelay *<1-999999>*] |	Configure the broadcast delay timer. By default, the IOLAN sets broadcast delay to Auto-negotiate. Select the auto-negotiate broadcast delay off if you wish to set your own broadcast delay time in microseconds. Broadcast delay time is the estimated round-trip delay between the broadcast NTP server and the IOLAN.
[logging] |	Logs NTP messages to a configured syslog server.
master *<1-15>* | peer *<A.B.C.D>* *<WORD>* *<X:X:X:X::X>* ip *<WORD>* ipv6 *<WORD>>* | key *<1-65534>* | maxpoll *<4-17>* | minpoll *<4-17>* | prefer | version *<1-4>*] |	Configure master or peer as the source clock. The stratum defines how far away the clock 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. Configure the IPv4/IPv6 address or hostname of the NTP peer that you are getting the clock from. Select prefer to use this NTP source over another. A preferred peer's responses are discarded only if they vary greatly from the other time sources. Otherwise, the preferred peer is used for synchronization without consideration of the other time sources.

[server ***<A.B.C.D> <WORD> <X:X:X:X::X>*** **ip** ***<WORD>*** **ipv6** ***<WORD>>*** **| key** ***<1-65534>*** **| maxpoll** ***<4-17>*** **| minpoll** ***<4-17>*** **| prefer | version** ***<1-4>*** **] |**	Configure the IPv4/IPv6 address or hostname of the NTP peer that you are getting the clock from. Select prefer to use this NTP source over another. A preferred server's responses are discarded only if they vary greatly from the other time sources. Otherwise, the preferred server is used for synchronization without consideration of the other time sources. Changes to the polling interval is not recommended and is discouraged. NTP dynamically selects the optimal poll interval between the values of minpoll and maxpoll, which defaults to 64 and 1024 seconds respectively and are correct for most environments. Shorter values are used to correct large errors and larger values are to refine accuracy. Default is minimum poll 64. Versions 1 to 4 are supported
[trusted-key ***1-65534*****]**}	Configure a trusted key to be used for trusted time sources.
Command Modes	Perle(config)#ntp

Usage Guidelines

Use this command to distribute and maintain 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) the IOLAN should synchronize with. NTP will not synchronize with nodes whose time is significantly off even if its stratum is lower. During this "settling" period, the IOLAN may not have the correct time. NTP can usually achieve time synchronization between two systems in the order of a few milliseconds. This is achieved with a time transmission rate of as little as one packet per minute.

Examples

```
Perle(config)#ntp server 172.16.4.181
 23:40:31:  %NTPD-5: ntpd 4.2.8p6@1.3265-o Wed May 18 14:33:49 UTC 2016 (10):
Starting
 23:40:31:  %NTPD-6: Command line: ntpd -n -g
 23:40:31:  %RSYSLOGD-6:LOGGINGHOST_STARTSTOP: Logging to UDP host
```

```
172.16.55.88 port 514 started
 23:40:31:  %NTPD-6: proto: precision = 3.840 usec (-18)
 23:40:31:  %NTPD-6: Listen and drop on 0 v6wildcard [::]:123
 23:40:31:  %NTPD-6: Listen and drop on 1 v4wildcard 0.0.0.0:123
 23:40:31:  %NTPD-6: Listen normally on 2 lo 127.0.0.1:123
 23:40:31:  %NTPD-6: Listen normally on 3 Vl1 172.16.113.77:123
 23:40:31:  %NTPD-6: Listen normally on 4 lo [::1]:123
23:40:31:  %NTPD-6: Listen normally on 5 Gi2 [fe80::6ac9:bff:fec1:58da%4]:123
 23:40:31:  %NTPD-6: Listen normally on 6 Gi1 [fe80::6ac9:bff:fec1:58d9%3]:123
 23:40:31:  %NTPD-6: Listen normally on 7 eth0 [fe80::6ac9:bff:fec1:58d8%2]:123
 23:40:31:  %NTPD-6: Listening on routing socket on fd #38 for interface updates
 23:40:31:  %NTPD-3: Unable to listen for broadcasts, no broadcast interfaces
available
 23:40:31:  %NTPD-6: 0.0.0.0 c01d 0d kern kernel time sync enabled
 23:40:31:  %NTPD-6: 0.0.0.0 c012 02 freq_set kernel 0.000 PPM
 23:40:31:  %NTPD-6: 0.0.0.0 c011 01 freq_not_set
 23:40:31:  %NTPD-6: 0.0.0.0 c016 06 restart
Perle(config)#ntp status
Clock is synchronized, stratum 12, reference is 172.16.4.181
Precision is 2**-18 s
Reference time is dae84dc5.33013328 (Thu, May 19 2016 10:35:49.199)
Clock offset is 7.595002 msec, root delay is 0.439 msec
Root dispersion is 7956.293 msec
```

Related Commands

show ntp

policy-map

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**policy-map**
{**[<*WORD*>] |**	Specifies the name of the policy map to be created or modified.
[priority-queue <*WORD*>] |	Configure priority-queue policy-map. See ***(config-pmapPQ)***
[rate-control <*WORD*> bandwidth <*1-2000000*>] |	Configure rate-control policy-map. See ***(config-pmapRC)***
[traffic-limit <*1-2000000*>]}	Configure traffic-limit policy-map. See (***(config-pmapTL)***

Command Modes	Perle(config)#policy-map

Usage Guidelines

Use this command to create a policy-map. A policy map references class maps and identifies a series of actions to perform based on the traffic match criteria. A policy map essentially defines a policy stating what happens to traffic that has been classified using class maps and ACLs.
Your IOLAN provides you with three mechanisms for configuring Quality of Service (QOS).

1) Priority-queuing—packets are placed in queues, high priority packets are sent first.

2) Rate-control—rate control is a classless policy that limits the packet flow to a set rate. Traffic is filtered based on the expenditure of tokens. Tokens roughly correspond to bytes. Short bursts can be allowed to exceed the limit. On creation, the Rate-Control traffic is stocked with tokens which correspond to the amount of traffic that can be burst in one go. Tokens arrive at a steady rate, until the bucket is full.

3) Traffic-limiting—traffic limiting is a mechanism that can be used to "police" incoming traffic. The mechanism assign each traffic flow a bandwidth limit. All incoming traffic within a flow in excess of the bandwidth is dropped.This policy can be applied to both ingress and egress packets.

Examples

Creates a policy-map called test-policy.

```
Perle(config)# policy-map test-policy
Perle(config-pmap)#
```

Related Commands

(config-pmap)

(config-pmap-c)

(config-pmapRC)

(config-pmapPQ)

(config-pmapPQ-c)

(config-pmapTL)

(config-pmap)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-pmap)**
{[**bandwidth** *<1-2000000>*] |	Configure the available bandwidth in Kbps for this policy. Default is to match interface speed.
[class *<1-4094>* **| default] |**	Configure a class identifier. Values are 1–4094
[description *<LINE>***]**}	Configure policy map description.
Command Modes	Perle(config-pmap)#

Usage Guidelines

Configure parameters for his policy map.

Examples

Configures class identifier as 10.

```
Perle(config-pmap)#class 10
Perle(config-pmap-c)#
```

Related Commands

policy-map

(config-pmap-c)

(config-pmap-c)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-pmap-c)
{[**bandwidth** *<1-2000000>*] |	Configure the base guaranteed bandwidth for this traffic class (in Kbps or in percent). Bandwidth must be below the entire bandwidth set for this policy.
[**burst** *<1-20000>*] |	Configure the burst size for this class. Values are 1 to 20000 in Kbytes Default is 15 Kbytes
[**ceiling** *<1-2000000>* | **percent** *<1-100>*] |	Configure a bandwidth ceiling for a traffic class in Kbps. ● Percentage based on interface physical rate ● Must be equal or greater then specified bandwidth Default is 100 percent of bandwidth if no ceiling specified.
[**codel-flows** *<1-4294967295>*] |	Configure the number of flows into which the incoming packets are classified. Values are 1 to 4294967295 Default is 1024
[**codel-interval** *<1-4294967295>*] |	Configure the interval to the measured minimum delay as not to become stale. It should be set on the order of the worst-case round trip time (RTT) through the bottleneck to give endpoints sufficient time to react. Values are 1 to 4294967295 milliseconds. Default is 100 milliseconds.
[**codel-quantum** *<1-4294967295>*] |	Configure the maximum amount of bytes dequeued from a queue at once. Values are 1 to 4294967295 Default is 1514

[codel-target *<1-4294967295>*] |

Configure the minimum standing/persistent queue delay.

Values are 1 to 4294967295 milliseconds
Default is 5 milliseconds

[description *<LINE>*] |

Configure a description for this traffic class.

[queue-limit *<1-4294967295>*] |

Configure the maximum size for this traffic class.

Values are 1 to 4294967295 milliseconds
Default is none

[queue-type] |

Configure the type of queuing to use for this traffic class.

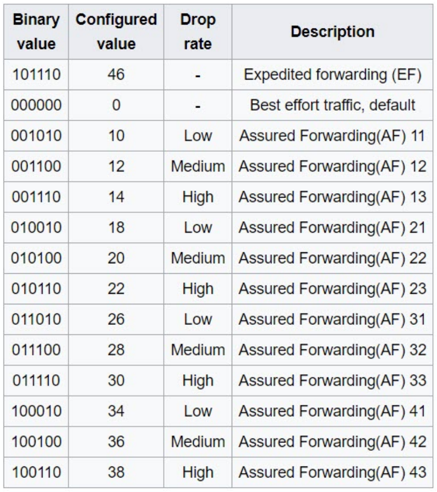
- fq-code1
- fair-queue
- drop-tail
- priority
- random-detect

Default is fair-queue

[set-dscp *<0-63>*]|}

Rewrites the DSCP field in packets in this traffic class to the specified value.

Values are 0–63



Binary value	Configured value	Drop rate	Description
101110	46	-	Expedited forwarding (EF)
000000	0	-	Best effort traffic, default
001010	10	Low	Assured Forwarding(AF) 11
001100	12	Medium	Assured Forwarding(AF) 12
001110	14	High	Assured Forwarding(AF) 13
010010	18	Low	Assured Forwarding(AF) 21
010100	20	Medium	Assured Forwarding(AF) 22
010110	22	High	Assured Forwarding(AF) 23
011010	26	Low	Assured Forwarding(AF) 31
011100	28	Medium	Assured Forwarding(AF) 32
011110	30	High	Assured Forwarding(AF) 33
100010	34	Low	Assured Forwarding(AF) 41
100100	36	Medium	Assured Forwarding(AF) 42
100110	38	High	Assured Forwarding(AF) 43

Default is none

Command Modes Perle(config-pmap)#

Usage Guidelines

Use this command to specify the Quality of Service (QoS) settings applied to the default class. You configure your default traffic in the same way you do with a class. Default is considered a class as it behaves like that. It contains any traffic that did not match any of the defined classes, so it is like an open class, a class without matching filters.

Examples

Set the queue type for this traffic class to random-detect.

```
Perle(config-pmap)#class 10
Perle(config-pmap-c)#queue-type random-detect
```

Related Commands

policy-map

(config-pmap)

(config-pmapRC)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-pmapRC)
{**[bandwidth** ***<1-2000000>*****]** | |	Changes configured bandwidth limit.
[burst ***<1-20000>*****]** |	Configure a burst size in kbytes. Default is 15Kbps
[description ***<LINE>*****]** |	Configure a Policy-Map Rate-Control description.
[latency ***<1-5000>*****]**}	Configure the limit on queue size. This is the maximum amount of time a packet can sit in the Token Bucket Filter. Packets with more latency then this value will be dropped since they are no longer considered useful. Value is 1 to 500 milliseconds Default is 50 milliseconds
Command Modes	Perle(config-pmapRC)#

Usage Guidelines

Use this command to configure parameters for Rate-control policy. This policy is egress only.

Rate Control is a classless policy that limits the packet flow to a set rate. It provides queuing on the Token Bucket filter algorithm. This algorithm only passes packets arriving at a rate which does not exceed an administratively set rate. Traffic is filtered based on the expenditure of these tokens.

Tokens roughly correspond to bytes. Short bursts can be allowed to exceed the limit. Once created, the rate control traffic is stocked with tokens which correspond to the amount of traffic that can be burst in one go. Tokens arrive at a steady rate, until the bucket is full—newly arriving tokens are discarded. To send a packet, the regulator must remove from the bucket a number of tokens equal in representation to the packet size.

Examples

Set the latency for this rate-control policy to 100 milliseconds.

```
Perle(config)#policy-map rate-control factory-RC bandwidth 2000
Perle(config-pmapRC)#latency 100
```

Related Commands

policy-map

(config-pmapPQ)

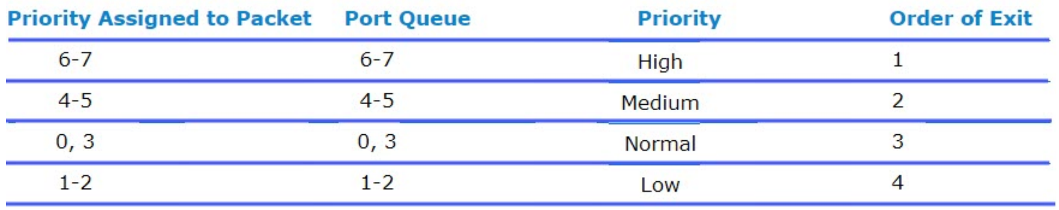
Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-pmapPQ)
{[class *<1-7>* | default] |	Configure a priority queue class identifier.
[description *<LINE>*]}	Configure the description of this Priority Queue policy-map.
Command Modes	Perle(config-pmapPQ)#

Usage Guidelines

Use this command to create a Priority-Queue Policy map. This policy is egress only.

Your IOLAN has four types of outbound traffic queues based on priority: low, normal, medium, and high. These outbound traffic queues are divided into seven priority queues (see table below). The queue priority determines the order of exit for packets in the queue. For example, the packets in a high priority (6–7) queue leave the IOLAN before packets in other queues. If packets continually fill the higher priority queues, those waiting in lower priority queues will not be serviced until the higher priority traffics load finishes.



Priority Assigned to Packet	Port Queue	Priority	Order of Exit
6-7	6-7	High	1
4-5	4-5	Medium	2
0, 3	0, 3	Normal	3
1-2	1-2	Low	4

Examples

This example creates a priority queue called important with a class identifier of 7.

```
Perle(config)#policy-map priority-queue priority
Perle(config-pmapPQ)#class 7trricky sok
```

Related Commands

policy-map

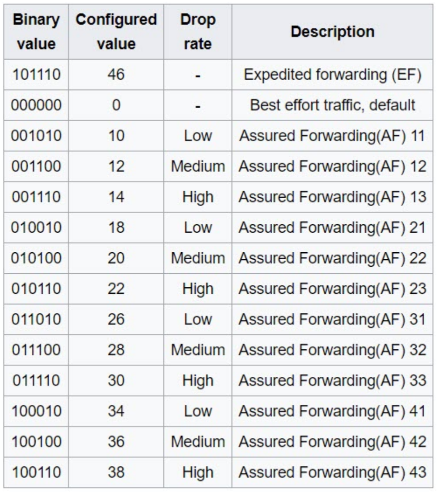
(config-pmapPQ-c)

(config-pmapPQ-c)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-pmapPQ-c)
{**[codel-flows** ***<1-4294967295>*****] |**	Configure the number of flows into which the incoming packets are classified. Values are 1 to 4294967295 Default is 1024
[codel-interval ***<1-4294967295>*****] |**	Configure the interval to the measured minimum delay so as not to become stale. It should be set on the order of the worst-case round trip time (RTT) through the bottleneck to give endpoints sufficient time to react. Values are 1 to 4294967295 milliseconds. Default is 100 milliseconds.
[codel-quantum ***<1-4294967295>*****] |**	Configure the maximum amount of bytes dequeued from a queue at once. Values are 1 to 4294967295 Default is 1514
[codel-target ***<1-4294967295>*****] |**	Configure the minimum standing/persistent queue delay. Values are 1–4294967295 milliseconds Default is 5 milliseconds
[description ***<LINE>*****] |**	Configure a policy map class description.
[queue-limit ***<1-4294967295>]*** **|**	Configure maximum queue size in packets.
[queue-type drop-tail | fair-queue | fq-code1 | priority | random-detect] |	Specifies the type of queuing to use for this traffic class. ● Drop Tail ● Fair-queuing ● fqcode1 ● priority ● random-detect

set-dscp *<0-63>*}	Rewrites the DSCP field in packets in this traffic class to the specified value. Values are 0–63



Binary value	Configured value	Drop rate	Description
101110	46	-	Expedited forwarding (EF)
000000	0	-	Best effort traffic, default
001010	10	Low	Assured Forwarding(AF) 11
001100	12	Medium	Assured Forwarding(AF) 12
001110	14	High	Assured Forwarding(AF) 13
010010	18	Low	Assured Forwarding(AF) 21
010100	20	Medium	Assured Forwarding(AF) 22
010110	22	High	Assured Forwarding(AF) 23
011010	26	Low	Assured Forwarding(AF) 31
011100	28	Medium	Assured Forwarding(AF) 32
011110	30	High	Assured Forwarding(AF) 33
100010	34	Low	Assured Forwarding(AF) 41
100100	36	Medium	Assured Forwarding(AF) 42
100110	38	High	Assured Forwarding(AF) 43

Default is none

Command Modes	Perle(config-pmapPQ-c)#

Usage Guide

Use this command to set parameters for your defined priority queue policy map.

Examples

This example sets the queue-type to fair-queue.

```
Perle(config)#policy-map priority-queue priority-voice
Perle(config-pmapPQ)#class 1
```

Related Commands

policy-map

(config-pmapTL)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-pmapTL)**
{[**class** *<1-4094>* | **default**] |	Configure a priority queue class identifier or default.
[**description** *<LINE>*]}	Configure the description of this Traffic Limiting policy-map.
Command Modes	Perle(config-pmapTL)#

Usage Guidelines

Use this command to configure the parameters for policy map.This traffic policy mechanism is to "police" in coming traffic. The mechanism assign each traffic flow a bandwidth limit. All incoming traffic within a flow in excess of the bandwidth is dropped.This policy can be applied to both ingress and egress packets.

Examples

Creates a policy-map called test-policy.

```
Perle(config)# policy-map test-policy
Perle(config-pmap
```

Related Commands

policy-map

(config-pmapTL-c)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-pmapTL-c)**
{[**bandwidth** *<1-2000000>*] |	Specifies the base guaranteed bandwidth for this traffic class (in Kbps or in percent). Bandwidth must be below the entire bandwidth set for this policy.
[**burst** *<1-20000>*] |	Configure the burst size for this class. Values are 1 to 20000 in Kbytes Default is 15 Kbytes
[**description**] |	Configure the description of this Traffic Limiting policy-map.
[**priority**]}	Specifies the order of evaluation of matching rules (the higher the value, the lower the priority). Values are 0 to 20 Default is 20
Command Modes	Perle(config-pmapTL-c)#

Examples

This example sets the bandwidth to 20000 for this traffic class.

```
Perle(config)#policy-map traffic-class test-traffic
Perle(config-pmapTL-c)#class 10
Perle(config-pmapTL-c)#bandwidth 20000
```

Related Commands

policy-map

radius

Use the no form of this command to negate a command or set to defaults.

Syntax Description	radius
{**server** *<WORD>*}	Configure RADIUS server name.
Command Modes	Perle(config)#radius

Usage Guidelines

Use this command to configure the RADUIS server name.

Examples

This example configures the RADIUS server name.

```
Perle(config)#radius server testrad
```

Related Commands

clear radius

show radius

(config-radius-server)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-radius-server)
{[**address ipv4** *<A.B.C.D>* **acct-port** *<0-65536>* | **auth-port** *<0-65536>*] |	Configure the RADIUS server address. Default port for authentication is 1812 Default port for accounting is 1813
[**key 0** *<WORD>* | **7** *<WORD>* | *<WORD>*] |	Configure an encryption key to be shared with the RADIUS servers.
[**radsec enable**] |	Enable RadSec.
[**retransmit** *<1-100>*] |	Configure the number of retries to the active RADIUS server. Values are
[**timeout** *<1-1000>*]}	Configure the time to wait for the RADIUS server to reply. Values are 1–1000 Default is 5 seconds
Command Modes	Perle(config-radius-server)#

Usage Guidelines

Use this command to configure RADUIS parameters.

Examples

This example sets the timeout to 30 seconds to wait for a reply from a RADIUS server.

```
Perle(config-radius-server)#timeout 5
```

Related Commands

clear radius

show radius

(config-radius-server-radsec)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-radius-server-radsec)
{[**address ipv4** *<A.B.C.D>* | **ipv6** *<X:X:X:X::X>*] |	Configure the address of the RadSec server.
[**certificate-name** *<WORD>*] |	Specific the certificate file name.
[**private-key-name** *<WORD>*] |	Enter the RadSec private key.
[**protocol tls | dtls**] |	TLS–Transport Layer Security DTLS–(Data Transport Layer Security)–a more secure communication method, used on top of the TLS protocol, to communicate with clients securely without eavesdropping, unauthorized accesses, or message tampering. Default is TLS
[**secure-port** *<1-65535>*] |	Enter the secure port number Default is 2083
[**trustpoint-name** *<WORD>*]}	Enter the filename for the trustpoint.
Command Modes	Perle(config-radius-server-radsec)#

Usage Guidelines

Use this command to configure RadSec parameters.

Examples

This example

```
Perle(config-radius-server)#timeout 5
```

Related Commands

clear radius

show radius

radius-server

Use the no form of this command to negate a command or set to defaults.

Syntax Description	radius-server
{[deadtime *<1-1440>*] |	Sets the time the IOLAN ignores unresponsive RADIUS servers.
[key 0 *<WORD>*7 *<WORD>* | *<WORD>*] |	Configure an encryption key to be shared with the RADIUS servers.
[retransmit *<1-100>*] |	Configure the number of retries to the active RADIUS server.
[timeout *<1-1000>*]}	Configure the time to wait for the RADIUS server to reply.
Command Modes	Perle(config)#radius-server

Usage Guidelines

Use this command to configure RADUIS server parameters.

Examples

This example sets the radius server name.

```
Perle(config)#radius-server
```

Related Commands

clear radius

show radius

remote-management

Syntax Description	remote-management
Command Modes	Perle(config)#remote-management

Usage Guidelines

Use this command to enter sub-command mode for remote management configuration.

Examples

This example enables remote management config mode.

```
Perle(config)#remote-management
Perle(config-remote-mgmt)#
```

Related Commands

(config-remote-mgmt)

(config-remote-mgmt)

Use the no form of this command to negate a command or set to defaults. [

Syntax Description	(config-remote-mgmt)
{[restful-api cookie-max-age] |	Enables set-cookie based authentication. Values are 1 to 20160 (14 days) Default is 1440 minutes (24 hours)
[http local-port] |	If enabled, the IOLAN accepts and responds to HTTP Restful client requests. Values for local port are 80, 1025 to 65535 Default local port is 8080 Default is Disabled
[https local-port] |	If enabled, the IOLAN accepts and responds to HTTPS Restful client requests. Values for the local port are 443, 1025 to 65535 Default is Disabled
[jwt [claims aud <*WORD*>] |	**Claim sets:** **aud: audience**—identifies the recipients that the JWT is intended for. This tends to be the "client id" or "client key" of the application that the JWT is intended to be used by. It allows the client to verify that the JWT was sent by someone who actually knows who they are.
[exp <*1-3153600*>] |	**exp: expiration time**—identifies the expiration time on and after which the JWT must not be accepted for processing Values are 1–3153600 seconds Default is 3153600 seconds
[iat: issued at] |	Identifies the time on which the JWT will start to be accepted for processing.
[iss <*WORD*>] |	Identifies principal that issued the JWT.
[jti <*WORD*>] |	case sensitive unique identifier of the token
[nbf <*1-31336000*>] |	JWT will start to be accepted for processing at this time. Values are 1–3156000 seconds
[sub: subject] |	identifies the subject of the JWT

jws algorithm es256 | es384 | es512 | hs256 | hs384 | hs512 | ps256 | ps 384 | ps512 | rs256 | rs384 | rs512 | none] |	**Algorithm types:** es256, es384, es512, hs256, hs384, hs512, ps256, ps384, ps512, none
key import terminal]}	**key**—import the key via the terminal screen. To end entry type "quit" on a blank line by itself.
Command Modes	Perle(config-remote-mgmt)#

Usage Guidelines

Use this command to configure RESTful API options.

JSON Web Token (JWS) is an Internet standard way to securely transfer information between devices as a JSON object. This information can be verified and trusted because it is digitally signed. JSON Web Tokens (JWTs) can be signed using an algorithm or a public/private key pair.

Examples

This example sets the local port for HTTPS to 1025.

```
Perle(config-remote-mgmt)#restful-api https local-port 1025
```

route-map

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**route-map**
{<***WORD***> ***<1-65535>*** **[deny** ***<1-65535>*** **| permit** ***<1-65535>*****]**}	Insert, delete, deny, or permit from existing route map table.
Command Modes	Perle(config)#route-map

Usage Guidelines

Use this command to create route maps or enter route map command mode.

Examples

This example creates a route map called test-route.

```
Perle(config)#route-map test-route
```

Related Commands

show route-map

(config-route-map)

(config-route-map)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-route-map)**

{call *<WORD>* |	Calls to another route map.
[continue *<1-65535>* |	Calls to another rule within the current route map. The new route map rules is called after all set actions specified in the route map rule have been performed.
[description *<LINE>* |	Configure a route map description.
[match | [as-path *<WORD>*] | [community *<1-500>*] | [extcommunity *<1-500>*] | [interface bvi *<1-9999>*] | [dialer *<0-15>*] | [ethernet *<1-24>. <1-4000>*] | [openvpn-tunnel *<0-999>*] | [tunnel *<0-999>*] | [ip address *<1-199>* | *<1300-2699>* | prefix-list] | [ipv6 *<WORD>* | prefix-list] | [metric *<1-4294967295>*] | [origin egp | igp | unknown] | [peer *<A.B.C.D>*] | [tag *<1-65535>*] |	Defines a match condition based on parameter.
[on-match goto *<1-65535>* | next |	Specifies an alternative exit policy for a route map.
[set aggregator as *<1-4294967295> <A.B.C.D>*] |	Set BGP aggregator number and IP address.
[as-path exclude *<1-4294967295>* | prepend *<1-4294967295>*] |	**Excludes**—removes the AS path from a BGP AS-path attribute (up to 10 numbers) **Prepend**—prepends to the AS path of the route (up to 10 numbers)
[atomic-aggregate] |	Sets the atomic aggregate attribute in a route.
[comm-list *<1-500>* delete] |	Set the BGP community list for deletion.
[community *<1-4294967295>* | *<AA:NN>* |	Configure the community number or AA:NN.
internet | local-as | no-advertise | no export] |	Internet (well know community) local-AS—do not send outside local AS no-advertise—do not advertise to any peer no-export—do not export to next AS
[ext-community rt *<AA:NN>* | soo *<AA:NN>*] | [ip nexthop *<A.B.C.D>*]	Configure the extended community list or AA:NN.
[ip nexthop *<A.B.C.D>*] |	Modifies the next hop destination of a route.

[ipv6 nexthop global ***<X:X:X:X::X>*** **| local** ***<X:X:X:X::X>*****] |**	Modifies the IPv6 next-hop destination of a route.
[local-preference ***<0-4294967295>*****] |**	Modifies the BGP local-pref attribute in a route.
[metric ***<1-4294967295>*****] |**	Modifies the metric of a route.
[metric-type ***<type-1>*** **|** ***<type-2>*****] |**	Specifies the OSPF external metric-type for a route.
[origin epg | igp | unknown] |	Modifies the BGP origin code of a route.
[originator-id ***<A.B.C.D>*****] |**	modifies the BGP originator ID attribute of a route.
[src ***<A.B.C.D>*****] |**	Modifies th BGP source address for the route.
[tag ***<1-65535>*****] |**	Modifies the OSPF tag value of a route.
[weight ***<0-4294967295>*****]**}	Modifies the BGP weight of a route.
Command Modes	Perle(config-route-map)#

Usage Guidelines

Use this command to configure route map parameters.

Examples

This rule defines a match rule for community list BGP 50.

```
Perle(config-route-map)#match community 50
```

Related Commands

show route-map

router

Use the no form of this command to negate a command or set to defaults.

Syntax Description	router
{**[bgp** ***<1-4294967295>*****] |**	Configures Broader Gateway Protocol (BGP) routing protocol on the IOLAN. If using your IOLAN to connect to the Internet, BGP should be enabled. Configure the 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.

{[bgp *<1-4294967295>*] |	Your service provider will assign you the first three digit for ASN, the last two digits should be unique. Values are 1–4294967295
[ospf] |	Configure OSPF routing protocol on the IOLAN. Open Shortest Path First (ospf) is a protocol used to find the best paths for packets as they pass through a set of connected networks. OSFP was designed to replace the RIP protocol as it optimizes the updating up of the routing table. OSPF should be enabled on your IOLAN.
[rip]}	Configure RIP routing protocol on the IOLAN. Routing Information Protocol (rip). Older protocol for finding the shortest path for routing information using a routing metric/hop count algorithm. RIP should be enabled on your IOLAN if there are older routers on your network that need to use RIP.
Command Modes	Perle(config)#router

Usage Guidelines

Use this command to select the routing protocol for your IOLAN.

Examples

This example sets the routing protocol to BGP.

```
Perle(config)#router bgp 10
```

Related Commands

show ip ospf

show ip rip

(config-router)—BGP

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-router)-BGP** **Some parameters may not be available on some firmware versions or models.**
{[bgp address-family ipv4 | ipv6 unicast] |	Enters address family mode.
[aggregate address *<A.B.C.D>* *<A.B.C.D>* as-set | summary-only] |	Specifies the block of addresses to be aggregated. Specifies that the routes resulting from the aggregation include the AS-set.
[summary-only] |	Specifies that aggregated routes are summarized. These routes will not be advertised.

[bgp always-compare-med] |	Configure BGP parameters. Directs the IOLANto compare the MED for paths from neighbors in different autonomous systems. Default is disabled
[bestpath as-path confed | ignore] | [compare-router-id] | [med confed | missing-as-worst] |	**best-path** **as-path** [confed | ignore]—directs the IOLAN to compare the AS paths during best-path selection. Default is does not compare **compare-router-id**—directs the IOLAN to compare identical routes received from different external peers during best path selection. Default is does not compare **med** confed | missing-as-worst—direct the IOLAN to compare the Multi Exit Discriminator (MED) among paths learned from confederation peers during best path selection.
[client-to-client reflection] |	Enables or disables route reflection from a BGP route reflector to clients. Default is disabled
[cluster-id ***<1-4294967295> <A.B.C.D>*****] |**	Sets the cluster ID for a BGP route reflection cluster as a 32 bit number Values are 1–4294967295 or IP address Default is none
[confederation identifier ***<1-4294967295>*** **| peers** ***<1-4294967295> <1-4294967295>*****] |**	Defines a BGP confederation. Values are AS number 1–4294967295 Peers range from 1–4294967295 to 1–4294967295 Values are 128 peers
[dampening ***<1-45>*** **|** ***<1-20000>*** **|** ***<1-20000>*** **|** ***<1-255>*****] |**	**dampening**—enables or disables route dampening and sets IOLAN dampening value. **half-life**—1 to 45 mins Default is 15 mins **reusing-route**—1 to 20000 Default is 750 **start-suppress-time**—to 20000 Default is 20000 **max-suppress-time**—1 to 255 Default is 4 x of half life

[deterministic-med] | [enforce-first-as] | [fast-external-failover] |	**deterministic-med**—enables of disables enforcing of deterministic MED **enforce first-as**—forces eBGP peers to list AS number at the beginning of the AS_path attribute in coming updates Default is disabled **fast-external-failover** —immediately reset session if a link to a directly connected external peer goes down Default is disabled
[graceful-restart stalepath-time ***<1-3600>*****] |**	Enables or disables grateful restart of the BGP process Default is enabled Grateful stale-time is 1-3600 seconds Graceful stale time default is 360 seconds
[log-neighbor-changes] |	Log neighbor up/down and reset reason Default is disable
[network import-check] |	Check BGP network route exists in IGP Default is enabled
[router-id] |	Configure a fixed BGP router ID for the router, overriding the automate ID selection process Default automatically selected by BGP
[distance ***<1-255> <A.B.C.D> <A.B.C.D/nn>*****] |**	Enter an **Administrative Distance**. (AD) is a value that your IOLAN uses to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance is the reliability of a routing protocol. A static route is normally set too The smaller the administrative distance value, the more reliable the protocol. Administrative Distance is locally significant, it is not advertised to the network. Range is 1-255 (with 1 being the most reliable) and 255 is route not used or unknown Configure a source IP prefix address and mask.
[bgp distance ***<1-255> <1-255> <1-255>*****] |**	**BGP distance** Distance for external router to AS Values are 1 to 255 Default 20 Distance for internal outer to AS Values 1 to 255 Default is 200 Distance for local router Value 1 to 255 Default 200

[maximum-paths *<1-64>* **ibgp** *<1-64>***] |**	Configure the maximum number of eBGP/iBGP paths to a destination. ebgp values are 1 to 255 Default is 1 ibgp values are 1 to 255 Default is 1
[neighbour *<A.B.C.D>* *<X:X:X:X::X>***] |**	Configure neighbor configuration. Specify an IPv4 or IPv6 address.
[advertisement-interval *<0-600>***] |**	Configure the minimum interval between sending BGP routing updates. Values 0 to 600 Default eBGP is 30 secs Default iBGP peers is 5 seconds
[allowas-in *<1-10>***] |**	Allows or disallows receiving BGP advertisements containing the AS path of the local router. Default readvertisement is disabled. Default is 3
[asoverride] |	Override ASN's in outbound updates if AS–path equals remote–AS. Only applies to eBGP neighbor. Default is disable
[attribute-unchanged as-path | med | next-hop] |	Allows the IOLAN to send updates to a neighbor with unchanged attributes. Value is on for all if no option provided Default is disabled
[capability dynamic] |	Advertise dynamic capability to this neighbor. Default is session is brought up with minimal capability on both sides
[capability dynamic | orf prefix-list both | receive | send] |	Advertises support for Outbound Route Filtering (OFR) for updating BGP capabilities advertised and received from this neighbor. Default is the session is brought up with minimal capability on both sides.
[default-originate] |	Enables or disables forwarding of the default route to a BGP neighbor. Default is disabled
[description *<LINE>***] |**	Provide a description for a BGP neighbor.
[disable-connected-check] |	Enables a directly connected eBGP neighbor to peer using a loopback address without adjusting the default TTL of 1. Default is off

[distributed-list *<1-99>* in | out *<1300-2699>* in | out] |	Applies an access list to filter inbound/outbound routing updates from this neighbor. Default is none
[dont't-capability-negotiate] |	Disables BGP capability negotiation Default is capability negotiation is performed.
[ebgp-multihop *<1-255>*] |	Allows you to establish eBGP peer relationships between routers that aren't directly connected to one another. Default is only directly connected neighbors are allowed
[filter-list *<WORD>*] |	Applies an AS–path list to routing updates to this neighbor Default is none
[local-as *<1-4294967295>* no-prepend] |	Defines a local autonomous system number for eBGP peering Default is none
[maximum-prefix *<1-4294967295>*] |	Configure the maximum number of prefixes to accept from this neighbor before that neighbor is taken down. Values are 1–4294967295 Default is none
[next-hop-self] | [override-capability] | [passive] | [password *<LINE>*] |	Sets the local router as the next ho for this neighbor Default is disable
[override-capability] |	Overrides capability negotiation to allow a peering session to be established with a neighbor that does not support capabilities negotiation Default is a session cant be established if the neighbor does not support capability negotiation.
[passive] |	Directs the router not to initiate connections with this neighbor
[password *<LINE>*] |	Configure a BGP MD5 password Default is none
[port *<1-65535>*] |	Specifies the port on which the neighbor is listening for BGP signals Values are 1 to 65535 Default port is 179
[prefix-list *<WORD>* in | out] |	Applies this prefix list filter updates to/from this neighbor Default is none

[remote-as *<1-4294967295>*] |	Configure the autonomous system number of the neighbor. Default is none
[remove-private-as] |	Directs the IOLAN to remove private AS numbers from updates sent to this neighbor (eBGP only) Default is disable (do not remove)
[route-map *<WORD>* in | out] |	Applies a route map to filter updates to/from this neighbor Default is none
[route-reflector -client] |	Specify this neighbor as a route reflector client (iBGP only) Default is disabled
[route-server-client] |	Specify this neighbor as a route server client Default is disable
[send-community both | extended | standard] |	Enables or disables the sending of community attributes to the specified neighbor Value— no type specified send standard attributes Default is both
[shutdown] |	Administratively shuts down a BGP neighbor Default is disabled
[soft-reconfiguration] |	Directs the IOLAN to store received routing updates.
[strict-capability-match] |	Directs the router to strictly match the capabilities of the neighbor Default is disable
[timers *<0-65535> <0-65535>*] |	**timers**— **keepalive interval** Values are 0—-65535 Default is 60 seconds **holdtime** Value are 0-65535 Default is 180 seconds
[connect *<0-65535>*] |	**connect** Values are 0-65535 Default is 120 seconds
[ttl-security hops *<1-254>*] |	Configure the time-to-live (ttl) security hop count. This option and ebgp-multihop cannot be set at the same time Values are 1 to 254 hops Default is 1

[unsuppress-map *<WORD>*] |	Directs the IOLAN to selectively advertise routes suppressed by aggregating addresses, based on a route map Value specify a router map
[update-source interface interface bvi *<1-9999>* | dialer *<0-15>* | ethernet *<1-24>*sfp<1-2>. *<1-4000>* | openvpn-tunnel *<0-999>* | tunnel *<0-999>* | *<X:X:X:X::X>*] |	Specifies the source ip address or interface for routing updates Default is none
[weight *<1-65335>*] |	Defines a default weight for routes from this neighbor Values are 1-65335 Default is routes learned from a BGP neighbor have a weight of 0. Routes sourced by the local router have a weight of 32768
[network *<A.B.C.D>* *<A.B.C.D>* | backdoor | route-map *<WORD>*] |	Configure a network to be advertised by the BGP routing process. **Backdoor**—indicates that this network is reachable by a back door route. A back door network is considered to be like a local network but is not advertised. **Route-map**—specifies a configured route map to be used when advertising the network Default is none
[redistribute connected | kernel | ospf | rip | static | metric *<1-4294967295>* | route-map *<WORD>*] |	Select route type for redistribution. BGP. Connected (directly attached subnet or host) • Kernel • OSPF • RIPng • Static Select a router map from the drop-down list. Configure the metric used by the routing protocol to calculate the best path to a given destination. Value range is 1-4294967295 A route map consists of a series of statements to check if the route matches the policy, then it permits or denies the route. Default is none

[timers bgp ***<0-65535> <0-65335>*****]**}	Configure BGP times globally for the local IOLAN. Keepalive interval Values are 0-65535 Default is 60 seconds Hold-time Values are 0-65535 Default is 180 seconds
Command Modes	Perle(config-router)#

Usage Guidelines

Use this command to configure BGP protocol parameters.

Examples

This example sets BGP timers keepalive to 10 seconds and hold time to 20 seconds.

```
Perle(config-router)#timers bgp 10 20
```

Related Commands

show bgp

(config-router-RIP)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-rtr)**
{**rip default-information originate] |**	Controls distribution of default information
[default-metric ***<1-16>*****] |**	Configure the metric for redistributed routes.
[distance ***<1-255>*****] |**	Enter an **Administrative Distance**. (AD) is a value that your IOLAN uses to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance is the reliability of a routing protocol. A static route is normally set too . The smaller the administrative distance value, the more reliable the protocol. Administrative Distance is locally significant, it is not advertised to the network. Range is 1-255 (with 1 being the most reliable) and 255 is route not used or unknown

[distribution-list [<*WORD*> | prefix <*WORD*>] | [in | out] [bvi <*1-9999*>] | [dialer <*0-15*>] | [ethernet <*1-x*> || sfp <*1-2*>. <*1-4000*>] | [openvpn-tunnel <*0-999*>] | [tunnel <*0-999*>] |	Filters networks in routing updates. Select the access list for IPv6 name or filter prefixes in routing updates. Specific whether the filter is for inbound or outbound. Specify the interface to apply this distribution list to.
[network <*A.B.C.D*> <*A.B.C.D*>] |	Enables routing on a network.
[passive-interface bvi <*1-9999*> | dialer <*0-15*> | ethernet <*1-x*> || sfp <*1-2*>. <*1-4000*>| openvpn-tunnel <*0-999*> | tunnel <*0-999*> | all] |	Suppress routing updates on an interface.
[redistribute connected | kernel | ospf | rip | static | metric <*1-4294967295*> | route-map <*WORD*>] |	Redistribute information from other routing protocol.
[route <*X:X:X:X::X*>/<*0-128*>] |	Static route setup.
[timers basic <*0-65535*> <*0-65535*> <*0-65535*>]}	**Timers basic—** Update period 0-65535 Route timeout period 0-65535 Route hold down period in seconds 0-65535
Command Modes	Perle(config-rtr)#

Usage Guidelines

Use this command to configure RIP protocol parameters.

Examples

This example sets timer for RIP updates to every 5 seconds.

```
Perle(config-router)#timers basic 5
```

Related Commands

router

(config-router)—OSPF

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-router)-OSPF**

{**[ospf [area** *<0-4294967295>* **|** *<A.B.C.D>***] |**	Configure OSPF area parameters. **Area**—OSPF area ID in decimal format or IP address format
[authentication message-digest] |	**Authentication**—enables message-digest authentication
default-cost *<1-6777215>* **|**	**Default-cost**—Configure a default metric to be applied to routes being distributed into OSPF. Range is 0 to 16777214 Default is none
nssa no-summary | translate |-always | translate-candidate | translate-never] |	**NSSA** ● No summary—Configure the OSFP VRF instance to not inject the inter-area routes into NSSA. ● Candidate translate—Configure the NSSA-ABR always to translate election. Default is enabled ● Always translate—Configure the NSSA-ABR never to translate. Default is enabled ● Never translate—Configure the NSSA-ABR server never to translate. By default this is disabled
[range *<A.B.C.D> <A.B.C.D>* **advertise | not-advertise cost** *<0-16777215>* **| substitute** *<A.B.C.D> <A.B.C.D>* **cost** *<0-16777215>***]**	**Range**—Configure a prefix specified as IP address and subnet mask. ● **Advertise**—sets the address range status to advertise and generates a Type 3 summary LSA. ● **Not-advertise**—sets the address range status to Do Not Advertise. The Type 3 summary LSA is suppressed and the component networks remain hidden from other networks. ● **Substitute**—(network prefix to be announced instead of range). The default is advertise ● **Cost**—Configure the metric for this area range. Range is 0 to 16777215
[shortcut enable | disable | default] |	**Shortcut**—This parameter allows to "shortcut" routes (non-backbone) for inter-area routes. ● enable—use this area for shortcutting ● disable—never use this are for route shortcutting ● default—use this area for shortcutting—only if the ABR does not have a link to the backbone area or this link was lost

[stub no-summary] |	**stub no-summary**—no-summary option creates a totally stubby area. A totally stubby area keeps only the intra-area routes (the O routes), and for any inter-area routing, it has a default route
[virtual-link *<A.B.C.D>*] |	**Virtual Link IP Address**—IPv4 address of this virtual link.
[authentication-key *<WORD>* | message-digest message-digest-key *<1-255>* md5 *<LINE>* | null] |	**Authentication**—Configure a password used by neighboring routers for simple password authentication. It can be any continuous string of up to eight characters. There is no default value. • None—no password • Authentication-key—Configure an authentication key for simple password authentication. • Message-digest—(Optional) Identifies the key ID and key (password) used between this router and neighboring routers for MD5 authentication.
[dead-interval *<1-65535>*] |	**Dead-interval**—Configure the interval during which at least one hello packet must be received from a neighbor before the IOLANdeclares that neighbor as down (dead).) As with the hello interval, this value must be the same for all IOLANs attached to a common network. Default is 4 times the hello interval Default is 40 seconds
[hello-interval *<1-65535>*] |	**Hello interval**—Configure the hello packet time interval for hello packets sent on an interface. The default is 10 seconds.
[retransmit-interval *<1-65535>*] |	**Retransmit interval**—Configure the time between link-state advertisement (LSA) retransmissions for adjacencies that belong to the virtual link. Default is 5

[transmit-delay*<1-65535>*] |	**Transmit delay**—Before a link-state update packet is propagated out of an interface, the routing device increases the age of the packet. The transit delay sets the estimated time required to transmit a link-state update on the interface. By default, the transit delay is 1 second.You should never have to modify the transit delay time. To avoid LSAs from aging out during transmission, set an LSA retransmission delay especially for low speed links. Default is 5 seconds.
[auto-cost reference-bandwidth *<1-4294967>*] |	Directs the IOLAN to use reference bandwidth method for calculating administrative costs. Default reference bandwidth is 108 Mbps
[capability opaque] |	Enables support for opaque link-state advertisement as described in RFC2370. Default is disabled
[compatibility rfc1583] |	Indicates whether handing of AS external routes should comply with RFC 1583. Default is disabled.
[default-information originate always] |	Sets the characteristics of an external default route originated into an OSPF routing domain. Default is off
[default metric *<0-16777214>*] |	Configure a default metric to be applied to routes being distributed into OSPF. Range is 0–16777214 Default is non
[max-metric router-lsa administrative | on-shutdown *<5-86400>* | on-startup *<5-86400>*] |	Enables or disables the OSFP maximum / infinite-distance metric. **Administratively**—administratively applied for an indefinite period **on shutdown**—advertise stub-router prior to full shutdown of OSPF **on-startup**—advertise a maximum metric at startup. on shutdown/on-startup value is 5–86400 seconds Range is 5 to 86400 seconds Default is 600 seconds

[neighbor poll-interval *<1-65535>* priority *<0-255>*] |	Configure the dead-router polling interval for non-broadcast neighbor. Values are 1-65535 in seconds Default is 120 in seconds Priority of non-broadcast neighbor. Values are 0-255 Default is 1
[network *<A.B.C.D>* *<A.B.C.D>* area *<0-4294967295>*] |	Configure IPv4 network address. Configure IPv4 wildcard address. Configure the area id or ip address
[passive-interface bvi *<1-9999>* | dialer *<0-15>* | | ethernet *<1-24>*. *<1-4000>* | openvpn-tunnel *<0-999>* | tunnel *<0-999>*] |	Suppresses routing updates on an interface or all interfaces.
[all | redistribute connected | kernel | ospf | rip | static | metric *<1-4294967295>* | route-map *<WORD>*] |	Redistributes information from other routing protocols. Select the type of route: ● BGP ● Connected (directly attached subnet or host) ● Kernel ● OSPF ● Static Select the route map.
[refresh timer *<5-1800>*] |	The IOLAN automatically updates link-state information with its neighbors. Only an obsolete information is updated when age has exceeded a specific threshold. Range is 10–1800 seconds Default is 1800 seconds
[router-id *<A.B.C.D>*] |	Configure a global OSPF router ID. If this command is not configured, OSFP chooses an IPv4 address as the router ID from one of its interfaces. If this command is used on an OSPF instance that has neighbors, OSFP uses the new router ID at the next reload or restart of OSFP.Router-ID for this OSPF process.

[timers throttle spf *<1-600000> <1-600000><1-600000>*]}	Delay between receiving a change to SPF calculation in milliseconds. Range is 1–600000 milliseconds Default is 1 milliseconds Delay between first and second SPF calculation. Range is 1–600000 milliseconds Default is 1 milliseconds Maximum wait time in milliseconds for SFP calculations. Range is 1–600000 milliseconds Default is 1 milliseconds
Command Modes	Perle(config-router)#

Usage Guidelines

Use this command to configure OSPF protocol parameters.

Examples

This example sets opaque feature for OSPF.

```
Perle(config-router)#capability opaque
```

Related Commands

show ip ospf

(config-router)—RIP

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-router)**
[rip default-information originate] |	Controls distribution of default information.
[default-metric *<1-16>*] |	Configure the metric for redistributed routes.
[distance *<1-255>*] |	Enter an **Administrative Distance**. (AD) is a value that your IOLAN uses to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance is the reliability of a routing protocol. A static route is normally set too 1. The smaller the administrative distance value, the more reliable the protocol. Administrative Distance is locally significant, it is not advertised to the network. Range is 1-255 (with 1 being the most reliable) and 255 is route not used or unknown

[distribution-list [*<1-99>* | *<1300-2699>* | prefix *<WORD>*] | [in | out] [bvi *<1-9999>*] | [dialer *<0-15>*] | [ethernet *<1-24>. <1-4000>*] | [openvpn-tunnel *<0-999>*] | [tunnel *<0-999>*] |	Filters networks in routing updates. Select the IP access list number or filter prefix list name. Specific whether the filer is for inbound or outbound. Specify the interface to apply this distribution list to.
[neighbor *<A.B.C.D>*] |	Configure a neighbor router.
[network *<A.B.C.D> <A.B.C.D>*] |	Enables routing on a specified interface or network.
[passive-interface bvi *<1-9999>* | dialer *<0-15>* | ethernet *<1-24>. <1-4000>*| openvpn-tunnel *<0-999>* | tunnel *<0-999>* | all] |	Suppress routing updates on an interface.
[redistribute connected | kernel | ospf | rip | static | metric *<1-4294967295>* | route-map *<WORD>*] |	Redistribute information from other routing protocol.
[timers basic *<5-2147483> <5-2147483> <5-2147483>*]}	**Timers basic—** Interval between updates for RIP Values are 5-2147483 in seconds Default is Invalid in secnds Values are 5–2147483 Default is Flush in seconds Values are 5-2147483

Command Modes	Perle(config-router)#

Usage Guidelines

Use this command to configure RIP protocol parameters.

Examples

This example sets timer for RIP updates to every 5 minutes.

```
Perle(config-router)#timers basic 5
```

Related Commands

router

sdm

Use the no form of this command to negate a command or set to defaults.

Syntax Description	sdm
{prefer default | dual-ipv4-and-ipv6 default}	Set IPv4 and IPv6 protocols on your IOLAN.
Command Default	(both IPV4 and IPV6 enabled)
Command Modes	Perle(config)#sdm

Usage Guidelines

The sdm command is used to set IP protocols on your IOLAN.

Examples

This example sets your IOLAN for both IPv4 and IPv6 traffic.

```
Perle(config)# sdm prefer dual-ipv4-and-ipv6 default
```

serial

Use the no form of this command to negate a command or set to defaults.

Syntax Description	serial
{[accounting *<WORD>* | default] |	Configure accounting parameters.
[advanced [break off | on] | data_logging_buffer_size *<1-2000>* | [flush-on-close off | on] | [line-menu-string *<WORD>*] | [monitor-connection-every *<1-32767>*] | monitor-connection-number *<1-32767>*] |	Configure advanced features for serial devices. Default for line-menu-string is ~menu
[monitor-connection-timeout *<1-32767>* | single-telnet off | on] |	
[authentication aaa login-authentication *<WORD>* | default] |	Configure authentication parameters.
[authorization exec *<WORD>* | default] |	Configure authorization parameters.

[modbus gateway addr-mod embedded | re-mapped] | [broadcast on | off] | char-timeout ***<10-10000>*** **| [exceptions off | on] | [idle-timer** ***<0-300>*****] | [ip-aliasing off | on] | mess-timeout** ***<10-10000>*** **| next-req-delay** ***<0-1000>*** **| port** ***<1-65535>*** **| remapped-id** ***<1-247>*** **| [req-off | on] | [ssl on | off] |**	Configure modbus gateway parameters.
[port buffering key-stroke-buffering on | off] | mode both | local | off | remote | nsf-directory ***<WORD>*** **| nfs-encryption off | on | [nfs-host** ***<A.B.C.D> <WORD> <X:X:X:X::X>*****] | syslog [level alert | critical | emergency | error | info | notice | warning] | off | on] | [time-stamp off | on] | view-port-buffer-string** ***<WORD>*****] |**	Configure port buffering parameters.
[trueport [remap 110 | 1200 | 134 | 150 | 1800 | 19200 | 200 | 2400 | 300 | 38400 | 4800 | 50 | 600 | 75 | 9600] | 115200 | 1200 | 1800 | 19200 | 23400 | 2400 | 38400 | 4800 | 57600 | 600 | 9600 | custom] |	Configure remap baud rates for Trueport devices.
[vmodem-phone entry ***<1-8>*** **phone-number** ***<phone -number>*** **| host** ***<A.B.C.D> <WORD> <X:X:X:X::X> <tcp-port>*****]}**	Configure parameters for virtual modem.
Command Modes	Perle(config)#serial

Usage Guidelines

Serial advanced feature settings

Examples

This example sets the vmodem phone number to 416-666-9900 for host 172.16.77.88.

```
Perle(config)#serial vmodem entry 1 phone-number 416-666-9900 host 172.16.77.88
```

Related Commands

serial

show serial

service

Use the no form of this command to negate a command or set to defaults.

Syntax Description	service
{[**dhcp relay-agent | server] |**	Enables DHCP server or relay agent.
[dhcpv6 server] |	Enables DHCPv6 server.
[sequence-numbers] |	Stamps the logger messages with a sequence number.
[timestamps log datetime | localtime | msec | show-time-zone | year] | uptime]}	Time stamp with date, time, and system uptime.

Command Modes	Perle(config)#service

Usage Guidelines

Use this command to configure parameters for DHCP relay agent or server.

Examples

This example sets date, time, and year to DHCP log messages.

```
Perle(config)#service timestamp log datetime localtime year
```

Related Commands

logging

snmp-server

Use the no form of this command to negate a command or set to defaults.

Syntax Description	snmp-server

{**[community** ***<WORD>*** **ip-access** ***<A.B.C.D>*** **| network** ***<A.B.C.D> <A.B.C.D>*** **|** ***<WORD>*** **|** ***<X:X:X:X::X:X>*** **ro | rw] |**	Configure community strings and access privileges. IP-access • *<A.B.C.D>* IPv4 address of SNMP client allowed to contact system • network *<A.B.C.D> <A.B.C.D>* subnet of SNMP clients allow to contact the system • *<WORD>* host name of the SNMP client allow to contact the system • *<X:X:X:X::X:X>* IPv6 address of the host allow to contact the system ro–read only access with this community string rw–community access with this community string
[contact ***<LINE>*****] |** |	Configure the contact name. (mib object sysContact).
[enable traps | [alarms ***<2 | 3>*** **| major | minor] | authentication | bgp entity | envmon | interface-ip | ipsec | lldp | network-watchdog | openvpn | ospf | [snmp authentication | coldstart | linkdown | linkup | warmstart] | software-update] |**	Enables SNMP traps and inform messages.
[engine-id ***<TEXT>*****] |**	Configure the default engine-id. Your uses the MAC address of the Ethernet interface to ensure that the Engine-id is unique to this agent. To set the engine id back to default, enter "".
[group ***<WORD>*****] |**	Configure a SNMPv3 user security model.
[host [***<A.B.C.D>*** **|** ***<WORD>*** **|** ***<X:X:X:X::X>*****]** ***<WORD>*****] | [version 2c** ***<WORD>*** **udp-port** ***<0-65535>*** **| version 2c** ***<WORD>*** **udp-port** ***<0-65535>*** **| version 3 engine-id** ***<WORD>*** **| informs engine-id** ***<WORD>*** **| traps engine-id** ***<WORD>*****] | user** ***<WORD>*** **auth md5 0** ***<WORD>*** **priv [aes 0 | 7 |** ***<WORD>*** **| sha 0** ***<WORD>*** **priv [aes 0 | 7 |** ***<WORD>*** **| udp-port** ***<0-65535>*** **|** ***<WORD> <WORD>*** **auth md5 0** ***<WORD>*** **priv [aes 0 | 7 |** ***<WORD>*** **| sha 0** ***<WORD>*** **priv [aes 0 | 7 |** ***<WORD>*** **|**	Configure hosts to receive SNMP notifications. Engine ID is the remote Engine ID. Configure SNMP V3 user parameters.

[listen-address *<A.B.C.D>* | *<X:X:X:X::X:X>* udp-port *<0-65535>*] |	Configure the listen address for incoming requests.
[location *<LINE>*] |	Configure the name for MIB object sysLocation. This is the physical location of this node.
[user *<WORD>* *<WORD>* v3 [auth md5 | sha *<WORD>* priv aes *<WORD>*] [encrypted auth md5 *<WORD>* priv aes *<WORD>* | sha *<WORD>*] |	Configure options for SNMP V3 user.
[view *<WORD>* excluded *<WORD>*]}	Configure a SNMPv3 MIB family view, Excludes this family MIB from the view.
Command Modes	Perle(config)#snmp-server

Usage Guidelines

Use this command to configure SNMP server parameters.

Examples

This example sets community name to public and contact person to admin, then enable trap messages for authentication.

```
Perle(config)#community public
Perle(config)#snmp-server contact admin
Perle(config)#snmp-server enable traps authentication
```

Related Commands

show snmp

tacacs

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**tacacs**
{server *<WORD>*}	Configure TACACS+ server name.
Command Modes	Perle(config)#tacacs

Usage Guidelines

Use this command to configure TACACS+ server name.

Examples

This example specifies the name of the TACACS+ server as TACTEST.

```
Perle(config)#tacacs server TACTEST
```

Related Commands

clear tacacs

show tacacs

(config-tacacs-server)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-tacacs-server)**
{[**address ipv4** <*hostname* | <*A.B.C.D*> | **ipv6** <*hostname* | *X:X:X:X::X*>] |	Configure the IPv4 or IPv6 address for your TACACS server.
[**key 0** <*WORD*> | **7** <*WORD*> | <*WORD*>] |	Configure the encryption key to be shared with the TACACS server.
[**timeout** <*1-1000*>]}	Configure the timeout if the TACACS server doesn't respond,

Command Modes	Perle(config-tacacs-server)#

Usage Guidelines

Use this command to configure TACACS+ server parameters.

Examples

This example sets the IPv4 address for your TACACS+ server to 172.17.88.99.

```
Perle(config-tacacs-server)# address ipv4 172.17.88.99
```

Related Commands

tacacs

clear tacacs

show tacacs

tacacs-server

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**tacacs-server**
{[**deadtime** <*1-1440*>] |	Sets the time the IOLAN ignores unresponsive TACACS+ servers.
[**key 0** <*WORD*>**7** <*WORD*> | <*WORD*>] |	Configure an encryption key to be shared with the TACACS+ servers.
[**retransmit** <*1-100*>] |	Configure the number of retries to the active TACACS+ server.
[**timeout** <*1-1000*>}	Configure the time to wait for the TACACS+ server to reply.

Command Modes	Perle(config)#tacacs-server

Usage Guidelines

Use this command to configure TACACS+ server parameters.

Examples

This example sets the TACACS+ server name.

```
Perle(config)#tacacs-server
```

tty

Use the no form of this command to negate a command or set to defaults.

Syntax Description	tty
{**tty** *<1-x>* **mode disable | line**}	Command only exists on models with serial ports. Configure serial port mode. **<1-x>**–depends on model type
Command Modes	Perle(config)#tty

Usage Guidelines

Use this command to configure the mode for the tty port.

Examples

This example set tty port 1 to line mode.

```
Perle(config)#tty 1 mode line
```

usb

Use the no form of this command to negate tty parameters.

Syntax Description	usb
{*<1-8>* **mode disable | line | line+other | other**}	Configure usb port mode. **disable**—not enabled **line**—used for serial connections **line+other**—used for a serial connection or connecting a flash drive **other**—used only with flash drives
Command Modes	Perle(config)#usb

Usage Guidelines

Use this command to configure the USB port mode.

Examples

This example sets the usb port to be used for line mode (serial).

```
Perle(config)#usb 1 mode line
```

Related Commands

line

username

Use the no form of this command to negate a command or set to defaults.

Syntax Description	username
{[<*WORD*>] |	Configure local user names and passwords
[access schedule <*1-10*> <*hh:mm*> <*hh:mm*> friday | monday | saturday | sunday | thursday | tuesday | wednesday] |	Configure date and time the user is allow access. Note: the user must exist to see this option.
[nopassword] |	No password is required for user to log in.
[openvpn-user] |	Configure user as an openVPN user.
[privilege 1 | 10 | 11 | 15] |	**Privilege levels** • 1—User Level (User Exec Only) • 10—User Privilege Level (Web only) • 11—User Privilege Level (Restful API only) • 15—User Privilege Level, EXEC, Web, and REST API)
[secret 0 <*LINE*> | 5 <*WORD*> | <*LINE*>] |	Configure a secret or password for this user. • 0—The unencrypted password follows • 5—An encrypted password follows • LINE—The unencrypted (cleartext) user password
[serial] |	This user is a serial user. Define more parameters for this user here ***(config-user-serial)***. Note: user must exist to see this option.
[two-factor] |	This user uses 2–factor authentication. Define more parameters for this user here ***(config-user-2factor)***. Note: User must exist to see this option
[web-access dashboard | diagnostics | logging | monitor-statistics | reset]}	10—User Privilege Level (Web only), select the information that can be accessed by this user.
Command Modes	Perle(config)#username

Usage Guidelines

Use this command to set user parameters.

Privilege level

- 1— Specifies user privilege level (user exec)
- 10—User Privilege Level (Web only)
- 11—User Privilege Level Restful API only)
- 15—Specifies privilege exec level (privilege exec)

Secret

- 0—Specifies that an UNENCRYPTED password follows.
- 5— Specifies an ENCRYPTED password follows.
- LINE – the UNENCRYPTED (cleartxt) password.

Examples

This example creates a user with user exec privileges and a clear text password.

```
Perle(config)#username lyn privilege 1 secret password123
```

Related Commands

show username

(config-user-serial)

(config-user-2factor)

(config-user-serial)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-user-serial)
{**[callback off | on] |**	Set the port for callback mode. ● on ● off
[framed-compression off | on] |	Configure Van Jacobson Compression. ● on ● off
[framed-interface-id *<ipv6 interface id>*] |	Configure the IPv6 interface identifier. The second part of an IPv6 unicast or anycast address is typically a 64-bit interface identifier used to identify a host's network interface. For example, if the MAC address of a network card is 00:BB:CC:DD:11:22 the interface ID would be 02BBCCFFFEDD1122
[framed-ip *<A.B.C.D>*] |	Configure the IPv4 address
[framed-mtu *<64-1500>*] |	Configure Maximum Transmission Unit (mtu) size. Default is 1500 Values are 64 to 1500

[host-ip *<Hostname>* | *<A.B.C.D>* | *<X:X:X:X::X>*] |	Configure a hostname, IPv4 or IPv6 address.
[hotkey-prefix *<1-ff>*] |	The prefix that a user types to control the current session. ● Data Options: ^a number—To switch from one session to another, press ^a (Ctrl-a) and then the required session number. For example, ^2 would switch you to session 2. Pressing ^a 0 returns you to the Menu. ● ^a n—Display the next session. The current session remains active. The lowest numbered active session is displayed. ● ^a p—Display the previous session. The current session remains active. The highest numbered active session is displayed. ● ^a m—To exit a session and return to the IOLAN. You are returned to the menu. The session is left running. ● ^a l—(Lowercase L) Locks the serial port until the user unlocks it. The user is prompted for a password (any password, excluding spaces) and the serial port is locked. The user must retype the password to unlock the serial port. ● ^r—When you switch from a session back to the Menu, the screen may not be redrawn correctly. If this happens, use this command to redraw it properly. This is always Ctrl R, regardless of the Hotkey Prefix. The User Hotkey Prefix value overrides the Serial Port Hotkey Prefix value. You can use the Hotkey Prefix keys to lock a serial port only when the serial port's Allow Port locking parameter is enabled. Default is Hex 01 (Ctrl -a or ^a)
[idle-timer *<0-4294967>*] |	Configure a session inactivity timer in seconds. Default is 0 seconds so the port never times out. Values are 0 to 4294967 seconds
[line-access readin *<1-8> <17-24>* | readout *<1-8> <17-24>* | readwrite *<1-8> <17-24>*] |	Configure the access for the serial lines.
[netmask *<A.B.C.D>*] |	Configure the IPv4 netmask
[phone-number *<phone-number> <A.B.C.D>*] |	Configure the call back phone number.

[port ssh *<1-65535>*| ssl_raw *<1-65535>* | tcp-clear *<1-65535>* | telnet *<1-65535>*] |	Configure the service to be used for outbound sessions on this port. ● ssh ● ssl-raw ● tcp-clear ● telnet
[routing listen | none | send | send-and-listen] |	Configure the routing mode (RIP, Routing Information Protocol) used on the PPP/SLIP interface. ● listen—enable PPP/SLIP receiving of RIP ● none—disable PPP/SLIP sending and receiving of RIP ● send—enable PPP/SLIP sending and receiving of RIP ● send-and-listen—enable PP/SLIP sending and receiving of RIP
[service dsprompt | ppp | rlogin | slip | ssh | ssl-raw | tcp-clear | telnet] |	Configure the service for outbound sessions. ● dsprompt ● ppp ● rlogin ● slip ● ssh ● ssl-raw ● tcp-clear ● telnet
[sess-timer *<0-4294967>*] |	Configure the maximum session time. Default is 0 seconds so the port never times out. Values are 0 to 4294967 seconds
[session *<1-4>* [auto off | on] | [rlogin-options host *<hostname>* | *<A.B.C.D>* | *<X:X:X:X::X>*| termtype *<WORD>*] | ssh-options | telnet-options echo *<0-0x7f>* | eof *<0-0x7f>* | erase *<0-0x7f>* | escape *<0-0x7f>* | host *<hostname>* | *<A.B.C.D>* | *<X:X:X:X::X>* | intr *<0-0x7f>* | [line-mode off | on] ||[local-echo off | on] | [map-cr-crlf on | off] | port *<1-65535>*| quit *<0-0x7f>* | termtype *<WORD>* | type [off | rlogin | ssh | telnet]}	Configure user session parameters.

Command Modes	Perle(config-user-serial)#

Usage Guidelines

Use this command to configure serial parameters for the user.

Examples

This example sets outbound telnet session for user fred.

```
Perle(config)#username fred serial
Perle(config-user-serial)# service telnet
```

(config-user-2factor)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-user-2factor)
{**[enable] |**	Enable two-factor one-time pin authentication.
[email *<WORD>*] |	Configure the email address to receive the 2factor authentication request.
[method email]}	Configure the 2-factor authentication method.

Command	Perle(config-user-2factor)#

Usage Guidelines

Use this command to configure 2factor authentication parameters for a user.

Examples

This example sets email authentication for 2factor authentication for user fred

```
Perle(config)#username fred two-factor
Perle(config-user-2factor)#email fred@yahoo.ca
Perle(config-user-2factor)#method email
Perle(config-user-2factor)#enable
```

Related Commands

email

wan

Use the no form of this command to negate a command or set to defaults.

Syntax Description	wan

{**[failover] |**	Configure failover. Failover is defined as a mode where 2 or more WANinterfaces 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. **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 an WAN interface has Internet connectivity (one or more of the ping or traceroute tests MUST pass).
[high-availability disable | failover | loadsharing] |	Configure the action for the High-availability feature.
[load-sharing]}	Configure Load Sharing. Load Sharing defines how routed traffic is sent over one or more configured 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 or divided over multiple active WAN interfaces. This is accomplished by defining one or more Load Sharing rules. **Flush-connections**—enables flushing to flush data on WAN interface outage. **Local traffic**—enables all local traffic in the rule. **Rule**—Configure a load–sharing rule. **Source-nat**—enables/disables source address translation on this rule. **Sticky-inbound**—enables/disables inbound connection tracking.
Command Modes	Perle(config)#wan

Usage Guidelines

Use this command to configure High Availability, Failover and Load Sharing features.

Examples

This example sets disables the High Availability feature.

```
Perle(config)#wan high-availability disable
```

Related Commands

(config-wan-failover)

(config-wan-failover)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-wan-failover
{[source-interface bvi *<1-9999>* **| dialer** *<0-15>* **| ethernet** *<1-24>* **.** *<1-4000>* **| openvpn-tunnel** *<0-999>* **| tunnel** *<0-999>*] |	Configure the source interface.
[wan-interface bvi *<1-9999>* **| dialer** *<0-15>* **| ethernet** *<1-24>* **.** *<1-4000>* **| openvpn-tunnel** *<0-999>* **| tunnel** *<0-999>*]}	Configure the WAN interface.
Command	Perle(config-wan-failover)#

Usage Guidelines

Use this command to configure source and WAN interfaces for failover.

Examples

This example configures source interface ethernet 1for failover mode.

```
Perle(config-wan-failover)#source-interface ethernet 1
```

Related Commands

show ip route

show zone-policy

(config-loadshare-rule)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-loadshare-rule
{[description *<LINE>*] |	Configure the description for this rule.
[exclude-rule] |	Enable or disable this rule.
[limit burst *<0-4294967295>* **| period hour minute | second | rate** *<0-4294967295>* **| threshold above | below] |**	Configure packet limit for this rule.

[match protocol ***<1-255>*** **| ah | dccp | dsr | egp | eigrp | encap | esp | etherip | ggp | gre | hmp | icmp | idpr | igmp | igp | ip | ipip | ipv6 | ipv6-frag | ipv6-icmp | ipv6-nonxt | ipv6-opts | ipv6-route | isis | l2tp | manet | mpls-in-ip | narp | not | ospf | pim | rdp | rohc | rsvp | sctp | sdrp | skim6 | skip | tcp | udp | udplite | vrrp | xns-idp] |**	Matches the criteria for this rule.
[per-packeting-sharing] |	Enables or disables per packet load sharing.
[source-interface bvi ***<1-9999>*** **| dialer** ***<0-15>*** **| ethernet** ***<1-24>*** **.** ***<1-4000>*** **| openvpn-tunnel** ***<0-999>*** **| tunnel** ***<0-999>*** **] |**	Select the source interface for matching criteria.
[wan-interface bvi ***<1-9999>*** **weight** ***<1-255>*** **| dialer** ***<0-15>*** **weight** ***<1-255>*** **| ethernet** ***<1-24>*** **weight** ***<1-255>*** **.** ***<1-4000>*** **weight** ***<1-255>*** **| openvpn-tunnel** ***<0-999>*** **weight** ***<1-255>*** **| tunnel** ***<0-999>*** **weight** ***<1-255>*** **]}**	Select WAN interface and weight for participating in this load sharing rule.
Command	Perle(config-load-sharing-rules)#

Usage Guidelines

Use this command to configure load sharing rules.

Examples

This example configures the BVI interface 10 to be part of WAN load sharing.

```
Perle(config-loadshare-rule)#wan bvi 10
```

Related Commands

show ip route

show zone-policy

virtual-machine

Syntax Description	**virtual-machine**
{[configure ***<WORD>*** **] |**	Re-configure an installed or inactive VM.
[enable] |	Enable virtualization support.

[import disk-image *<WORD>*]}	Import or install a new VM.
Command Modes	#virtual-machine

Usage Guidelines

Use this command to re-configure an installed or inactive VM. Enable VM services, or import disk images.

Examples

This example

```
Perle#virtual-machine import disk-image testVM
Perle(config-import-disk)#
```

Related Commands

(config-import-disk)

(config-import-disk)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-import-disk)#**
{**[cpu-cores *<WORD>*] |**	Enter the number of CPU cores. At lease one core must be specified, Default is 1. Values are 1–3.
[description *<LINE>*] |	Specify a description for this virtual machine.
[display [console | vnc authentication 0 | 7 | *<WORD>* | none] [port *<5900-5950* | auto] |	Display device at which you log into z/VM. Specify the authentication (if needed) and the port for the VNC server to connect to.
[image-file [remote-system ftp: | http: | https: | scp | sftp:] | usb-flash *<1-8>*] |	Specify the path to the disk image file.
[install] |	Install the VM to the IOLAN. All mandatory fields must be entered. ● iso-file ● name of VM ● network settings <bvi 1-9999> ● operating system (os) to be used.

[memory ***<1-2595>*****] |**	Specify the MB needed for this VM installation. Values are 1-2595 MB Default is 2048 MB
[network bvi ***<1-9999>*****] |**	Specify the bvi to be used with this VM. Values are 1–9999
[os generic | variant :***<WORD>*****] |**	Use this o/s or variant when creating the VM.
[seed-file [remote-system ftp: | http: | https: | scp | sftp:] | usb-flash ***<1-8>*****] |**	Specify the path to the disk image file.
[storage ***<WORD>*****]**}	Enter the MB size requirements of your installation. Value is 1 to 53 GB Default 15 GB
Command Modes	Perle(config-install-local)#

Usage Guidelines

Use these commands to configure import disk parameters.

flash:*perle-image-name.img*

ftp:*[[//username[:password]@location]/directory]/perle-image-name.img*

http://***[[username:password]@][hostname | host-ip [directory] /perle-image-name.img***

https://***[[username:password]@][hostname | host-ip [directory] /perle-image-name.img |***

scp:*[[username@location]/directory]/perle-image-name.img |*

sftp:*[[//username[:password]@location]/directory]/perle-image-name.img |*

usb:*<1-8>*

Examples

In this example the user is setting the cpu cores to 3.

```
Perle(install-local)#cpu-cores 3
```

Related Commands

show virtual-machine

zone

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**zone**
{**security** ***<WORD>***}	Name of security zone.
Command Modes	Perle(config)#zone

Usage Guidelines

Use this command to create a security zone.

Examples

This example creates a zone with the name secure1.

```
Perle(config)#zone security secure1
```

Related Commands

zone-pair

show zone-policy

(config-sec-zone)

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-sec-zone)
{**[default-action drop | reject] |**	Configure the default action for traffic coming into this zone. ● Drop packets—silently drop the packets ● Reject—drops packets and notifies the source Enter a zone description. Zone to be local-zoned.
[description *<WORD>*] |	Configure security zone description.
[local-zone]}	Sets zone to be local.
Command Modes	Perle(config-sec-zone)#

Usage Guidelines

Use this command to setup a default action for zone firewall.

Examples

This example rejects all incoming packets to this zone.

```
Perle(config)# default-action reject
```

Related Commands

show zone-policy

virtual-machine

zone-pair

zone-pair

Use the no form of this command to negate a command or set to defaults.

Syntax Description	zone-pair
{**from** *<WORD>* **to** *<WORD>* **firewall** *<WORD>* **| ipv6-firewall** *<WORD>*}	Configure parameters for zone pair firewalls. ● From—zone from which to filter traffic ● To—zone to which to filter traffic ● Firewall—select firewall to be used to filter traffic (IPv4 or IPv6)
Command Modes	Perle(config)#zone-pair

Usage Guidelines

Use this command to create zone-pair firewalls.

Examples

This example filters traffic from lab-zone to office-z using secure zone 1.

```
Perle(config)#zone-pair from lab-zone to office-zone firewall secure1
```

Note: Secure zone 1 needs to be created first.

Related Commands

show zone-policy

virtual-machine

5 Interface configuration

This chapter defines all the CLI commands in Interface Configuration Mode. Some CLI commands may not be applicable to your model or running software.

Interface

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**interface**
{**[bvi** ***<1-9999>*****] |**	Configure for a bridge interface. See ***(config-if)#***.
[cellular ***<0-0>*****] |**	Configure for a cellular interface. See ***(config-if)#cellular***
[dialer ***<0-15>*****] |**	Configure for a dialer interface. See ***(config-if)#dialer***
[ethernet ***<1-x>.<1-4000>*****] |**	Configure for an Ethernet interface. <1-x> = maximum number of ethernet ports, (depends on the model) See ***(config-if-ethernet)#***
[loopback] |	Configure for a loopback interface.
[openvpn-tunnel ***<0-999>*** **tap | tun] |**	Configure for an OpenVPN tunnel interface. See ***(config-if)#openvpn-tunnel***
[port-channel ***<1-13>*****] |**	Configure for port channel. See ***(config-if-port-channel)#***
[sfp ***<1-x>*****] |**	Configure for SFP interface. See ***(config-if-sfp)#***
[tunnel ***<0-999>*****] |**	Configure for a tunnel interface. See ***(config-if)#tunnel***
[range ethernet ***<1-x>*****]**}	Configure an Ethernet range. ***(config-if-range)#***
Command Modes	Perle(config) #interface ethernet 1 Perle(config-if)#

Usage Guidelines

Use this command to configure the interface type and number.

Examples

This example enter sub-menu configuration for Ethernet interface 1.

```
Perle(config)#interface ethernet 1
```

(config-if)#

These commands apply to all interfaces.

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-if)#
[description *<LINE>*] |	Configure interface description.
[ip firewall in | local | out *<WORD>*] |	**Firewall**—set firewall for inbound, traffic destined for this IOLAN or outbound traffic.
[ip health-profile *<WORD>* nexthop [*<A.B.C.D>* | *<dhcp>* vrrp *<1-255>* [bvi *<1-9999>*] | [ethernet *<1-x>*] good-prio *<1-255>* bad-prio *<1-255>*] |	Use this health profile for this interface, configure a next hop and priority and interface.
[ip ospf authentication message-digest | null] |	Enables message-digest authentication, text, or null.
[ip ospf authentication-key 0 *<WORD>* | 7 *<WORD>* | *<WORD>*] |	Authentication-key 0 | 7 <WORD>.
[ip ospf cost *<1-65535>*] |	Configure a default metric to be applied to routes being distributed into OSPF. Range is 0 to 16777214 Default is none
[ip ospf dead-interval *<1-65535>*] |	Configure the interval during which at least one hello packet must be received from a neighbor before the IOLAN declares that neighbor as down (dead).) As with the hello interval, this value must be the same for all IOLANs attached to a common network. Default is 4 times the hello interval Default is 40 seconds
[ip ospf hello-interval *<1-65535>*] |	Configure the hello packet time interval for hello packets sent on an interface. Default is 10 seconds

[ip ospf message-digest-key *<1-255>* md5 0 *<WORD>* | 7 *<WORD>* | *<WORD>*] |	Configure a password used by neighboring routers for simple password authentication. It can be any continuous string of up to eight characters. There is no default value. • None—no password • Key-ID—Configure an authentication key • md5—Identifies the key (password) used between this router and neighboring routers for MD5authentication • 0-unencrypted key will follow • specifies a hidden key will follow • specifies a password (key) will follow (max 16 characters). The default is none
[ip ospf mtu-ignore] |	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.
[ip ospf network broadcast] |	A designated router and backup designated router are elected using OSPF multicasting capabilities point-to-multipoint— configures selected routers with neighbor/cost parameters, identifying a specific cost for the connection to the specified peer neighbors and multicast is not required. Routers on an interface becoming neighbors should match the network type.
[ip ospf point-to-point] |	There are only two neighbors and multicast is not required. Routers on an interface becoming neighbors should match the network type all. (most common type).
[ip ospf point-to-multipoint] |	Directs the network to treats point-to-multipoint networks as a collective of point-to-point links. Point-to-Multipoint networks do not maintain a DR/ BDR relationship. Point-to-Multipoint networks advertise a hot route for all the frame-relay endpoints.
[ip ospf non-broadcast] |	Use this type of network on networks having no broadcast/multicast capability, such as frame-relay, ATM, SMDS, & X.25. The key point is that these layer 2 protocols are unable to send broadcasts/ multicasts
[ip ospf priority *<0-255>*] |	A router with a high priority will always win the DR/ BDR election process. Priority Range is 0-255 Default is 1

[ip ospf retransmit-interval *<1-65535>*] |	Time in seconds between link state advertisement retransmissions for adjacencies belonging to the interface, The expected round-trip delay between any two routers in the attached network. Range is 1–65535 Default is 5 seconds
[ip ospf transmit-delay *<1-65535>*] |	Configure the transmit delay. The estimated time in seconds required to transmit a link state update packet on the interface. Link state advertisements in the update packet have their age incremented by this amount before transmission. Range is 1–65535 Default is 1 seconds
[ip policy route-policy *<WORD>*] |	Enable this policy route for this interface.
[ip rip authentication key-chain *<WORD>* | mode md5 | text string 0 *<WORD>* | 7 *<WORD>* | *<WORD>*] |	Enable split horizon to prevent a routing loop in your network. Basically, information about the routing for a particular packet is never sent back in the direction from which it was received. Default is enabled
[ipsec restrict] |	Restricts IPsec on this interface.
[ipv6 address *<X:X:X:X::X/ <0-128>* eui-64] | dhcp | autoconfig] |	Configure IPv6 parameters. **IPv6 address/eui-64 or DHCP**—configure the IPv6 address and prefix length or obtain an IPv6 address using DHCP.
[ipv6 enable] |	Enable IPv6 on this interface.
[ipv6 firewall in | out | local *<WORD>*] |	**firewall**—set firewall for inbound, traffic destined for this IOLAN or outbound traffic.
[ipv6 nd dad attempts *<0-600>*] |	DAD (duplicate address detection) attempts—To check the uniqueness of an IPv6 address, a node sends Neighbor Solicitation messages. Use this command to specify the number of consecutive Neighbor Solicitation messages (dad_attempts) to be sent before this address can be configured. Range 1–600 Default is 1
[ipv6 nd managed config flags] |	Specify whether hosts use the administrated protocol for address auto-configuration. Default is disabled (host uses stateless)

[ipv6 nd other-config-flags] |	Specify whether hosts use the administrated protocol for non-address auto-configuration information. Default is disabled (hosts use stateless auto-configuration of no-address information.
[ipv6 nd prefix] |	prefix—specifies the IPv6 prefix advertised on the interface Configure the prefix length. Range is 0–128
[ipv6 nd no-autoconfig] |	A prefix is onlink when it is assigned to an interface on a specified link. Enable or disable prefix for onlink determination. Default is off
[ipv6 nd no-onlink] |	The sending router can indicate that a prefix is to be used for address autoconfiguration by setting the autonomous flag and specifying a nonzero Valid Lifetime value for the prefix. Default is off
[ipv6 nd ra] |	Router Advertisement Control.
[nd ra dns server ***<X:X:X:X::X>*****] |**	Specify the name server in RA.
[ipv6 nd ra hop-limit ***<1-255>*** **| unspecified] |**	Specifies the Hop Count field of the IP header for outgoing (unicast) IP packets. Range is 1–255 Default is 64
[ipv6 nd ra interval ***<4-1800> <3-1350>*****] |**	Specifies the maximum/minimum time allowed between sending unsolicited multicast router advertisements. Range of minimum is 3 to *0.75 max (dynamic range) Default maximum 600 seconds, minimum is 0.33*max Range is 1–1800 in seconds
[ipv6 nd ra lifetime ***<0> <4-9000>*****] |**	The lifetime associated with the default router in seconds. A value of 0 indicates that the router is not a default router and doesn't appear on the default router list. The router lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options. Range is 4-1800 seconds Minimum interval is 3-1350 in seconds Default is 1800 seconds 0 = not a default route
[ipv6 nd ra suppress] |	Enable or disable IPv6 Router advertisements. Default is send router advertisements

[ipv6 nd reachable time *<0-3600000>*] |	Specifies the length in time (milliseconds) a node assumes a neighbor is reachable after receiving a reachability confirmation Default is 0 (unspecified by this router) Range is 0-360000 milliseconds
[ipv6 nd retransmission-time *<0- 3600000>*] |	The retransmission timer is used to control the time (in milliseconds) between retransmissions of neighbor solicitation messages from the user equipment (UE). Range 0–3600000 in milliseconds Default is 0
[ipv6 nd router-preference high | low | medium] |	Set the default router preference. A High value means this IOLAN will be preferred. • **High** • **Medium** • **Low** Default is medium
[ipv6 ospf cost *<1-65535>*] |	Configure a default metric to be applied to routes being distributed into OSPF. Range is 0 to 16777214 Default is none
[ipv6 ospf dead-interval] |	Configure the interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down (dead).) As with the hello interval, this value must be the same for all IOLANs attached to a common network. Default is 4 times the hello interval Default is 40 seconds
[ipv6 ospf hello interval] |	Configure the hello packet time interval for hello packets sent on an interface. Default is 10 seconds
[ipv6 ospf ifmtu *<1280-1500>*] |	Interface MTU for OSPFv3.
[ipv6 ospf instance-id *<0-255>*] |	Instance id value. Values 0-255
[ospf mtu-ignore] |	By default, OSPF checks whether neighbors are using the same MTU on a common interface. Use this command to disable this check and allow adjacencies when the MTU value differs between OSPF neighbors.

[ospf network broadcast] |	A designated router and backup designated router are elected using OSPF multicasting capabilities point-to-multipoint— configures selected routers with neighbor/cost parameters, identifying a specific cost for the connection to the specified peer neighbors and multicast is not required. Routers on an interface becoming neighbors should match the network type all
[ospf network point-to-point] |	There are only two neighbors and multicast is not required. Routers on an interface becoming neighbors should match the network type all. (most common type)
[ospf network passive]	No adjacency will be formed on this interface.
[ospf priority *<0-255>*] |	A router with a high priority will always win the DR/BDR election process. Priority Range is 0-255 Default is 1
[ospf retransmit-interval *<1-65535>*] |	Time in seconds between link state advertisement retransmissions for adjacencies belonging to the interface, The expected round-trip delay between any two routers in the attached network. Range is 1–65535 Default is 5 seconds
[ospf transmit-delay *<1-65535>*] |	Configure the transmit delay. The estimated time in seconds required to transmit a link state update packet on the interface. Link state advertisements in the update packet have their age incremented by this amount before transmission. Range is 1–65535 Default is 1 seconds
[ipv6 policy route-policy *<WORD>*] |	Enable this policy route for this interface. Range is 0 to 16777214 Default is none Default is 40 seconds with the MTU value set on the interface.
[ipv6 rip enable | split-horizon | disable poisoned-reverse] |	Enable split horizon to prevent a routing loop in your network. Basically, information about the routing for a particular packet is never sent back in the direction from which it was received. Default is enabled
[logging event interface-ip | link-status] |	Configure interface logging events and link state.

[ntp broadcast client] |	Listens to NTP broadcasts.
[ntp broadcast destination *<A.B.C.D>*] | [key *<1-65534>*] | [minpoll *<4-17>*] | [version *<1-4>*] |	Configure broadcast destination address. **broadcast destination**—IP address **key**—Configure broadcast authentication key **versions** 1 to 4 are support. **minimum poll interval** is 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
[disable] |	Disable NTP.
[multicast [*<A.B.C.D>* | *<X:X:X:X::X>* | client *<A.B.C.D>* | *<X:X:X:X::X>*] | [key *<1-65534>*] | [minpoll *<4-17>*] | [version *<1-4>*] |	**multicast address**—IP or IPv6 address **key**—Configure multicast authentication key **versions** 1 to 4 are support. **minimum poll interval** is 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
[role lan | trusted | wan] |	Select the role for this interface. **LAN**—management access is from the LAN side **WAN**—management access is from the WAN side **Trusted**—management access from either the LAN or WAN side
[service-policy in *<WORD>* | out *<WORD>*] |	Assigns interface service policy. Configure for the policy for inbound or outbound traffic.
[shutdown] |	Shutdown this interface.
[snmp trap interface-ip | link-status] |	Configure interface SNMP traps and link status.
[zone-member security] | *<WORD>*}	Configure this interface as a member of this zone security.
Command Modes	Perle(config-if)#

Usage Guidelines

Use this command to configure parameters for the bridge interface.

Examples

This example enables an IP address on bvi 10.

```
Perle>enable
Perle#config
Perle#interface bvi 10
(config-if)#ip address 172.16.113.45 255.255.0.0
```

Related Commands

(config-if)#

(config-if)#bvi

(config-if)#cellular

(config-if)#dialer

(config-if-ethernet)#

(config-subif)#

(config-if-range)#

(config-if)#openvpn-tunnel

(config-if-port-channel)#

(config-if-sfp)#

(config-if)#tunnel

(config-if-vrrp)#

(config-if)#bvi

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-if)#bvi
{[arp disable-arp-filter |	Configure ARP parameters. If enabled the IOLAN responds to the 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
[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] |	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-proxy-arp] |	Enable IOLAN to respond to an ARP request on behalf of another node.

[timeout *<1-2147483>]* |	If an ARP entry is not used for a specific amount of time the entry is removed from the caching table.
[ip address *<A.B.C.D>* | dhcp] secondary] |	Specify the IP address or DHCP. Specify a secondary or alias address.
[ip ddns service dyndns login *<WORD>* password *<WORD>* | host *<WORD>*| host-group *<WORD>* | use-web skip *<WORD>* | url *<WORD>*] |	**DDNS—** **Service**—use dyndns login/password—configure the login id and password for the dnydns server. **host/host-group**—Hostname/list of hostnames registered with the DDNS service. **skip**—skip everything before this on the given URL. **Use-web URL**—This field contains the website URl.
[ip dhcp client class-id *<LINE>* | auto] |	**DHCP client** — Specify a Class-id string, truncated to 200 characters. This same string or text will be configured on the server side and associated with an address to give the client. **Class ID**: ● Auto ● Line
ip dhcp client-id ethernet *<1-2>* | ascii *<WORD>* | auto | hex *<Hex-String>*] |	**Client ID:** This can be configured to be the Ethernet interface number, ASCII text, Hex string or set to Auto. option—60—Vendor class identifier<oem-name>:<model>:<serial#> in ASCII
[ip dhcp client default-route-distance *<1-255>*] |	Default route distance is a value that your IOLAN uses to select the best path when there are two or more different routes to the same destination from two different routing protocols. A static route is normally set too 1. The smaller the default route distance, the more reliable the protocol. Range is 1-255 (with 1 being the most reliable) and 255 is route not used or unknown.
[ip dhcp client hostname] |	Specify a value for hostname option.
[ip dhcp–relay] |	Set DHCP-relay for this interface.
[ip dns dhcp] |	Use DNS servers received from DHCP server for specified interface.
[ipv6 address *<X:X:X:X::X/2-128>*] |	Specify an IPv6 address.

[ipv6 address autoconfig] |	Obtain address using autoconfig.
[ipv6 address dhcp] |	Obtain address using dhcp.
[ipv6 prefix-from-provider *<WORD>* address [*<1-65535>* | eui-64] | sla-length *<0-16>* sla-id *<0-65535>*] |	**Prefix from provider**–configure interface as delegated interface. This interface is used to delegate IPv6 address to other interfaces configured as PDs. • **address**—local interface address assigned to this interface. • **<1-65535> or EUI-64**–used to form IPv6 interface address EUI-64 is the (default) **Note:** length should be long enough to fit sla-length • **sla-length**—interface site-level aggregator (SLA) length • **sla-id**–specify a decimal integer which fits in the length of SLA IDs
[mac access-group *<WORD>* deny | disable | permit] |	Configure mac access-group parameters for this interface.
[mtu *<1280-1500>*]}	Configure maximum transmission unit (MTU). Values are 1280-1500 bytes
Command Modes	Perle(config-if)#

Usage Guidelines

Use this command to configure cellular profile parameters.

Examples

This example starts cellular connection after the IOLAN reboots.

```
Perle(config)# interface cellular 0
Perle(config-if)#start-connected
```

Related Commands

(config-if)#

(config-if)#bvi

(config-if)#cellular

(config-if)#dialer

(config-if-ethernet)#

(config-subif)#

(config-if-range)#

(config-if)#openvpn-tunnel

(config-if-port-channel)#

(config-if-sfp)#

(config-if)#tunnel

(config-if-vrrp)#

(config-if)#cellular

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-if)#cellular
{[alarm profile *<WORD>*] |	Use this alarm profile for this interface.
[idle-time *<1-60>*] |	Idle time in minutes to drop the on-demand connection. Value is 1 to 60 mins.
[ip ddns service dyndns login *<WORD>* password *<WORD>* | host *<WORD>*| host-group *<WORD>* | use-web skip *<WORD>* | url *<WORD>*] |	**DDNS**— **Service**—use dyndns login/password—configure the login id and password for the dnydns server. **host/host-group**—Hostname/list of hostnames registered with the DDNS service. **skip**—skip everything before this on the given URL. **Use-web URL**—This field should be left blank.
[ip dhcp–relay] |	Set DHCP-relay for this interface.
[ip dns dhcp] |	Use DNS servers received from DHCP server for specified interface.
[ipv6 address autoconfig] |	Obtain address using autoconfig.
[ipv6 pd *<WORD>* instance-id *<0-65535>* | request-length *<48-64>*] |	Specify the prefix name Specify the prefix delegation instance. Value is 0-65535
[monitor-traffic both | receive | transmit] |	Monitors the traffic for on demand feature. Traffic can be monitored for: ● in ● out ● both
[mtu *<1280-9000*] |	Sets Maximum Transmission Unit. (MTU). Values are 1280-9000 bytes
[on-demand] |	On demand feature brings up the interface when there is data to be sent or received only.
[start-connected]}	Establishes LTE data connection after reload or power up.
Command Modes	Perle(config-if)#

Usage Guidelines

Use this command to configure cellular profile parameters.

Examples

This example starts cellular connection after the IOLAN reboots.

```
Perle(config)# interface cellular 0
Perle(config-if)#start-connected
```

Related Commands

(config-if)#dialer

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-if)#dialer
{[**default-route auto** | **none** | **force**] |	Default-route—enable/disable default route to peer. - auto—install default route when link comes up - none—don't install default route when link comes up
[**encapsulation ppp**] |	Sets encapsulation type.
[**ip** [**address** *<A.B.C.D>* *<A.B.C.D>*] |	Configure the IP address/mask of this interface.
[**ipv6** [**address autoconfig**] | [**enable**] |	Obtains an address using autoconfiguration. Enable IPv6 on this interface
[**ipv6 pd** *<WORD>* **instance-id** *<0-65535>* | **request-length** *<48-64>*] |	Specify the prefix name Specify the prefix delegation instance. Value is 0-65535
[**mtu** *<64-1500>*] |	Sets Maximum Transmission Unit (MTU). Values are 64-1500 bytes Default is 1492
[**ppp access-concentrator** *<LINE>* | **chap hostname** *<WORD>* | **password 0** *<LINE>* | 7 *<LINE>* | *<LINE>* | **timeout idle** *<1-4294967>*]}	Configure Point to Point protocol parameters.
Command Modes	Perle(config-if)#

Usage Guidelines

Sets parameters for dialer interface.

Examples

This example sets the role for this interface to WAN.

```
Perle(config-if)role wan
```

Related Commands

(config-if)#

(config-if)#bvi

(config-if)#cellular

(config-if)#dialer

(config-if-ethernet)#

(config-subif)#

(config-if-range)#

(config-if)#openvpn-tunnel

(config-if-port-channel)#

(config-if-sfp)#

(config-if)#tunnel

(config-if-vrrp)#

(config-if-ethernet)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-if-ethernet)#
{**alarm profile** *<WORD>* |	Use this alarm profile for this interface.
{**arp disable-arp-filter |**	Configure ARP parameters. If enabled the IOLAN responds to the 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
[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] |	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-proxy-arp] |	Enable IOLAN to respond to an ARP request on behalf of another node.
[timeout *<1-2147483>*] |	If an ARP entry is not used for a specific amount of time the entry is removed from the caching table.
[authentication [host-mode | multi-auth] |	Selects authentication mode to use on this interface when using Dot1x devices. **Multiple authentication** ● Each device connecting to your IOLAN is required to authenticate. ● No limit as to the number of devices which can authenticate on the port
[authentication single host] |	**Single host** ● Only one device can authenticate and connect on the port This is the default mode of operation.
[authentication multi-host] |	**Multiple host** ● Unlimited number of devices can connect on the port once a single device has been authenticated on the port. This single device must be a data (as opposed to voice) device.
[authentication periodic] |	When enabled, the supplicant will be asked to re-authenticated based on the Advanced setting -> re-authentication timeout value.
[authentication port-control] |	● **Auto**—the port is locked expecting authentication from either a connected 802.1X client or if MAB is enabled, it will authenticate the MAC to the RADIUS server. ● **Force authorized**—the port is unsecure/unlocked meaning normal operation where no 802.1X client or MAB authentication via RADIUS is required. This is the default setting. ● **Force unauthorized**—the port is secured/locked and will NEVER allow any traffic to ingress into our Ethernet port/s.
[authentication re-authenticate] |	Set the number of times the authenticator will attempt to re-authenticate a supplicant. Range is 1-10 seconds Default is 2 seconds

[authentication restart] |	Interval in seconds after which an attempt should be made to authenticate an unauthorized port. If the parameter "server" is specified, the time is derived from the "Session-Timeout value" (RADIUS Attribute 27). Range is 1-65535 seconds Default is 60 seconds
[bridge-group *<1-9999>*] |	Adds this interface to the specified bridge-group.
[dot1x [credential *<WORD>*] |	Dot1x credential profile.
[dot1x max-auth-req *<1-10>*] |	Maximum number of re-authentication attempt.
[dot1x max-req *<1-10>*] |	Maximum number of retries.
[dot1x pae authenticator | supplicant] |	Sets the Port Access Entity (PAE) type. Select the pae type, authenticator or supplicant.
[dot1x authenticator] |	The interface acts only as an authenticator and does not respond to any messages meant for a supplicant.
[dot1x supplicant] |	The interface acts only as a supplicant and does not respond to messages that are meant for an authenticator.
[dot1x timeout quiet-period *<1-65535>* | supp-period *<1-65535>* | tx-period *<1-65535>*] |	Quiet period in seconds. Supplicant timeout for reply Supplicant timeout for retries.
[ip address [*<A.B.C.D>* *<A.B.C.D>* secondary] |	Configure IP parameters. **IP address/IP mask**—Configure the IP address/ mask of this interface. **secondary**—add secondary or ip aliasing address for this interface. Max secondary address-1-128 You must define a primary address before secondary IP addresses Primary and secondary address can be on the same of different subnets of the primary address.
[ip ddns service dyndns login *<WORD>* password *<WORD>* | host *<WORD>*| host-group *<WORD>* | use-web skip *<WORD>* | url *<WORD>*] |	**DDNS—** **Service**—use dyndns login/password—configure the login id and password for the dnydns server. **host/host-group**—Hostname/list of hostnames registered with the DDNS service. **skip**—skip everything before this on the given URL. **Use-web URL**—This field container the URL website.

[ip dhcp client class-id *<LINE>* | auto] |	**DHCP client** — Specify a Class-id string, truncated to 200 characters. This same string or text will be configured on the server side and associated with an address to give the client. **Class ID**: ● Auto ● Line
ip dhcp client-id ethernet *<1-x>* | ascii *<WORD>* | auto | hex *<Hex-String>*] |	**Client ID:** This can be configured to be the Ethernet interface number, ASCII text, Hex string or set to Auto. option—60—Vendor class identifier<oem-name>:<model>:<serial#> in ASCII
[ip dhcp client default-route-distance *<1-255>*] |	Default route distance is a value that your IOLAN uses to select the best path when there are two or more different routes to the same destination from two different routing protocols. A static route is normally set too 1. The smaller the default route distance, the more reliable the protocol. Range is 1-255 (with 1 being the most reliable) and 255 is route not used or unknown.
[ip dhcp client hostname] |	Specify a value for hostname option.
[ip dhcp–relay] |	Set DHCP-relay for this interface.
[ip dns dhcp] |	Use DNS servers received from DHCP server for specified interface.
[ipv6 address *<X:X:X:X::X/2-128>*] |	Specify an IPv6 address.
[ipv6 address autoconfig] |	Obtain address using autoconfig.
[ipv6 address dhcp] |	Obtain address using dhcp.

[ipv6 prefix-from-provider *<WORD>* address [*<1-65535>* | eui-64] | sla-length *<0-16>* sla-id *<0-65535>*] |	**Prefix from provider**–This interface is used to delegate IPv6 address to other interfaces configured as delegated PDs. The command is not available if <pd-name> is defined on the cellular interface. IPv6 address is assigned using Prefix Delegation which has name <pd-name>. SLA length and SLA-ID form the network part of IPv6 address for delegated interface. Range of sla-id: <0-65535>. Default: <0-128> Range for sla-length: <0-16>. Default is difference between requested length and 64 Value of SLA-ID must fit in the SLA length For a given <pd-name>, SLA ID must be unique Add • Prefix from provider— • PD name—select name from the drop-down box • PD ID# (0-65535) • Prefix length—length of prefix (48-64) • delegated interface • address used to form the IPv6 interface address or EUI-64
[enable] |	Enable IPv6 on this interface.
[ipv6 nd dad attempts *<0-600>*] |	DAD (duplicate address detection) attempts—To check the uniqueness of an IPv6 address, a node sends Neighbor Solicitation messages. Use this command to specify the number of consecutive Neighbor Solicitation messages (dad_attempts) to be sent before this address can be configured. Range 1–600 Default is 1
[ipv6 nd managed config flags] |	Specify whether hosts use the administrated protocol for address auto-configuration. Default is disabled (host uses stateless)
[ipv6 nd other-config-flags] |	Specify whether hosts use the administrated protocol for non-address auto-configuration information. Default is disabled (hosts use stateless auto-configuration of no-address information.
[ipv6 nd prefix] |	prefix—specifies the IPv6 prefix advertised on the interface Configure the prefix length. Range is 0–128

[ipv6 nd no-autoconfig] |	A prefix is onlink when it is assigned to an interface on a specified link. Enable or disable prefix for onlink determination. Default is off
[ipv6 nd no-onlink] |	The sending router can indicate that a prefix is to be used for address autoconfiguration by setting the autonomous flag and specifying a nonzero Valid Lifetime value for the prefix. Default is off
[ipv6 nd ra] |	Router Advertisement Control.
[nd ra dns server *<X:X:X:X::X>*] |	Specify the name server in RA.
[ipv6 nd ra hop-limit *<1-255>* | unspecified	Specifies the Hop Count field of the IP header for outgoing (unicast) IP packets. Range is 1–255 Default is 64
[ipv6 nd ra interval *<4-1800>* *<3-1350>*] |	Specifies the maximum/minimum time allowed between sending unsolicited multicast router advertisements. Range of minimum is 3 to *0.75 max (dynamic range) Default maximum 600 seconds, minimum is 0.33*max Range is 1–1800 in seconds
[ipv6 nd ra lifetime *<0>* *<4-9000>*] |	The lifetime associated with the default router in seconds. A value of 0 indicates that the router is not a default router and doesn't appear on the default router list. The router lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options. Range is 4-1800 seconds Minimum interval is 3-1350 in seconds Default is 1800 seconds 0 = not a default route
[ipv6 nd ra suppress] |	Enable or disable IPv6 Router advertisements. Default is send router advertisements
[ipv6 nd reachable time *<0-3600000>*] |	Specifies the length in time (milliseconds) a node assumes a neighbor is reachable after receiving a reachability confirmation Default is 0 (unspecified by this router) Range is 0-360000 milliseconds

[ipv6 nd retransmission-time *<0-3600000>*] |	The retransmission timer is used to control the time (in milliseconds) between retransmissions of neighbor solicitation messages from the user equipment (UE). Range 0–3600000 in milliseconds Default is 0
[ipv6 nd router-preference high | low | medium] |	Set the default router preference. A High value means this IOLAN will be preferred. • **High** • **Medium** • **Low** Default is medium
[ipv6 pd <word> instance-id <0-65535> | request-length <48-64>] |	Specify the prefix name Specify the prefix delegation instance. Value is 0-65535
[lldp max-neighbors *<1-50>* | receive | tvl-select mac-phy-cfg | management-address | max-frame-size | port-description | system-capabilities | system-description | system-name | transmit] |	Configure LLDP parameters.
[mab eap] |	Use MAC authentication bypass interface commands.
[mac access-group <word> deny | disable | permit] |	Sets interface MAC access-list parameters.
[mtu *<64-9000>*] |	Sets maximum transmission unit (MTU). Values are 64 t 9000 bytes Default is 1500 bytes
[power efficient-ethernet auto] |	Configure interface power settings.
[shutdown] |	Shutdown this interface.
[spanning-tree [bpdufilter enable | disable] |	Configure interface parameters for spanning tree. Don’t send or receive BPDUs on this interface. Default is Disabled
[bpduguard [disable | enable] |	Don’t accept BPDUs on this interface. Default is Disabled
[spanning-tree cost *<1-200000000>*] |	Change port path cost. Value is 1 to 200000000

[spanning-tree guard loop | none | root | topology-change] |	Default is auto (defined by STP protocol) ● loop ● none ● root ● topology-change
[spanning-tree link-type auto | point-to-point | shared] |	● auto—this interface is point-to-point if configured for full duplex operation ● point-to-point ● shared
[spanning-tree mcheck] |	Force the mode from STP to RSTP/MSTP mode.
[spanning-tree mst cost *<1-200000000>*] |	Change path cost and port priority for multiple spanning tree mode.
[spanning-tree port-priority *<0-240>*] |	Change the port priority for an instance. (increments of 16) Default is 128
[spanning-tree portfast disable] |	When enabled an interface will jump to the forwarding state of spanning-tree.
[spanning-tree portfast edge] |	Portfast edge is used to configure a port on which an end device is connected, such as a PC. All ports directly connected to end devices cannot create bridging loops in the network. Therefore, the edge port directly transitions to the forwarding state, and skips the listening and learning stages.
[spanning-tree portfast network] |	This feature causes the IOLAN to enter the STP forwarding-state immediately or upon a linkup event, thus passing the listening and learning states. Some applications need to connect to the network immediately, else they will timeout.
[speed 10 |100 | 1000 |auto] |	Configure the Ethernet speed.. ● 10 ● 100 ● 1000 ● auto
[vrrp *<1-255>*]}	This interface is part of VRRP group number.
Command Modes	Perle(config-if)#

Usage Guidelines

Set up Ethernet parameters for this interface.

Examples

This example sets the speed for this interface to 1000.

```
Perle(config-if)#speed 1000
```

Related Commands

(config-if)#

(config-if)#bvi

(config-if)#cellular

(config-if)#dialer

(config-if-ethernet)#

(config-subif)#

(config-if-range)#

(config-if)#openvpn-tunnel

(config-if-port-channel)#

(config-if-sfp)#

(config-if)#tunnel

(config-if-vrrp)#

(config-subif)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-subif)#
{**arp disable-arp-filter |**	Configure ARP parameters. If enabled the IOLAN responds to the 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
[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] |	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-proxy-arp] |	Enable IOLAN to respond to an ARP request on behalf of another node.
[timeout *<1-2147483>]* |	If an ARP entry is not used for a specific amount of time the entry is removed from the caching table.
bridge-group *<1-9999>* |	Add this interface to the specified bridge group.
ip [address *<A.B.C.D> < A.B.C.D>* | secondary | dhcp] | dhcp-relay] |	Configure IP parameters. **IP address/IP mask**—Configure the IP address/ mask of this interface **secondary**—add secondary or ip aliasing address for this interface Max secondary address-1-128 You must define a primary address before secondary IP addresses Primary and secondary address can be on the same of different subnets of the primary address. **DCHP relay**—Specify a destination address for UDP broadcasts.
[ip dhcp–relay] |	Set DHCP-relay for this interface.
[ip dns dhcp] |	Use DNS servers received from DHCP server for specified interface.
[ip dhcp client class-id *<LINE>* | auto] |	**DHCP client —** Specify a Class-id string, truncated to 200 characters. This same string or text will be configured on the server side and associated with an address to give the client. **Class ID**: - Auto - Line
[ip dhcp client-id ethernet *<1-x>* | ascii *<WORD>* | auto | hex *<Hex-String>]* |	**Client ID:** This can be configured to be the Ethernet interface number, ASCII text, Hex string or set to Auto. option—60—Vendor class identifier<oem-name>:<model>:<serial#> in ASCII

[ip dhcp client default-route-distance *<1-255>*] |	Default route distance is a value that your IOLAN uses to select the best path when there are two or more different routes to the same destination from two different routing protocols. A static route is normally set too 1. The smaller the default route distance, the more reliable the protocol. Range is 1-255 (with 1 being the most reliable) and 255 is route not used or unknown.
[ip dhcp client hostname]	Specify a value for hostname option.
[ipv6 address *<X:X:X:X::X/<0-128>* eui-64]	Configure the IPv6 address and prefix length and EUI-64 for this interface.
[ipv6 address dhcp] |	Obtain an IPv6 address using DHCP.
[ipv6 address autoconfig] |	Obtain address from autoconfiguration.
ipv6 address prefix-from provider] *<WORD>* address [*<1-65535>* | eui-64] | sla-length *<0-16>* sla-id *<0-65535>*] |	The command is not available if <pd-name> is defined on the cellular interface. IPv6 address is assigned using Prefix Delegation which has name <pd-name>. SLA length and SLA-ID form the network part of IPv6 address for delegated interface. Range of sla-id: <0-65535>. Default: <0-128> Range for sla-length: <0-16>. Default is difference between requested length and 64 Value of SLA-ID must fit in the SLA length For a given <pd-name>, SLA ID must be unique Add ● Prefix from provider— ● PD name—select name from the drop-down box ● PD ID# (0-65535) ● Prefix length—length of prefix (48-64)
[enable] |	Enable IPv6 on this interface.
[ipv6 nd dad attempts *<0-600>*	IPv6 Interface Neighbor Discovery sub-commands

[ipv6 nd dad attempts *<0-600>*] |	DAD (duplicate address detection) attempts—To check the uniqueness of an IPv6 address, a node sends Neighbor Solicitation messages. Use this command to specify the number of consecutive Neighbor Solicitation messages (dad_attempts) to be sent before this address can be configured. Range 1–600 Default is 1
[ipv6 nd managed config flags] |	Specify whether hosts use the administrated protocol for address auto-configuration. Default is disabled (host uses stateless)
[ipv6 nd other-config-flags] |	Specify whether hosts use the administrated protocol for non-address auto-configuration information. Default is disabled (hosts use stateless auto-configuration of no-address information.
[ipv6 nd prefix] |	prefix—specifies the IPv6 prefix advertised on the interface Configure the prefix length. Range is 0–128
[ipv6 nd no-autoconfig] |	A prefix is onlink when it is assigned to an interface on a specified link. Enable or disable prefix for onlink determination. Default is off
[ipv6 nd no-onlink] |	The sending router can indicate that a prefix is to be used for address autoconfiguration by setting the autonomous flag and specifying a nonzero Valid Lifetime value for the prefix. Default is off
[ipv6 nd ra] |	Router Advertisement Control.
[nd ra dns server *<X:X:X:X::X>*] |	Specify the name server in RA.
[ipv6 nd ra hop-limit *<1-255>* | unspecified	Specifies the Hop Count field of the IP header for outgoing (unicast) IP packets. Range is 1–255 Default is 64
[ipv6 nd ra interval *<4-1800>* *<3-1350>*] |	Specifies the maximum/minimum time allowed between sending unsolicited multicast router advertisements. Range of minimum is 3 to *0.75 max (dynamic range) Default maximum 600 seconds, minimum is 0.33*max Range is 1–1800 in seconds

[ipv6 nd ra lifetime *<0> <4-9000>*] |	The lifetime associated with the default router in seconds. A value of 0 indicates that the router is not a default router and doesn't appear on the default router list. The router lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options. Range is 4-1800 seconds Minimum interval is 3-1350 in seconds Default is 1800 seconds 0 = not a default route
[ipv6 nd ra suppress] |	Enable or disable IPv6 Router advertisements. Default is send router advertisements
[ipv6 nd reachable time *<0-3600000>*] |	Specifies the length in time (milliseconds) a node assumes a neighbor is reachable after receiving a reachability confirmation Default is 0 (unspecified by this router) Range is 0-360000 milliseconds
[ipv6 nd retransmission-time *<0-3600000>*] |	The retransmission timer is used to control the time (in milliseconds) between retransmissions of neighbor solicitation messages from the user equipment (UE). Range 0–3600000 in milliseconds Default is 0
[ipv6 nd router-preference high | low | medium] |	Set the default router preference. A High value means this IOLAN will be preferred. • **High** • **Medium** • **Low** Default is medium
[ipv6 pd <word> instance-id <0-65535> | request-length <48-64>] |	Specify the prefix name Specify the prefix delegation instance. Value is 0-65535
mtu *<64-9000>* |	Configure Maximum Transmission Unit (MTU). Values are 64-9000 bytes Default is 1500 bytes
shutdown |	Shut down this interface.
[spanning-tree [bpdufilter enable | disable] |	Configure interface parameters for spanning tree. Don’t send or receive BPDUs on this interface. Default is Disabled
[spanning-tree bpduguard [disable | enable] |	Don’t accept BPDUs on this interface. Default is Disabled

[spanning-tree cost *<1-200000000>*] |	Change port path cost. Value is 1 to 200000000
[spanning-tree guard loop | none | root | topology-change] |	Default is auto (defined by STP protocol) ● loop ● none ● root ● topology-change
[spanning-tree link-type auto | point-to-point | shared] |	● auto—this interface is point-to-point if configured for full duplex operation ● point-to-point ● shared
[spanning-tree mcheck] |	Force the mode from STP to RSTP/MSTP mode.
[spanning-tree mst cost *<1-200000000>*] |	Change path cost and port priority for multiple spanning tree mode.
[spanning-tree port-priority *<0-240>*] |	Change the port priority for an instance. (increments of 16) Default is 128
[spanning-tree portfast disable] |	**portfast disable**—when enabled an interface will jump to the forwarding state of spanning-tree.
[spanning-tree portfast edge] |	**portfast edge**—is used to configure a port on which an end device is connected, such as a PC. All ports directly connected to end devices cannot create bridging loops in the network. Therefore, the edge port directly transitions to the forwarding state, and skips the listening and learning stages.
[spanning-tree portfast network] |	**portfast network**—This feature causes the IOLAN to enter the STP forwarding-state immediately or upon a linkup event, thus passing the listening and learning states. Some applications need to connect to the network immediately, else they will timeout.
vrrp *<1-255>* |	This interface is part of VRRP group number.

Command Modes	Perle(config)#interface ethernet 1.100 Perle(config-subif)#

Usage Guidelines

Set a sub interface within an Ethernet interface.

Examples

This example sets a sub interface of 100 on Ethernet 1interface.

```
Perle(config)# interface ethernet 1.100
```

Related Commands

(config-if)#

(config-if)#bvi

(config-if)#cellular

(config-if)#dialer

(config-if-ethernet)#

(config-subif)#

(config-if-range)#

(config-if)#openvpn-tunnel

(config-if-port-channel)#

(config-if-sfp)#

(config-if)#tunnel

(config-if-vrrp)#

(config-if-range)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-if-range)#
{**[alarm profile *<WORD>*] |**	Use this alarm profile for this interface.
[arp disable-arp-filter] |	Configure ARP parameters. If enabled the IOLAN responds to the 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
[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] |	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-proxy-arp] |	Enable IOLAN to respond to an ARP request on behalf of another node.
[timeout *<1-2147483>]* |	If an ARP entry is not used for a specific amount of time the entry is removed from the caching table.
[authentication [host-mode | multi-auth] |	Selects authentication mode to use on this interface when using Dot1x devices. **Multiple authentication** ● Each device connecting to your IOLAN is required to authenticate. ● No limit as to the number of devices which can authenticate on the port
[authentication single host] |	**Single host** ● Only one device can authenticate and connect on the port This is the default mode of operation.
[authentication multi-host] |	**Multiple host** ● Unlimited number of devices can connect on the port once a single device has been authenticated on the port. This single device must be a data (as opposed to voice) device.
[authentication periodic] |	When enabled, the supplicant will be asked to re-authenticated based on the Advanced setting -> re-authentication timeout value.
[authentication port-control] |	● **Auto**—the port is locked expecting authentication from either a connected 802.1X client or if MAB is enabled, it will authenticate the MAC to the RADIUS server. ● **Force authorized**—the port is unsecure/unlocked meaning normal operation where no 802.1X client or MAB authentication via RADIUS is required. This is the default setting. ● **Force unauthorized**—the port is secured/locked and will NEVER allow any traffic to ingress into our Ethernet port/s.

[authentication re-authenticate] |	Set the number of times the authenticator will attempt to re-authenticate a supplicant. Range is 1-10 seconds Default is 2 seconds
[authentication restart] |	Interval in seconds after which an attempt should be made to authenticate an unauthorized port. If the parameter "server" is specified, the time is derived from the "Session-Timeout value" (RADIUS Attribute 27). Range is 1-65535 seconds Default is 60 seconds
bridge-group *<1-9999>* |	Add this interface to the specified bridge-group.
[dot1x [credential *<WORD>*] |	Dot1x credential profile.
[dot1x max-auth-req *<1-10>*] |	Maximum number of reauthentication attempt.
[dot1x max-req *<1-10>*] |	Maximum number of retries.
[dot1x pae authenticator | supplicant] |	Sets the Port Access Entity (PAE) type. Select the pae type, authenticator or supplicant.
[dot1x authenticator] |	The interface acts only as an authenticator and does not respond to any messages meant for a supplicant.
[dot1x supplicant] |	The interface acts only as a supplicant and does not respond to messages that are meant for an authenticator.
[dot1x timeout quiet-period *<1-65535>* | supp-period *<1-65535>* | tx-period *<1-65535>*] |	Quiet period in seconds. Supplicant timeout for reply Supplicant timeout for retries.
[ip address [*<A.B.C.D>* *<A.B.C.D>* secondary | dhcp] |	Configure IP parameters. **IP address/IP mask**—Configure the IP address/ mask of this interface. **secondary**—add secondary or ip aliasing address for this interface. Max secondary address-1-128 You must define a primary address before secondary IP addresses Primary and secondary address can be on the same of different subnets of the primary address.

[ip dhcp client class-id *<LINE>* | auto] |	**DHCP client —** Specify a Class-id string, truncated to 200 characters. This same string or text will be configured on the server side and associated with an address to give the client. **Class ID**: ● Auto ● Line
[ip dhcp client-id ethernet *<1-x>* | ascii *<WORD>* | auto | hex *<Hex-String>]* |	**Client ID:** This can be configured to be the Ethernet interface number, ASCII text, Hex string or set to Auto. option—60—Vendor class identifier<oem-name>:<model>:<serial#> in ASCII
[ip dhcp client default-route-distance *<1-255>*] |	Default route distance is a value that your IOLAN uses to select the best path when there are two or more different routes to the same destination from two different routing protocols. A static route is normally set too 1. The smaller the default route distance, the more reliable the protocol. Range is 1-255 (with 1 being the most reliable) and 255 is route not used or unknown.
[ip dhcp client hostname]	Specify a value for hostname option.
[ipv6 address *<X:X:X:X::X/<0-128>* eui-64]	Configure the IPv6 address and prefix length and EUI-64 for this interface.
[ipv6 address dhcp] |	Obtain an IPv6 address using DHCP.
[ipv6 address autoconfig] |	Obtain address from autoconfiguration.

ipv6 address prefix-from provider] ***<WORD>*** **address [*<1-65535>*** **| eui-64] | sla-length** ***<0-16>*** **sla-id** ***<0-65535>*** **] |**	The command is not available if <pd-name> is defined on the cellular interface. IPv6 address is assigned using Prefix Delegation which has name <pd-name>. SLA length and SLA-ID form the network part of IPv6 address for delegated interface. Range of sla-id: <0-65535>. Default: <0-128> Range for sla-length: <0-16>. Default is difference between requested length and 64 Value of SLA-ID must fit in the SLA length For a given <pd-name>, SLA ID must be unique Add • Prefix from provider— • PD name—select name from the drop-down box • PD ID# (0-65535) • Prefix length—length of prefix (48-64)
[enable] |	Enable IPv6 on this interface.
[ipv6 nd dad attempts ***<0-600>***	IPv6 Interface Neighbor Discovery sub-commands
[ipv6 nd dad attempts ***<0-600>*** **] |**	DAD (duplicate address detection) attempts—To check the uniqueness of an IPv6 address, a node sends Neighbor Solicitation messages. Use this command to specify the number of consecutive Neighbor Solicitation messages (dad_attempts) to be sent before this address can be configured. Range 1–600 Default is 1
[ipv6 nd managed config flags] |	Specify whether hosts use the administrated protocol for address auto-configuration. Default is disabled (host uses stateless)
[ipv6 nd other-config-flags] |	Specify whether hosts use the administrated protocol for non-address auto-configuration information. Default is disabled (hosts use stateless auto-configuration of no-address information.
[ipv6 nd prefix] |	prefix—specifies the IPv6 prefix advertised on the interface Configure the prefix length. Range is 0–128
[ipv6 nd no-autoconfig] |	A prefix is onlink when it is assigned to an interface on a specified link. Enable or disable prefix for onlink determination. Default is off

<table>
<tr><td><b>[ipv6 nd no-onlink] |</b></td><td>The sending router can indicate that a prefix is to be used for address autoconfiguration by setting the autonomous flag and specifying a nonzero Valid Lifetime value for the prefix.
Default is off</td></tr>
<tr><td><b>[ipv6 nd ra] |</b></td><td>Router Advertisement Control.</td></tr>
<tr><td><b>[nd ra dns server <i>&lt;X:X:X:X::X&gt;</i>] |</b></td><td>Specify the name server in RA.</td></tr>
<tr><td><b>[ipv6 nd ra hop-limit <i>&lt;1-255&gt;</i> | unspecified</b></td><td>Specifies the Hop Count field of the IP header for outgoing (unicast) IP packets.
Range is 1–255
Default is 64</td></tr>
<tr><td><b>[ipv6 nd ra interval <i>&lt;4-1800&gt;</i> <i>&lt;3-1350></i>] |</b></td><td>Specifies the maximum/minimum time allowed between sending unsolicited multicast router advertisements.
Range of minimum is 3 to *0.75 max (dynamic range)
Default maximum 600 seconds, minimum is 0.33*max
Range is 1–1800 in seconds</td></tr>
<tr><td><b>[ipv6 nd ra lifetime <i>&lt;0&gt;</i> <i>&lt;4-9000&gt;</i>] |</b></td><td>The lifetime associated with the default router in seconds. A value of 0 indicates that the router is not a default router and doesn't appear on the default router list. The router lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options.
Range is 4-1800 seconds
Minimum interval is 3-1350 in seconds
Default is 1800 seconds
0 = not a default route</td></tr>
<tr><td><b>[ipv6 nd ra suppress] |</b></td><td>Enable or disable IPv6 Router advertisements.
Default is send router advertisements</td></tr>
<tr><td><b>[ipv6 nd reachable time <i>&lt;0-3600000></i>] |</b></td><td>Specifies the length in time (milliseconds) a node assumes a neighbor is reachable after receiving a reachability confirmation
Default is 0 (unspecified by this router)
Range is 0-360000 milliseconds</td></tr>
<tr><td><b>[ipv6 nd retransmission-time <i>&lt;0-</i>
<i>3600000&gt;</i>] |</b></td><td>The retransmission timer is used to control the time (in milliseconds) between retransmissions of neighbor solicitation messages from the user equipment (UE).
Range 0–3600000 in milliseconds
Default is 0</td></tr>
</table>

[ipv6 nd router-preference high | low | medium] |	Set the default router preference. A High value means this IOLAN will be preferred. • **High** • **Medium** • **Low** Default is medium
[ipv6 pd *<WORD>* instance-id *<0-65535>* | request-length *<48-64>*] |	Specify the prefix name Specify the prefix delegation instance. Value is 0-65535
lldp max-neighbors *<1-50>* | receive | tvl-select mac-phy-cfg | management-address | max-frame-size | port-description | system-capabilities | system-description | system-name | transmit |	Configure LLDP parameters.
mab eap |	Sets MAC authentication bypass interface commands.
[mac access-group *<WORD>* deny | disable | permit] |	Configure mac access-group parameters for this interface.
mtu *<1280-9000>* |	Configure maximum transmission unit (MTU). Values are 1280-9000
power efficient-ethernet auto |	Configure Ethernet interface power settings.
shutdown |	Shutdown this interface.
[spanning-tree [bpdufilter enable | disable] |	Configure interface parameters for spanning tree. Don’t send or receive BPDUs on this interface. Default is Disabled
[spanning-tree bpduguard [disable | enable] |	Don’t accept BPDUs on this interface. Default is Disabled
[spanning-tree cost *<1-200000000>*] |	Change port path cost. Value is 1 to 200000000
[spanning-tree guard loop | none | root | topology-change] |	Default is auto (defined by STP protocol) • loop • none • root • topology-change

[spanning-tree link-type auto | point-to-point | shared] |	● auto—this interface is point-to-point if configured for full duplex operation ● point-to-point ● shared
[spanning-tree mcheck] |	Force the mode from STP to RSTP/MSTP mode.
[spanning-tree mst cost *<1-200000000>*] |	Change path cost and port priority for multiple spanning tree mode.
[spanning-tree port-priority *<0-240>*] |	Change the port priority for an instance. (increments of 16) Default is 128
[spanning-tree portfast disable] |	When enabled an interface will jump to the forwarding state of spanning-tree.
[spanning-tree portfast edge] |	Portfast edge—is used to configure a port on which an end device is connected, such as a PC. All ports directly connected to end devices cannot create bridging loops in the network. Therefore, the edge port directly transitions to the forwarding state, and skips the listening and learning stages.
[spanning-tree portfast network] |	This feature causes the IOLAN to enter the STP forwarding-state immediately or upon a linkup event, thus passing the listening and learning states. Some applications need to connect to the network immediately, else they will timeout.
[speed |	Configure the Ethernet speed ● 10 ● 100 ● 1000 ● auto
[vrrp *<1-255>*] |	This interface is part of VRRP group number.
Command Modes	Perle**(config-if-range)**#

Usage Guidelines

Set parameters for multiple Ethernet ports.

Examples

This example restricts IPv6 on Ethernet port range 1-2.

```
Perle(config)#interface range ethernet 1 , 2
Perle(config-if-range)#ipsec restrict
```

Related Commands

(config-if)#

(config-if)#bvi

(config-if)#cellular

(config-if)#dialer

(config-if-ethernet)#

(config-subif)#

(config-if-range)#

(config-if)#openvpn-tunnel

(config-if-port-channel)#

(config-if-sfp)#

(config-if)#tunnel

(config-if-vrrp)#

(config-if)#openvpn-tunnel

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-if)# openvpn-tunnel**
{*<0-999>* **tap | tun] |**	Tunnel interface number. Choose tap or tun device. tap (L2 link layer) tun (L3 network layer)
[bridge-group *<1-9999>*] |	Sets transparent bridging interface parameters.
[ip ddns service dyndns login *<WORD>* **password** *<WORD>* **| host** *<WORD>***| host-group** *<WORD>* **| use-web skip** *<WORD>* **| url** *<WORD>*] |	**DDNS**— **Service**—use dyndns login/password—configure the login id and password for the dnydns server. **host/host-group**—Hostname/list of hostnames registered with the DDNS service. **skip**—skip everything before this on the given URL. **Use-web URL**—This field should be left blank.
[ip dhcp–relay] |	Set DHCP-relay for this interface.
ipv6 [enable] |	Enable IPv6 on this interface.
[ipv6 nd dad attempts *<0-600>*] |	DAD (duplicate address detection) attempts—To check the uniqueness of an IPv6 address, a node sends Neighbor Solicitation messages. Use this command to specify the number of consecutive Neighbor Solicitation messages (dad_attempts) to be sent before this address can be configured. Range 1–600 Default is 1

[ipv6 nd managed config flags] |	Specify whether hosts use the administrated protocol for address auto-configuration. Default is disabled (host uses stateless)
[ipv6 nd other-config-flags] |	Specify whether hosts use the administrated protocol for non-address auto-configuration information. Default is disabled (hosts use stateless auto-configuration of no-address information.
[ipv6 nd prefix] |	Specifies the IPv6 prefix advertised on the interface Configure the prefix length. Range is 0–128
[ipv6 nd no-autoconfig] |	A prefix is onlink when it is assigned to an interface on a specified link. Enable or disable prefix for onlink determination. Default is off
[ipv6 nd no-onlink] |	The sending router can indicate that a prefix is to be used for address autoconfiguration by setting the autonomous flag and specifying a nonzero Valid Lifetime value for the prefix. Default is off
[ipv6 nd ra] |	Router Advertisement Control.
[nd ra dns server *<X:X:X:X::X>*] |	Specify the name server in RA.
[ipv6 nd ra hop-limit *<1-255>* | unspecified	Specifies the Hop Count field of the IP header for outgoing (unicast) IP packets. Range is 1–255 Default is 64
[ipv6 nd ra interval *<4-1800>* *<3-1350>*] |	Specifies the maximum/minimum time allowed between sending unsolicited multicast router advertisements. Range of minimum is 3 to *0.75 max (dynamic range) Default maximum 600 seconds, minimum is 0.33*max Range is 1–1800 in seconds

[ipv6 nd ra lifetime *<0> <4-9000>*] |	The lifetime associated with the default router in seconds. A value of 0 indicates that the router is not a default router and doesn't appear on the default router list. The router lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options. Range is 4-1800 seconds Minimum interval is 3-1350 in seconds Default is 1800 seconds 0 = not a default route
[ipv6 nd ra suppress] |	Enable or disable IPv6 Router advertisements. Default is send router advertisements
[ipv6 nd reachable time *<0-3600000>*] |	Specifies the length in time (milliseconds) a node assumes a neighbor is reachable after receiving a reachability confirmation Default is 0 (unspecified by this router) Range is 0-360000 milliseconds
[ipv6 nd retransmission-time *<0-3600000>*] |	The retransmission timer is used to control the time (in milliseconds) between retransmissions of neighbor solicitation messages from the user equipment (UE). Range 0–3600000 in milliseconds Default is 0
[ipv6 nd router-preference high | low | medium] |	Set the default router preference. A High value means this IOLAN will be preferred. • **High** • **Medium** • **Low** Default is medium
Command Modes	(config-if)#

Usage Guidelines

Set configuration parameters for OpenVPN tunnel.

Examples

This example sets SNMP to trap for link-status.

```
(config-if)#snmp trap link-status
```

Related Commands

(config-if)#
(config-if)#bvi
(config-if)#cellular
(config-if)#dialer
(config-if-ethernet)#
(config-subif)#
(config-if-range)#
(config-if)#openvpn-tunnel
(config-if-port-channel)#
(config-if-sfp)#
(config-if)#tunnel
(config-if-vrrp)#

(config-if-port-channel)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-if-port-channel)#
port-channel number *<1-13>*	Enter the port channel number.
[hash-policy ip-port | mac | mac_ip] |	Select the hash policy to use for this port channel. **Note:** hash-policy option available only when mode is set to active-lacp.
[ip address [*<A.B.C.D> <A.B.C.D>* **| dhcp] |**	Configure IP parameters. **IP address/IP mask**—Configure the IP address/ mask of this interface or DHCP.
[ipv6 address *<X:X:X:X::X/ <0-128>* **eui-64]**	Configure the IPv6 address, prefix length and EUI-64 for this interface.
[ipv6 address autoconfig] |	Obtain IPv6 address from autoconfiguration.
[ipv6 address dhcp] |	Obtain an IPv6 address using DHCP.
[enable] |	Enable IPv6 on this interface.
[mode active-lacp | active-standby] |	Sets port-channel for active LACP or active standby.
[mtu *<64-1500]* **|**	Sets maximum transmission unit (MTU). Values are 64 to 1500 bytes

[primary-interface interface ethernet *<1-x>* | sfp *<1-x>*] |	Select the primary interface for active standby. <1-x> = maximum number of ethernet ports, (depends on the model) sfp <1-x> (depends on the model) Note: primary interface option is available when mode is set to active standby.
[shutdown] |	Shutdown this interface.
Command Modes	Perle(config-if)#

Usage Guidelines

Set up port channel parameters for this interface.

Examples

This example sets the mode of the interface to active LACP.

```
Perle(config-if-portchannel)#mode lacp-active
```

Related Commands

(config-if)#

(config-if)#bvi

(config-if)#cellular

(config-if)#dialer

(config-if-ethernet)#

(config-subif)#

(config-if-range)#

(config-if)#openvpn-tunnel

(config-if-port-channel)#

(config-if-sfp)#

(config-if)#tunnel

(config-if-vrrp)#

(config-if-sfp)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-if-sfp)#**
{**[alarm profile *<WORD>*] |**	Use this alarm profile for this interface.
[arp disable-arp-filter] |	Configure ARP parameters. If enabled the IOLAN responds to the 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

[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] |	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-proxy-arp] |	Enable IOLAN/router to respond to an ARP request on behalf of another node.
[timeout *<1-2147483>*] |	If an ARP entry is not used for a specific amount of time the entry is removed from the caching table.
[bridge-group *<1-9999>*] |	Adds this interface to the specified bridge-group.
[channel-group *<1-13>*] |	
[ip address [*<A.B.C.D>* *<A.B.C.D>* secondary | dhcp] |	Configure IP parameters. **IP address/IP mask**—Configure the IP address/ mask of this interface. **secondary**—add secondary or ip aliasing address for this interface. Max secondary address-1-128 You must define a primary address before secondary IP addresses Primary and secondary address can be on the same of different subnets of the primary address.
[ip ddns service dyndns login *<WORD>* password *<WORD>* | host *<WORD>*| host-group *<WORD>* | use-web skip *<WORD>* | url *<WORD>*] |	**DDNS—** **Service**—use dyndns login/password—configure the login id and password for the dnydns server. **host/host-group**—Hostname/list of hostnames registered with the DDNS service. **skip**—skip everything before this on the given URL. **Use-web URL**—This field should be left blank.
[ip dns dhcp] |	Use DNS servers received from DHCP server for specified interface.
[ip dhcp–relay] |	Set DHCP-relay for this interface.

[ipv6 address *<X:X:X:X::X/ <0-128>* eui-64]	Configure the IPv6 address and prefix length and EUI-64 for this interface.
[ipv6 address autoconfig] |	Obtain address from autoconfiguration.
[ipv6 address dhcp] |	Obtain an IPv6 address using DHCP.
ipv6 address prefix-from provider] *<WORD>* address [*<1-65535>* | eui-64] | sla-length *<0-16>* sla-id *<0-65535>*] |	The command is not available if <pd-name> is defined on the cellular interface. IPv6 address is assigned using Prefix Delegation which has name <pd-name>. SLA length and SLA-ID form the network part of IPv6 address for delegated interface. Range of sla-id: <0-65535>. Default: <0-128> Range for sla-length: <0-16>. Default is difference between requested length and 64 Value of SLA-ID must fit in the SLA length For a given <pd-name>, SLA ID must be unique Add ● Prefix from provider— ● PD name—select name from the drop-down box ● PD ID# (0-65535) ● Prefix length—length of prefix (48-64)
[enable] |	Enable IPv6 on this interface.
[ipv6 nd dad attempts *<0-600>*] |	DAD (duplicate address detection) attempts—To check the uniqueness of an IPv6 address, a node sends Neighbor Solicitation messages. Use this command to specify the number of consecutive Neighbor Solicitation messages (dad_attempts) to be sent before this address can be configured. Range 1–600 Default is 1
[ipv6 nd managed config flags] |	Specify whether hosts use the administrated protocol for address auto-configuration. Default is disabled (host uses stateless)
[ipv6 nd other-config-flags] |	Specify whether hosts use the administrated protocol for non-address auto-configuration information. Default is disabled (hosts use stateless auto-configuration of no-address information.
[ipv6 nd prefix] |	prefix—specifies the IPv6 prefix advertised on the interface Configure the prefix length. Range is 0–128

[ipv6 nd no-autoconfig] |	A prefix is onlink when it is assigned to an interface on a specified link. Enable or disable prefix for onlink determination. Default is off
[ipv6 nd no-onlink] |	The sending router can indicate that a prefix is to be used for address autoconfiguration by setting the autonomous flag and specifying a nonzero Valid Lifetime value for the prefix. Default is off
[ipv6 nd ra] |	Router Advertisement Control.
[nd ra dns server *<X:X:X:X::X>*] |	Specify the name server in RA.
[ipv6 nd ra hop-limit *<1-255>* | unspecified	Specifies the Hop Count field of the IP header for outgoing (unicast) IP packets. Range is 1–255 Default is 64
[ipv6 nd ra interval *<4-1800> <3-1350>*] |	Specifies the maximum/minimum time allowed between sending unsolicited multicast router advertisements. Range of minimum is 3 to *0.75 max (dynamic range) Default maximum 600 seconds, minimum is 0.33*max Range is 1–1800 in seconds
[ipv6 nd ra lifetime *<0> <4-9000>*] |	The lifetime associated with the default router in seconds. A value of 0 indicates that the router is not a default router and doesn't appear on the default router list. The router lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options. Range is 4-1800 seconds Minimum interval is 3-1350 in seconds Default is 1800 seconds 0 = not a default route
[ipv6 nd ra suppress] |	Enable or disable IPv6 Router advertisements. Default is send router advertisements
[ipv6 nd reachable time *<0-3600000>*] |	Specifies the length in time (milliseconds) a node assumes a neighbor is reachable after receiving a reachability confirmation Default is 0 (unspecified by this router) Range is 0-360000 milliseconds

[ipv6 nd retransmission-time *<0-3600000>*] |	The retransmission timer is used to control the time (in milliseconds) between retransmissions of neighbor solicitation messages from the user equipment (UE). Range 0–3600000 in milliseconds Default is 0
[ipv6 nd router-preference high | low | medium] |	Set the default router preference. A High value means this IOLAN will be preferred. • **High** • **Medium** • **Low** Default is medium
[ipv6 pd *<WORD>* instance-id *<0-65535>* | request-length *<48-64>*] |	Specify the prefix name Specify the prefix delegation instance. Value is 0-65535
[lldp max-neighbors *<1-50>* | receive | tvl-select mac-phy-cfg | management-address | max-frame-size | port-description | system -capabilities | system-description | system-name | transmit] |	Configure LLDP parameters.
[mac access-group <word> deny | disable | permit] |	Sets interface MAC access-list parameters.
[mtu *<1280-1500>*] |	Sets maximum transmission unit (MTU). Values are 64 t 9000 bytes Default is 1500 bytes
[sgmii] |	Set interface to support sgmii.
[shutdown |	Shutdown this interface.
[spanning-tree [bpdufilter enable | disable] |	Configure interface parameters for spanning tree. Don’t send or receive BPDUs on this interface. Default is Disabled
[spanning-tree bpduguard [disable | enable] |	Don’t accept BPDUs on this interface. Default is Disabled
[spanning-tree cost *<1-200000000>*] |	Change port path cost. Value is 1 to 200000000

[spanning-tree guard loop | none | root | topology-change] |	Default is auto (defined by STP protocol) • loop • none • root • topology-change
[spanning-tree link-type auto | point-to-point | shared] |	• auto—this interface is point-to-point if configured for full duplex operation • point-to-point • shared
[spanning-tree mcheck] |	Force the mode from STP to RSTP/MSTP mode.
[spanning-tree mst cost *<1-200000000>*] |	Change path cost and port priority for multiple spanning tree mode.
[spanning-tree port-priority *<0-240>*] |	Change the port priority for an instance. (increments of 16) Default is 128
[spanning-tree portfast disable] |	When enabled an interface will jump to the forwarding state of spanning-tree.
[spanning-tree portfast edge] |	Portfast edge—is used to configure a port on which an end device is connected, such as a PC. All ports directly connected to end devices cannot create bridging loops in the network. Therefore, the edge port directly transitions to the forwarding state, and skips the listening and learning stages.
[spanning-tree portfast network] |	This feature causes the IOLAN to enter the STP forwarding-state immediately or upon a linkup event, thus passing the listening and learning states. Some applications need to connect to the network immediately, else they will timeout.
	Therefore, the edge port directly transitions to the forwarding state, and skips the listening and learning stages. **portfast disable**—when enabled an interface will jump to the forwarding state of spanning-tree.
speed 1000 | nonegotiate |	Configure the Ethernet speed.. • 1000 • nonegotiate
vrrp *<1-255>* |	This interface is part of VRRP group number.
zone-member security *<WORD>*}	This interface is a member of zone security.

Command Modes	Perle(config-if)#

Usage Guidelines

Set up SFP parameters for this interface.

Examples

This example sets the speed for this interface to 1000.

```
Perle(config-if)#speed 1000
```

Related Commands

(config-if)#
(config-if)#bvi
(config-if)#cellular
(config-if)#dialer
(config-if-ethernet)#
(config-subif)#
(config-if-range)#
(config-if)#openvpn-tunnel
(config-if-port-channel)#
(config-if-sfp)#
(config-if)#tunnel
(config-if-vrrp)#

(config-if)#tunnel

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-if)# tunnel**
{**[tunnel** *<0-999>* **mode [gre ip | ipv6ip 6in4] |**	Sets mode gre and ipv6up tunnel interface parameters.
[arp disable-arp-filter] |	Configure ARP parameters. If enabled the IOLAN responds to the 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
[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] |	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-proxy-arp] |	Enable IOLAN to respond to an ARP request on behalf of another node.
[timeout *<1-2147483>* **] |**	If an ARP entry is not used for a specific amount of time the entry is removed from the caching table.
ip [address *<A.B.C.D> <A.B.C.D>* **] |**	Configure IP parameters. **IP address/IP mask**—Configure the IP address/ mask of this interface **secondary**—add secondary addresses) IP aliasing) for this interface
[ip ddns service dyndns login *<WORD>* **password** *<WORD>* **| host** *<WORD>* **| host-group** *<WORD>* **| use-web skip** *<WORD>* **| url** *<WORD>* **] |**	**DDNS**— **Service**—use dyndns login/password—configure the login id and password for the dnydns server. **host/host-group**—Hostname/list of hostnames registered with the DDNS service. **skip**—skip everything before this on the given URL. **Use-web URL**—Enter the URL that you want to obtain an IP address from. This allows the IOLAN to be seen on the Internet as a public address.
[ip dhcp–relay] |	Set DHCP-relay for this interface.
[ipv6 address *<X:X:X:X::X/<0-128>* **eui-64]**	Configure the IPv6 address and prefix length and EUI-64 for this interface.
[ipv6 nd dad attempts *<0-600>* **] |**	DAD (duplicate address detection) attempts—To check the uniqueness of an IPv6 address, a node sends Neighbor Solicitation messages. Use this command to specify the number of consecutive Neighbor Solicitation messages (dad_attempts) to be sent before this address can be configured. Range 1–600 Default is 1
[ipv6 nd managed config flags] |	Specify whether hosts use the administrated protocol for address auto-configuration. Default is disabled (host uses stateless)

[ipv6 nd other-config-flags] |	Specify whether hosts use the administrated protocol for non-address auto-configuration information. Default is disabled (hosts use stateless auto-configuration of no-address information.
[ipv6 nd prefix] |	Specifies the IPv6 prefix advertised on the interface Configure the prefix length. Range is 0–128
[ipv6 nd no-autoconfig] |	A prefix is onlink when it is assigned to an interface on a specified link. Enable or disable prefix for onlink determination. Default is off
[ipv6 nd no-onlink] |	The sending router can indicate that a prefix is to be used for address autoconfiguration by setting the autonomous flag and specifying a nonzero Valid Lifetime value for the prefix. Default is off
[ipv6 nd ra] |	Router Advertisement Control.
[nd ra dns server *<X:X:X:X::X>*] |	Specify the name server in RA.
[ipv6 nd ra hop-limit *<1-255>* | unspecified] |	Specifies the Hop Count field of the IP header for outgoing (unicast) IP packets. Range is 1–255 Default is 64
[ipv6 nd ra interval *<4-1800> <3-1350>*] |	Specifies the maximum/minimum time allowed between sending unsolicited multicast router advertisements. Range of minimum is 3 to *0.75 max (dynamic range) Default maximum 600 seconds, minimum is 0.33*max Range is 1–1800 in seconds
[ipv6 nd ra lifetime *<0> <4-9000>*] |	The lifetime associated with the default router in seconds. A value of 0 indicates that the router is not a default router and doesn't appear on the default router list. The router lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options. Range is 4-1800 seconds Minimum interval is 3-1350 in seconds Default is 1800 seconds 0 = not a default route
[ipv6 nd ra suppress] |	Enable or disable IPv6 Router advertisements. Default is send router advertisements

[ipv6 nd reachable time *<0-3600000>*] |	Specifies the length in time (milliseconds) a node assumes a neighbor is reachable after receiving a reachability confirmation Default is 0 (unspecified by this router) Range is 0-360000 milliseconds
[ipv6 nd retransmission-time *<0-* *3600000>*] |	The retransmission timer is used to control the time (in milliseconds) between retransmissions of neighbor solicitation messages from the user equipment (UE). Range 0–3600000 in milliseconds Default is 0
[ipv6 nd router-preference high | low | medium] |	Set the default router preference. A High value means this IOLAN will be preferred. • **High** • **Medium** • **Low** Default is medium
[ipv6 mtu *<64-1500>*] |	Configure maximum transmission unit (MTU). Values are 64-1500 Default is 1476
[shutdown] |	Shutdown this interface.
tunnel destination *<A.B.C.D>*] |	Specify the destination of the tunnel packets.
[multicast] |	Set multicast for the tunnel.
[source *<A.B.C.D>* source *<A.B.C.D>*] |	Specify the source of the tunnel packets.
[tos *<0-99>*] |	Set the type of service byte.
[ttl *<1-255>*] |	Set the time to live.
Command Modes	Perle(config-if)#

Usage Guidelines

Use this command to configure tunnel interface parameters.

Examples

This example enables ARP accepts on this interface.

```
Perle(config-if)# arp enable-accepts
```

Related Commands

(config-if)#

(config-if)#bvi

(config-if)#cellular

(config-if)#dialer

(config-if-ethernet)#

(config-subif)#

(config-if-range)#

(config-if)#openvpn-tunnel

(config-if-port-channel)#

(config-if-sfp)#

(config-if)#tunnel

(config-if-vrrp)#

(config-if-vrrp)#

Use the no form of this command to negate a command or set to defaults.

Syntax Description	(config-if-vrrp)#
[authentication 0 *<WORD>* | 7 *<WORD>*| md5 *<key-string>* 0 *<WORD>* | 7 *<WORD>*| text 0 *<WORD>* | 7 *<WORD>*] |	Enter authentication password.
[ip *<A.B.C.D> <A.B.C.D>*] |	Configure IP parameters. VRRP group IP address and netmask.
[enable] |	Enable IPv6 on this interface.
[ipv6 [address *<X:X:X:X::X/ <0-128>*] |	VRRP group IPv6 address and netmask.
[ipv6 nd dad attempts *<0-600>*] |	DAD (duplicate address detection) attempts—To check the uniqueness of an IPv6 address, a node sends Neighbor Solicitation messages. Use this command to specify the number of consecutive Neighbor Solicitation messages (dad_attempts) to be sent before this address can be configured. Range 1–600 Default is 1
[ipv6 nd managed config flags] |	Specify whether hosts use the administrated protocol for address auto-configuration. Default is disabled (host uses stateless)
[ipv6 nd other-config-flags] |	Specify whether hosts use the administrated protocol for non-address auto-configuration information. Default is disabled (hosts use stateless auto-configuration of no-address information.

[ipv6 nd prefix] |	Specifies the IPv6 prefix advertised on the interface Configure the prefix length. Range is 0–128
[ipv6 nd no-autoconfig] |	A prefix is onlink when it is assigned to an interface on a specified link. Enable or disable prefix for onlink determination. Default is off
[ipv6 nd no-onlink] |	The sending router can indicate that a prefix is to be used for address autoconfiguration by setting the autonomous flag and specifying a nonzero Valid Lifetime value for the prefix. Default is off
[ipv6 nd ra] |	Router Advertisement Control.
[nd ra dns server *<X:X:X:X::X>*] |	Specify the name server in RA.
[ipv6 nd ra hop-limit *<1-255>* | unspecified	Specifies the Hop Count field of the IP header for outgoing (unicast) IP packets. Range is 1–255 Default is 64
[ipv6 nd ra interval *<4-1800>* *<3-1350>*] |	Specifies the maximum/minimum time allowed between sending unsolicited multicast router advertisements. Range of minimum is 3 to *0.75 max (dynamic range) Default maximum 600 seconds, minimum is 0.33*max Range is 1–1800 in seconds
[ipv6 nd ra lifetime *<0>* *<4-9000>*] |	The lifetime associated with the default router in seconds. A value of 0 indicates that the router is not a default router and doesn't appear on the default router list. The router lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options. Range is 4-1800 seconds Minimum interval is 3-1350 in seconds Default is 1800 seconds 0 = not a default route
[ipv6 nd ra suppress] |	Enable or disable IPv6 Router advertisements. Default is send router advertisements

[ipv6 nd reachable time *<0-3600000>*] |	Specifies the length in time (milliseconds) a node assumes a neighbor is reachable after receiving a reachability confirmation Default is 0 (unspecified by this router) Range is 0-360000 milliseconds
[ipv6 nd retransmission-time *<0- 3600000>*] |	The retransmission timer is used to control the time (in milliseconds) between retransmissions of neighbor solicitation messages from the user equipment (UE). Range 0–3600000 in milliseconds Default is 0
[ipv6 nd router-preference high | low | medium] |	Set the default router preference. A High value means this IOLAN will be preferred. - **High** - **Medium** - **Low** Default is medium
[mtu *<64-9000>*] |	Configure maximum transmission unit (MTU). Values are 64 to 9000 bytes Default is 1500 bytes
[peer-address *<A.B.C.D>*] |	Configure an unicast VRRP peer IP address.
[preempt delay *<0-1000>*] |	By default, the preemption delay is 0, indicating immediate preemption. In immediate preemption mode, a backup immediately switches to the master when detecting that its priority is higher than the master's priority. Delay is 0 to 1000 in seconds. Disabled—Even if a VRRP router with a higher priority than the current master is up, it does not replace the current master. Only the original master (when it becomes available) replaces the backup. Values 1-000 seconds Default is 0 (no delay)
[priority *<1-255>*] |	The priority value for the VRRP router that owns the IP address(es) associated with the virtual router. Values are 1-255 Default is 100
[shutdown] |	Shutdown this interface.

[sync-group *<WORD>*] |	Adds this sync VRRP group to a sync group. Sync groups are used to link VRRP groups together in order to propagate transition changes from one group to another group.Assign this interface to a sync group. Adds this sync VRRP group to a sync group. Sync groups are used to link VRRP groups together in order to propagate transition changes from one group to another group. To clarify, in a VRRP synchronization group (“sync group”) are synchronized such that, if one of the interfaces in the group fails over to backup, all interfaces in the group fail over to backup. For example, if one interface on a master router fails, **Note:** VRRP groups in a sync group must have similar priority and preemption configurations. Before enabling a sync-group you should verify that one IOLAN is master of both groups and the other is backup of both groups. If both side think they are master of the same group, then enabling a sync group can cause endless transitioning to get in sync.
[timers *<10-255000>*] |	Configure the time interval between the advertisement packets that are being sent to other Virtual Router Redundancy Protocol (VRRP) routers in the same group Values are 10–255000 milliseconds Default is 1000 milliseconds
[version] |	Configure the version number. Values are 2–3 Default is 3
Command Modes	Perle(config-if-vrrp)#

Usage Guidelines

Use this command to configure VRRP parameters.
Your IOLAN supports the Virtual Router Redundancy Protocol (VRRP).
VRRP is an election and redundancy protocol that dynamically assigns the responsibility of a virtual router to one of the physical routers on a LAN.
This increase the availability and reliability of routing paths in the network.
In VRRP, one physical router in a virtual router is elected as the master, with the other physical router of the same virtual router acting as backups in case the master fails. The physical routers are referred as VRRP routers.
The default gateway of a participating host is assigned to the virtual router instead of a physical router. If the physical router is routing packets on behalf of the virtual router fails, another physical router is selected to automatically replace it. The physical router forwarding packets at any given time is called the master router.

Examples

This example sets VRRP for version 2.

```
Perle(config)#interface ethernet 2
Perle(config-if)#vrrp 10
Perle(config-if-vrrp)#version 2
```

Related Commands

(config-if)#

(config-if)#bvi

(config-if)#cellular

(config-if)#dialer

(config-if-ethernet)#

(config-subif)#

(config-if-range)#

(config-if)#openvpn-tunnel

(config-if-port-channel)#

(config-if-sfp)#

(config-if)#tunnel

(config-if-vrrp)#

6 Interface line mode

This chapter defines all the CLI commands associated with configuring the console and tty ports. Some CLI commands may not be applicable to your model or running software.

line

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**line**
{**[console *<0-0>*] |**	Applies only to models with serial ports. Configure console port parameters.
[tty <1-x>] |	Applies only to models with serial ports. Configure tty port parameters.
[vty]}	Configure vty port parameters.
Command Modes	Perle>enable Perle>config Perle#line

Usage Guidelines

Use this command to change to line mode.

Examples

This example set terminal width to 80.

```
Perle(config)#line vty
Perle(config-line)#width 80
```

Related Commands

(config-line)#tty and #usb

(config-line)#console

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-line)#console** This command applies only to models with console port/s.
{**[accounting exec *<WORD>* | default] |**	Use an accounting list with a specified name or default list.
[authorization exec *<WORD>* | default] |	Use an authorization with a specified name or default list.
[databits 7 | 8] |	Type 7 or 8 to set data bits.
[exec] |	Enables EXEC CLI session

[exec-timeout *<0-35791> <0-2147483>*] |	Configure the console session CLI timeout. Values are 0 to 35791 in minutes Default is 5 minutes
[history size *0-256>*] |	Configure the size of the history buffer.
[length *0-512>*] |	Configure the number of lines displayed on the screen. Type 0 for no pausing at end of page.
[login authentication *<WORD>* | default] |	Use the specified list for authentication requests or use the default list.
media interface auto | null	● use null for no console port ● use usb/tty as the console port
[parity even | odd | none] |	Configure parity for console mode.
[speed | 115200 | 19200 | 38400 | 57600 | 9600] |	Set the speed for this interface. ● 115200 ● 19200 ● 38400 ● 57600 ● 9600
[stopbits 1 | 2] |	Configure stop bits for console mode.
[timeout login response *<1-300>*] |	Configure timeout for user responses during the login sequence.
[transport output all | none | ssh | telnet] |	Allows the user on the console port to telnet or ssh out of the IOLAN.
[width *<0-512>*]}	Configure the width of the terminal display.
Command Default	console 0 timeout login response 30 login authentication default databits 8 parity none stopbits 1 speed 9600
Command Modes	Perle>enable Perle>config Perle(config)#line config 0 Perle(config-line)#

Usage Guidelines

Use these commands to set parameters for console mode.

Examples

These commands sets your console to speed 38400, databits 7 and stopbits 2.

```
Perle(config-line)#speed 38400
Perle(config-line)#databits 7
Perle(config-line)#stopbits 2
```

Related Commands

(config-line)#tty and #usb

(config-line)#tty and #usb

USB options only available on models with USB line ports.

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-line)#tty** Applies only to models with serial ports.
{**break break-interrupted |**	Configure how the break signal is interpreted from the peer. 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. Default is None
{**[break break-interrupted none] |**	The IOLAN ignores the break key completely and it is not passed through to the host.
[break break-interrupted 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.
{**break break-interrupted off] |**	When the break key is pressed, the IOLAN translates this into a telnet break signal which it sends to the host machine.
[break-delay *<1-65535>***] |**	This parameter defines the delay between the termination of a a break condition and the time data is sent out the serial port. Default is 0 ms (no delay).
[break-length *1-65535>***]** |	When the IOLAN receives a command from its peer to issue a break signal, this parameters defines the length of time the break condition is asserted on the serial port Default is 1000ms (1 second)

[connection-method dial-in | dial-out | dial-in-out | direct-connect | ms-direct-guest | ms-direct-host] |	**Dial in**—Enable this parameter if the device is remote and is dialing via a modem or ISDN TA Default is Disabled **Dial out**—Enable this parameter if the device if you want the modem to dial a number when the serial port is started. Default is Disabled
[cts-toggle off | on] |	Configure CTS toggle. Default is Off
[ts-toggle-final-delay *<0-1000>*] |	Configure CTS final delay in milliseconds. Value is 1–1000
[cts-toggle-inital-delay *<0-1000>*] |	Configure CTS initial delay in milliseconds. Value is 1–1000
[databits 5 | 6 | 7 | 8] |	Configure the data bits for this connection. Data bit options are
[data-logging off | on] |	When enabled, serial data is buffered if the TCP connection is lost. When the TCP connection is re-established, the buffered serial data is sent to its destination. If using the Trueport profile, data logging is only supported in Lite mode. When the data buffer fills, incoming serial data overwrites the oldest data. The minimum data buffer size is 4K. The maximum data buffer size is 256K. **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.
[dial-retries *<0-99>*] |	Configure the number of times the IOLAN attempts to re-establish a connection with a remote modem. Range is 0–99 Default is 2
[dial-timeouts *<0-99>*] |	Configure the number of seconds the IOLAN waits to establish a connection to a remote modem. Range is 1–99 Default is 45 seconds
[discard-characters-rxd-with-errors off |on] |	When enabled, the IOLAN discards characters received with a parity or framing error. Default is Disabled

[flow both | hard | none | soft] |	Configure handling of the data flow. Choose software (soft), hardware (hard), both or none. If you are using SLIP, set to Hard only. If you are using PPP set to either soft or hard (hard is recommended). If you select soft with PPP, you must set the ACCM parameter when you configure PPP for the serial port. Note: For USB ports the only valid options are none or soft. Default is None
[flowin off | on] |	Configure for flowin control. Default is On
[flowout off on] |	Configure for flowout control. Default is On
[hotkey-prefix *<0-ff>*] |	Configure the prefix that a user types to lock a serial port or redraw the Menu. Data Range: • ^a l—(Lowercase L) Locks the serial port until the user unlocks it. • ^a l—(Lowercase L) Locks the serial port until the user unlocks it. The user is prompted for a password (any password, excluding spaces) and locks the serial port. Next, the user must retype the password to unlock the serial port. • ^r—When you switch from a session back to the Menu, the screen may not be redrawn correctly. If this happens, use this command to redraw it properly. This is always Ctrl R, regardless of the Hot Key prefix. You can use the Hotkey Prefix to lock a serial port only when the Allow Port Locking parameter is enabled. Default is hexadecimal 01 (Ctrl-a, ^a)
[idle-timer *<0-4294967>*] |	Configure the inactivity timer to close a connection due to inactivity. When the idle timeout expires, the IOLAN ends the connection. Range is 0–4294967 seconds (about 49 days) Default is 0 seconds so the port never times out.

<table>
<tr><td>**[initiate-connection any-char | specific-char *<0-ff>*] |**</td><td>Configure the initiate a connection parameter
• Initiates a connection to the specified host when any data is received on the serial port.
• Initiates a connection to the specified host only when the specified character is received on the serial port.
Default is Disabled
Default is Disabled</td></tr>
<tr><td>**[internet address *<A.B.C.D>* | *<X:X:X::X>*] |**</td><td>Configure the Internet address of this serial port.</td></tr>
<tr><td>**[keepalive off | on] |**</td><td>Configure the TCP keepalive option. This parameter is used in conjunction with the Monitor Connection Status Interval parameter found under config ***serial***. The connection is monitored based on the monitor connection status interval timer. This timer specifies the inactivity period before "testing" the connection. Should the end device not respond, the connection will be dropped.
Note: If a network connection is accidentally dropped, it can take as long as the specified interval before reconnecting to the serial port.
Default is Off</td></tr>
<tr><td>**[lock off | on] |**</td><td>When enabled, the user can lock his terminal with a password using the hotkey prefix (ctrl-a) ^a (lowercase L). The IOLAN prompts the user for a password and a confirmation.
Default is Off.</td></tr>
<tr><td>**[map-cr-crlf off | on] |**</td><td>Configure to map carriage returns (CR) to carriage return line feed (CRLF).
Default is off</td></tr>
<tr><td>**media-type [straight | rolled]**</td><td>Option not valid on USB ports.
Select "straight" if you are connecting a straight thru cable.
Select "rolled" if the cable you are connecting a rolled cable.
See the Hardware guide for your model for cable pinouts.
Default is straight</td></tr>
<tr><td>**[modbus [master crlf | entry | protocol] | [slave cflf | protocol | uid-range] |**</td><td>Configure Modus master/ slave parameters.
Default is enabled</td></tr>
<tr><td>**[modem-init-string *<WORD>*] |**</td><td>Configure the initialization string to send to the modem.</td></tr>
</table>

[monitor-dsr-dtr on | off] |	Option not valid on USB interfaces. Configure port to monitor for dsr-dtr signals.
[motd off | on] |	Configure enables/disables the message of the day. Default is Disabled
[multihost entry *<1-49> <A.B.C.D>* | *<X:X:X::X>* port *<1-65535>*] |	Adds a multihost entry to the multihost table. Range 1 to 49 Port number 1 to 65535
[multisessions *<1-8>*] |	Configure the number of extra network connections available on a serial port, in addition to the single session that is always available. Enabling multisessions permits multiple users to monitor the same console port. Range is 1 to 8 Default is 0
[name *<WORD>*] |	Configure a name.
[packet-forwarding delay-between-messages *<1-65535>*] |	Packet forwarding option not available on USB ports. The minimum time, in milliseconds, between messages that must pass before the data is forwarded by the IOLAN. The range is 0-65535. The default is 250 ms.
[enable-end-tigger1 on | off] |	Enable or disable the end trigger1 hex character.
[enable-end-tigger2 on | off] |	Enable or disable the end trigger2 hex character.
[enable-eof1 on | off] |	Enable or disable the eof1 (end of frame) hex character
eof2 on | off] |	Enable or disable the eof2 (end of frame) hex character.
[enable-sof1 on | off] |	Enable or disable the sof1 (start of frame) hex character.
[enable-sof2 on | off] |	Enable or disable the sof2 (start of frame) hex character.
force-transmit-timer *<1-65535>*] |	When the specified amount of time, in milliseconds, elapses after the first character is received from the serial port, the packet is transmitted. After a packet is transmitted, the next character received starts the timer again. A value of zero (0) ignores this parameter. Valid values are 0-65535 ms. The default is 0.

[forwarding-rule strip-trigger | trigger | trigger+1 | trigger+2] |	Determines what is included in the Frame (based on the EOF1 or EOF1/EOF2) or Packet (based on Trigger1 or Trigger1/Trigger2). Choose one of the following options: **Strip-Trigger**—Strips out the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings. **Trigger**—Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings. **Trigger+1**—Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings, plus the first byte that follows the trigger. **Trigger+2**—Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings, plus the next two bytes received after the trigger.
[idle-timer *<1-65535>*] |	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. Valid values are 0-65535 ms. The default is 0.
[mode custom-on-frame-definition] |	This section 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. The default frame definition is SOF=00 and EOF=00.
[mode custom-on-specific-events] |	This section allows you to set a variety of packet definition options. The first criteria that is met causes the packet to be transmitted. For example, if 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.
[minimize-latency] |	This option ensures that any data received on the serial port will immediately be forwarded to the LAN. Select this option for timing-sensitive applications.
[minimize-latency optimize-network-throughput] |	This option provides optimal network usage while ensuring that the application performance is not compromised. Select this option when you want to minimize overall packet count, such as when the connection is over a WAN.

[minimize-latency prevent-message-fragmentation] |	This option detects the message, packet, or data blocking characteristics of the serial data and preserves it throughout the communication. Select this option for message-based applications or serial devices that are sensitive to inter-character delays within these messages.
[packet-size *<1-1024>*] |	The number of byte that must be received from the serial port before the packet is transmitted to the network. A value of zero (0) ignores this parameter. Valid values are 0-1024 bytes. The default is 0.
[sof1*<0-0xff>*] |	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. Valid values are in hex 0-FF. The default is 0.
[sof2*<0-0xff>*] |	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). Valid values are in hex 0-FF. The default is 0.
[start-frame-transmit off | on] | |	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.
[pages *<1-7>*] |	Configure the number of video pages the terminal supports. Range: 1 to 7 Default is 5 pages
[parity even | mark | none | odd | space] |	Configure the parity type. Data Options are: ● Even ● Odd ● Mark ● space ● none
[ppp phone-number *<number>*] |	Configure the phone number to use when Dial Out is enabled.

[ppp accm <*8 hex digits*>] |	Specifies the ACCM (Asynchronous Control Character Map) characters that should be escaped from the data stream. This 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). So entering 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 Line, you must enter a value of at least 000a0000 for the ACCM. The default value is 00000000, which means no characters will be escaped.
[ppp address-comp on | off] |	This determines whether compression of the PPP Address and Control fields take place on the link. The default is On. For most applications this should be enabled.
[ppp auth-tmout <*1-255*>] |	The timeout, in minutes, during which successful PAP or CHAP authentication must take place (when PAP or CHAP is turned On). If the timer expires before the remote end has been authenticated successfully, the link will be terminated.
[ppp authentication chap | pap | none] |	The type of authentication that will be done on the link. The default is CHAP. You can use PAP or CHAP (MD5CHAP, MSCHAP and MSCHAPv2) to authenticate a port or user on the IOLAN, from a remote location, or authenticate a remote client/ device, from the IOLAN. PAP is a one time challenge of a client/device requiring that it respond with a valid username and password. A timer operates during which successful authentication must take place. If the timer expires before the remote end has been authenticated successfully, the link will be terminated. CHAP challenges a client/device at regular intervals to validate itself with a username and a response, based on a hash of the secret (password). A timer operates during which successful authentication must take place.I f the timer expires before the remote end has been authenticated successfully, the link will be terminated. MD5CHAP and Microsoft's MSCHAP/MSCHAPv2 are supported. The IOLAN will attempt MSCHAPv2 with MPPC compression, but will negotiate to the variation of CHAP, compression and encryption that the remote peer wants to use .

	When setting either PAP and CHAP, make sure the IOLAN and the remote client/device 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.Select the authentication type.
[ppp challenge-interval *<0-255>*] |	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 re-challenges 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. The default value is 0 (zero), meaning CHAP re-challenge is disabled.
[ppp cr-retry *<0-255>*] |	The maximum number of times a configure request packet will be re-sent before the link is terminated. cr-timeout.
[ppp cr-timeout *<1-255>*] |	The maximum time, in seconds, that LCP (Link Control Protocol) will wait before it considers a configure request packet to have been lost.
[ppp dynamic-dns on | off] |	Enable or disable dynamic DNS.
[ppp hostname] |	Specify the host name that will be updated with the PPP session's IP address on the DynDNS.org server.
[ppp password] |	Specify the password used to access the DynDNS.org server.
[ppp username *<WORD>*] |	Specify the user name used to access the DynDNS.org server.
[echo-retry *<0-255>*] |	The maximum number of times an echo request packet will be re-sent before the link is terminated. Range: 0-255 Default: 30 seconds.
[echo-timeout *<0-255>*] |	The maximum time, in seconds, between sending an echo request packet if no response is received from the remote host. Range: 0-255 Default: 30 seconds
[ipaddr-neg on | off] |	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. The default value is Off. When On, the IP address specified by the remote end will be used in preference to the Remote IP Address set for a Line. When Off, the Remote IP Address set for the Line will be used.

[ipv6-global-network-prefix *<WORD>*] |	You can optionally specify an IPv6 global network prefix that the IOLAN will advertise to the device at the other end of the PPP link. Enter the IPv6 network prefix in the aaaa:bbbb:cccc:dddd:: format.
[ipv6-local-interface *<WORD >*] |	The local IPv6 interface identifier 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. Do not use the IOLAN's (main) IP address in this field; if you do so, routing will not take place correctly. The first 64 bits of the Interface Identifier must be zero, therefore, ::abcd:abcd:abcd:abcd is the expected format.
[pv6-remote interface *<WORD>*] |	The remote IPv6 interface identifier 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-Interface-ID is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here. The first 64 bits of the Interface Identifier must be zero, therefore, ::abcd:abcd:abcd:abcd is the expected format.
[lipaddr *<A.B.C.D>*] |	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.
[magic-neg on | off] |	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. The default is Off.

[ppp mru *<64-1500>*] |	The Maximum Receive Unit (MRU) parameter specifies the maximum size of PPP packets that the IOLAN’s port will accept. Enter a value between 64 and 1500 bytes; for example, 512. The default value is 1500. If your user is authenticated by the IOLAN, the MRU value will be overridden if 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.
[ppp ms-direct guest | host] |	Select guest or host for ms-direct.
[ppp nak-retry *<0-255>*] |	The maximum number of times a configure NAK packet will be re-sent before the link is terminated.
[ppp netmask *<A.B.C.D>*] |	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.
[ppp password *<WORD>*] |	This field defines the password which is associated with the user defined by the user parameter. It is used to authenticate a user connecting to the IOLAN. You can enter a maximum of 16 alphanumeric characters.
[ppp proto-comp off | on] |	This determines whether compression of the PPP Protocol field takes place on this link. The default is On.
[ppp lipaddr *<A.B.C.D>*] |	The IPV4 IP 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 255.255.255.254; this value allows the IOLAN to use the remote IP address value configured here.

[ppp roaming-callback off | on] |	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 Callback parameter is set to On. Roaming callback therefore overrides (fixed) User Callback.To use 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. The default is Off.
[ppp routing listen | none | send |send-and-listen] |	Determines the routing mode (RIP, Routing Information Protocol) used on the PPP interface as one of the following options: ● None—Disables RIP over the PPP interface. ● Send—Sends RIP over the PPP interface. ● Listen—Listens for RIP over the PPP interface. ● Send and Listen—Sends RIP and listens for RIP over the PPP interface. This is the same function as the Framed-Routing attribute for RADIUS authenticated users. Default is None
[ppp rpassword <*WORD*>] |	The rpassword is the password which is associated with the user defined by ruser. It is used to authenticate a user connecting to the IOLAN. You can enter a maximum of 16 alphanumeric characters.
[ppp ruser <*WORD*>] |	This field is used to authenticate a user connecting to this line. It is used in conjunction with the rpassword field. By specifying a name here, this line becomes dedicated to that user only. If left blank, the internal user database will be used to authenticate the connection and any user configured will be able to access this line. You can enter a maximum of 254 alphanumeric characters. This option does not work with external authentication
[ppp tr-retry <*0-255*>] |	The maximum number of times a terminate request packet will be re-sent before the link is terminated.
[ppp tr-timeout <*1-255*>] |	The maximum time, in seconds, that LCP (Link Control Protocol) will wait before it considers a terminate request packet to have been lost.
[ppp user <*WORD*>] |	This field is used by a remote peer to authenticate a PPP connection on this line. It is used in conjunction with the password field. You can enter a maximum of 254 alphanumeric characters.

[ppp vj-comp on | off] |	This determines whether Van Jacobson Compression is used on this link. The default is On. If your user is authenticated by the IOLAN, this VJ compression value will be overridden if you have set the User Framed Compression On. If your user is authenticated by RADIUS and the RADIUS parameter Framed-Compression is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.
[reset off | on] |	When enabled, resets the terminal definition connected to the serial port when a user logs out. Default is Disabled
[rev-session-security off | on] |	Configure reverse telnet session authentication.
[rlogin-client termtype *<WORD>*] |	Configure the terminal type for rlogin sessions.
[rts-toggle off | on] |	Configure RTS toggle. Default is Off
[rts-toggle-final-delay *<0-1000>*] |	Configure RTS final delay in milliseconds. Value is 1–1000
rts-toggle-inital-delay *<0-1000>*] |	Configure RTS initial delay in milliseconds. Value is 1–1000
[send-name off | on] |	Configure the port name to be sent to the host when session is initiated. This is done before any other data is sent or received to/from the host. Default is Disabled
[send-port-id off | on] |	Configure port-id to send.
[service bidir *<A.B.C.D> <1-65535> <1-65535>*] |	Configure service type for bidir. Use bidir for TCP Sockets, Reverse and Silent connections. Configure the host to connect to, server port number and host port number.
[service client-tunnel *<A.B.C.D> <1-65535>*] |	Configure service type to client-tunnel. Configure the Enter the host to connect to and host port number.
[service direct raw *<A.B.C.D>* | rlogin *<A.B.C.D>* | ssh *<1-65535>* | telnet *<A.B.C.D> <1-65535>*] |	Configure service type as direct raw.
[service dslogin] |	Connects to the serial port in Command Line Interface (CLI) mode on this port.
[ervice modbus-master] |	Configure service type as modbus master.

[service modbus-slave] |	Configure service type as modbus slave.
[service ppp] |	Configure service type as PPP for this serial port.
[service printer] |	Configure service type as printer.
[service reverse raw [multihost on | off | tcp-port *<1-65535>* | multihost] | ssh *<1-65535>* | telnet *<1-65535>*] |	Configure parameters for a reverse raw connection.
[service server-tunnel *<1-65535>*] |	Configure service to server tunnel connection.
[service silent raw *<1-65535>* | multihost all | backup *<A.B.C.D> <1-65535> <1-65535>* | none] |	Configure service type as silent raw parameters. **Multihost**–used for connections coming from the network to the serial port for Trueport or Raw. Multihost all allows multiple hosts to connect to the serial port. **Backup**–Multihost in primary backup mode.
[service slip] |	Configure service type as slip.
[service trueport client-initiated off *<A.B.C.D> <X:X:X:X::X <1-65535>* | on *<1-65535>* multihost off | on | signal-active on | off] |	Configure service type as trueport.
[service udp *<1-65535>*] |	Configure service type as udp.
[service vmodem *<1-65535>*] |	Configure service type as modem.
[sess-timer *<0-4294967>*] |	Configure session timer to forcibly close the session/ connection when the Session Timeout expires. Default is 0 seconds so that the port never timeouts. Range is 0 to 294967 seconds (about 49 days)
[session-strings delay *<0-65535>*] |	Configure session string delay options. **Delay after Send**—If configured, a delay time is sent to the device. This delay is used to provide the serial device time to process the string before the session is initiated.

[session-strings initiate *<WORD>*] |	**Initiate at Start**—If configured, this string is sent to the serial device on the power-up of the IOLAN or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set, the string is also sent when the monitored signal is raised. **Range is** 0–127 alpha-numeric characters. Non printable ascii characters must be entered in this format <027>. The decimal numbers within the brackets must be 3 digits long (example 003 not 3).
[terminate *<WORD>*] |	**Send at Terminate**—If configured, this string is sent to the serial device when the TCP session on the LAN is terminated. If multi-host is configured, this string is only sent in listen mode to the serial device when all multi-host connections are terminated. **Range is** 0–127 alpha-numeric characters. Non printable ascii characters must be entered in this format <027>. The decimal numbers within the brackets must be 3 digits long (example 003 not 3)
[slip lipaddr | mtu *<WORD>* | |*<A.B.C.D>* | netmask *<A.B.C.D>* | ripaddr *<A.B.C.D>* | routing listen | none | send | send-and-listen | vj-comp on | off] |	The IPv4 address of the IOLAN end of the SLIP link. For routing to work you must enter an IP address in this field. 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
[slip mtu *<WORD>*] |	The Maximum Transmission Unit (MTU) parameter restricts the size of individual SLIP packets being sent by the IOLAN. Enter a value between 256 and 1500. 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.
[slip netmask *<A.B.C.D>*] |	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.SLIP netmask.

slip [ripaddr *<A.B.C.D>]* |	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.
[slip routing listen | none | send | send-and-listen] |	Determines the routing mode (RIP, Routing Information Protocol) used on the SLIP interface as one of the following options: • None—Disables RIP over the SLIP interface. • Send—Sends RIP over the SLIP interface. • Listen—Listens for RIP over the SLIP interface. • Send and Listen—Sends RIP and listens for RIP over the SLIP interface. This is the same function as the Framed-Routing attribute for RADIUS authenticated users. Default is None.
[slip vj-comp on | off] |	This determines whether Van Jacobson compression is used on this link; that is, whether you are using SLIP or C-SLIP (compressed SLIP). The choices are On (C-SLIP) or Off (SLIP). The default is On. C-SLIP greatly improves the performance of interactive traffic, such as Telnet or Rlogin. If your user is authenticated by the IOLAN, this VJ compression value will be overridden if you have set a Framed Compression value for a user. If your user is authenticated by RADIUS and the RADIUS parameter Framed-Compression is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.
[speed 115200 | 1200 | 1800 | 19200 | 230400 | 2400 | 28800 | 300 | 38400 | 4800 | 57600 | 600 | 9600] |	Configure the speed for this interface. • 115200, 1200, 1800, 19200, 230400,2400, 28800, 300, 38400, 4800, 57600, 600, 9600
[ssh-client authentication [dsa on | off] |	An authentication method used by SSH version 2. When enabled, an SSH client session will try to authenticate via DSA.
[ssh keyboard-interactive on | off] |	The user types in a password for authentication.Used for SSH2 only.

[ssh rsa on | off] |	An authentication method used by SSH version 1 and 2. When enabled, an SSH client session will try to authenticate via RSA. authentication.
[ssh compression on | off] |	Requests compression of all data. Compression is desirable on modem lines and other slow connections, but will only slow down things on fast networks. protocol.
[ssh login on | off] |	Enable or disable auto login.
[ssh name <*WORD*>] |	The name of the user logging into the SSH session
[ssh password <*WORD*>] |	The password for the user logging into the SSH session.
[ssh-2-cipher-list 3des | aes-cbc | aes-ctr | aes-gcm | | chacha20-poly1305 | rijndael-cbc] |	Select the order pf negotiation for the encryption methods (ciphers) that the IOLAN will use for SSH V2 connections.
[ssh strict-host-key-checking on | off] |	Enable or disable strict host checking.
[ssh termtype <word>] |	The type of terminal attached to this line.
ssh [verbose on | off] |	Enable or disable debug messages on the terminal.
[ssl [cipher-suite | enable | type | validation-criterial | verify-peer | version] |	Enables or disables SSL
[ssl enable on | off] |	Enables or disables SSL
[ssl type client | server] |	Select mode for SSL ● client ● server
[ssl verify-peer off | on] |	Configure for peer validation.
[ssl version any suite-b-tls | tlsv1.2 | tlsv3 | use-global] |	Configure TLSV version.
[stop-bits 1 | 2] |	Configure the stop bits. ● 1 ● 2
[telnet-client escape <*0-0x7f*>] |	**escape**—Defines the escape character. Returns you to the command line mode. This value is hexadecimal. Default is 1d (ASCII value GS)

[telnet-client echo *<0-0x7f>*] |	**echo**—toggles between local echo of entered characters and suppressing local echo. Local echo is used for normal processing, while suppressing the echo is convenient for entering text that should not be displayed on the screen, such as passwords. This parameter can be used only when Enable Line mode is enabled. Default is Disabled
[telnet-client eof *<0-0x7f>*] |	**eof**—Defines the end-of-file character. When enabled Line mode is enabled, entering the EOF character as the first character on a line sends the character to the remote host. This value is in hexadecimal. Default is 4 (ASCII value ^D) This parameter can be used only when Enable Line mode is enabled. Default is Disabled
[telnet-client erase *<0-0x7f>*] |	**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)
[telnet-client intr *<0-0x7f>*] |	Define the interrupt character. Typing the interrupt character interrupts the current process. This value is in hexadecimal with a default value of 1c) AASCII value FS).
[telnet-client line-mode off | on] |	**line mode**—When enabled, keyboard input is not sent to the remote host until Enter is pressed, otherwise input is sent every time a key is pressed. Default is Disabled
[telnet-client local-echo off | on] |	**local echo**—Toggles between local echo of entered character and suppressing local echo Local echo is used for normal processing, while suppressing the echo is convenient for entering text that should not be display on the screen such as passwords. This parameter can only be used when Enable Line Mode is enabled. Default is Disabled
[telnet-client map-cr-crlf on | off |	**map cr to crlf**—When enabled, maps carriage return (CR) to carriage return/line feed (CR/LF). Default is Disabled
[telnet-client quit *<0-0x7f>*] |	**quit**—defines the quit character. Typing the quit character closes and exits the current telnet session. This value is in hexadecimal. Default is 1c (ASCII value FS)

[telnet-client termtype ansi | dumb | hp700 | ibm3151te | term1 | term2 | term3 | tvi925 | vt100 | vt320 | wyse60] |	Configure a terminal type. Values are: ansi, dumb, hp700, ibm3151te, tvi925, vt100, vt320, wyse60
[udp entry <*1-4*>] |	Configure a udp entry— For each entry you specify a different IP address range, udp port, and the direction of data flow. **both | in | out | none** The direction in which information is received or relayed: **both**—both directions **in**—LAN to serial. The IOLAN listens on the port value configured in the DS Port parameter for messages coming from the learned or configured port. **out**—Serial to LAN. The IOLAN forwards data received on the serial port to the IP address range, UDP port configured for this entry. **none**—UDP service not enabled.
[udp auto-learn <*A.B.C.D*> | <*X:X:X:X::X*> | specfic <*1-65535*> | any-port] |	**auto-learn**—The IOLAN only listens to the first port that it receives a UDP packet from. Auto learn is applicable when direction is set to In or Both. **specific**—The port that the IOLAN listens for UDP packets, configured using the DS port parameter. **any-port**—The IOLAN receives messages from any port sending UDP packets Applicable when direction is set to In.
[upd <*A.B.C.D*>] | <*X:X:X:X::X*>] |	The first host IP address in the range of IP addresses (for IPV4 or IPV6) that the IOLAN will listen for messages from and/or send messages to.
[udp <*A.B.C.D*> | <*X:X:X:X::X*>] |	The last host IP address in the range of IP addresses (for IPV4, not required for IPV6) that the IOLAN will listen for messages from and/or send messages to.
[udp suppress off | on]}	When enabled, the connection success/failure indication strings are sent to the connected device, otherwise, these indications are suppressed. The default is Disabled
[user <*WORD*>] |	Line dedicated to specific user.
[vmodem echo off | on] |	Configure echoes to have the terminal echo back typed characters. (equivalent to ATE0/ATE1 commands). Disabled by default

[vmodem [failure-string *<WORD>*] |	Configure the string sent to the serial device when a connection fails. If no string is entered, the string NO CARRIER is sent.
[vmodem [host *<A.B.C.D>* | *<X:X:X:X::X>*] |	Configure the target host name.
[vmodem[init-string *<WORD>*] |	Configure additional vmodem commands that affects how vmodem starts. The following commands are supported: ATQn, ATVn, ATEn, ATS0, AT&Z1, AT&Sn, AT&Rn, AT&Cn, AT&F, ATS2, ATS12, and ATDS1.
[vmodem [mode [auto | manual] |	Configure auto mode to establish the connection when the line becomes active. You must supply the AT command or phone number to start the connection.
[vmodem [port *<1-65535>*] |	Configure the port number the target host is listening on for messages.
[vmodem response-delay *<1-999>*] |	The amount of time, in milliseconds, before an AT response is sent to the requesting device. The default is 250 ms.
[vmodem style numeric | verbose] |	One of the following: • **Verbose**—Return codes (strings) are sent to the connected device. • **Numeric**—The following characters are sent to the connected device: • **0** OK • **1** CONNECTED • **2** RING • **3** NO CARRIER • **4** ERROR • **6** INTERFACE DOWN • **7** CONNECTION REFUSED • **8** NO LISTENER See *VModem Initialization Commands* in the *’s SCR User’s Guide* for a more detailed explanation of the supported initialization commands.
[vmodem success-string *<WORD>*] |	String that is sent to the serial device when a connection succeeds. If no string is entered, then the string CONNECT is sent with the connecting speed. For example CONNECT 9600
Command Modes	Perle(config-line)#

Usage Guidelines

Use this command to configure line tty parameters.

Examples

This example disables CLI mode for tty.

```
Perle(config)#tty  mode disable
```

Related Commands

(config-line)#console

(config-line)#tty and #usb

(config-line)#vty

Use the no form of this command to negate a command or set to defaults.

Syntax Description	**(config-line)#vty**
[accounting exec <*WORD*> | default] |	Configure accounting parameters.
[authorization exec <*WORD*> | default] |	Configure authorization parameters.
[exec-timeout <*0-35791*> <*0-2147483*>] |	Configure the time in minutes and seconds for CLI to timeout on the vty session.
[history size <*0-256*>] |	Configure the size of the history buffer.
[length <*0-512*>] |	Configure the number of lines displayed on the screen. Type 0 for no pausing at end of page.
]login <*WORD*> default] |	Configure login authentication parameters.
[width <*0-512*>]}	Configure terminal screen width.
Command Modes	Perle>enable Perle>config Perle(config)#line vty Perle(config-line)#

Usage Guidelines

Configure vty line parameters.

Examples

Configure the terminal width to 132.

```
Perleconfig)#line vty
Perle(config-line)#width 132
```

Related Commands

(config-line)#tty and #usb

(config-line)#console