IDS Managed PoE Switches

User Guide

Updated: February 2021
Revision: A.5
Document Part: 5500392-10

Table of contents

Table of contents

1 - Overview

Audience

This guide is for the networking professional managing your switch. Before using this guide, you should be familiar with the concepts and terminology of Ethernet and local area networking.

Purpose

This guide provides the information that you need to configure and manage your Perle IDS Managed Switch.

For Web Manager (GUI) users, this guide provides the navigation reference that can be used within web sessions for each feature. As an additional reference, the applicable CLI (Command Line Interface) command for users who prefer working with CLI is provided.

Detailed information on specific CLI commands can be found in the Perle IDS Command Reference Guide available for download from the Perle web site (www.perle.com).

Guide Updates

This guide may be updated from time to time and is available at no charge from the download area of Perle's web site at https://www.perle.com/downloads/

Copyright Statement

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

Perle reserves the right to make changes without further notice, to any products to improve reliability, function, or design.

1.1 - Features

Perle IDS Switches meet the needs of **enterprise-grade industrial environments** where additional security and network integration functionality is required.

Performance Features	Description
Port Auto-sensing	Auto-sensing of port speed and auto-negotiation of duplex on all switch ports for optimizing bandwidth
Auto MDI/MDIX	Medium-dependent interface crossover (Auto-MDIX) capability on 10/100 and 10/100/1000 mbps interfaces that enables the interface to automatically detect the required cable type (straight thru or crossover) and to configure the connection appropriately
802.3x flow control	IEEE 802.3x flow control on all ports.
Link Aggregation protocol	Increase port bandwidth through link aggregation. Support is provided for IEEE 802.3ad using Link Aggregation Control Protocol (LACP). Up to eight (8) ports in a single port-channel.
Static Link Aggregation	Provides the ability to operate under a static (manual) link aggregation scenario (where the remote switch peer does not support LACP)
Storm Control	Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Storm Control enables limits to be placed on broadcast, multicast and unicast traffic
Bandwidth Control Monitoring	Bandwidth Control provides the ability to monitor the flow rates on a per port basis and the ability to cause an SNMP trap to occur (selectable) and put the port in an "error-disabled" state
Static MAC Addressing	This feature enables the manual configuration of the MAC addresses on a per port basis. Flooding is prevented by retaining MAC entries across a reboot of the switch.
Port Blocking	Port Blocking provides the ability to block the flooding of unknown layer 2 unicast and multicast traffic on an Interface
IPV4 IGMP Snooping	Internet Group Management Protocol (IGMP) constrains the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. IGMPv1, v2, v3, IGMP snooping querier mode, IGMP report suppression, topology change notification and robustness variable features are supported
IPV6 MLD Snooping	With Multicast Listener Discovery (MLD) snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

GMRP	GARP Multicast Registration Protocol (GMRP) provides a constrained multicast flooding facility similar to IGMP snooping. GMRP provides a mechanism that allows bridges and end stations to dynamically register group membership information with the MAC bridges attached to the same LAN segment and for that information to be disseminated across all bridges in the Bridged LAN that supports extended filtering services.
Quick Port Disconnect	In some network environments, it is desirable to move an Ethernet from one switch port to another and have the device come on-line quickly. The Quick Port Disconnect feature if enabled, provides an immediate age-out of the MAC addresses learned on the port when the port status changes from a link-up to a link-down state
Manageability Features	
Web Device Manager	The Perle Web Device Manager is an embedded Web based application that provides an easy to use browser interface for managing the switch. Operates with both http and secure https streams. Unlike some competitive products, Java applet technology is not required or used
Command Line Interface (CLI)	A familiar text-based Command Line Interface that is based on accepted industry standard syntax and structure. Ideal for CCNA and CCNP trained engineers, this interface is available via in-band Telnet/SSH or the out-band serial console port
SNMP	Manage the switch with an SNMP-compatible management platform such as HP Openview or Perle's PerleVIEW NMS. SNMP V1, V2C and V3 are supported.
PerleVIEW	PerleVIEW is Perle's SNMP-based central network management system that provides a view of the Perle device network for large scale deployments.
IPv6	Manage with an IPv4 or IPV6 address
DHCP Client Auto-Configuration	Automates configuration of switch information such as IP address, default gateway, hostname and Domain Name System (DNS) as well as TFTP server names. Firmware and configuration file locations are provided through options 54, 66, 67, 125 and 150
DHCP Relay	DHCP Relay is used for forwarding requests from DHCP clients when they are not on the same physical subnet. As a DHCP relay agent the switch operates as a Layer 3 device that forwards DHCP packets between clients and servers.
DHCP Option 82 Insertion	Normally used in metro or large enterprise deployments DHCP Option 82 insertion is used to provide additional information on "physical attachment" of the client. As per RFC 3046, option 82 enables additional pre-defined information to be inserted into the DHCP request packet (for DHCP Servers that support this option)
DHCP Server	For networks where a central DHCP server is not provided, the switch can provide a DHCP Server function for allocation of IP addresses to the connected devices

DHCP server port-based address allocation	When Ethernet switches are deployed in the network, they offer connectivity to the directly connected devices. In some environments, such as on a factory floor, if a device fails, the replacement device must be working immediately in the existing network. When configured, the DHCP server port-based address allocation feature ensures that the same IP address is always offered to the same connected port even as the client identifier or client hardware address changes in the DHCP messages received on that port.
LLDP	LLDP-Link Layer Discovery Protocol as per IEEE 802.1AB is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other (via TLVs – Type-Length-Value)
LLDP-MED	LLDP Media Endpoint Discovery is an extension to LLDP that operates between endpoint devices such as IP phones and network devices such as switches. It specifically provides support for voice over IP (VoIP) applications and provides additional TLVs for capabilities discovery, network policy, Power over Ethernet, inventory management and location information.
NTP	The switch can provide the time to NTP/SNTP capable client devices (or other switches, etc). You can run the SNTP client and the NTP server concurrently on your system. Therefore you can obtain time from an outside source and serve that time to the devices connected to the switch.
IEEE 1588 – PTP (Precision Time Protocol)	IEEE 1588 V1 and V2 Boundary Clock V1 Boundary Clock V2 End-to-End Transparent Clock Sync Two Step Operation End-to-End Transparent Clock Sync One Step Operation Peer-to-Peer Transparent Clock End-to-end Boundary clock Peer-to-peer boundary clock Microsecond accuracy
File Download	Firmware can be transferred via TFTP, SCP, HTTP, HTTPS, or via insertion of a microSD card (model dependent). Text-based files that can be created or edited by common text editors.
Secure Copy Protocol (SCP)	SCP based on the Secure Shell (SSH) protocol, is a means of securely transferring computer files between a local host and a remote host or between two remote hosts.
Availability and Redundancy Features	
Spanning Tree Protocol (STP)	IEEE 802.1D now incorporated in IEEE 802.1Q-2014, STP prevents bridge loops and the broadcast radiation that results from them. Other Spanning Tree features include BPDU guard, Root guard, loop guard, root guard and TCN Guard.

Rapid Spanning Tree Protocol (RSTP)	Interoperable with STP, RSTP (IEEE 802.1w) takes advantage of point-to-point wiring and provides rapid convergence of the spanning tree. Reconfiguration of the spanning tree can occur in less than 1 second
Multiple Spanning Tree Protocol (MSTP)	Originally defined in IEEE 802.1s and now incorporated IEEE 802.1Q-2014, defines an extension to RSTP for use with VLANs. The Multiple Spanning Tree Protocol configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.
P-Ring	Perle’s Ring Protocol provides resilient operation of a network made up of managed switches in a ring topology. The implementation prevents a switch loop scenario and also enables communication within the ring if a failure occurs somewhere in the ring.
MRP-Ring	MRP (Media Redundancy Protocol) is defined in International Electrotechnical Commission (IEC) standard 62439-2. It provides fast convergence in a ring network topology. MRP provides recovery times for a ring in the following range: 10, 30, 200 and 500 ms
Link Standby	A link recovery feature using a primary and backup link. Provides a simple alternative to spanning tree protocols for link redundancy.
VLAN Features	
VLAN Range	Up to 255 VLANS across a VLAN ID range of 1 to 4094
GVRP	Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) is an application defined in the IEEE 802.1Q standard that allows for the control of VLANs. With GVRP, the switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches that are connected through 802.1Q trunk ports.
Voice VLANs	Voice VLANs enables one to separate, prioritize, and authenticate voice traffic moving through your network, and to avoid the possibility of broadcast storms affecting VoIP (Voice-over-IP) operation. With an IP Phone connected to an access port, a switchport voice VLAN enables the use of one VLAN for voice traffic and another VLAN for data traffic from an Ethernet device attached to the phone.
VLAN Interfaces	Perle switches provide the ability to configure management VLAN interfaces. This enables network administrators to access the switch’s management interface from separate VLAN networks
Security Features	

IEEE 802.1X	Provides secure access to switch ports from a central RADIUS server. The switch operating as an authenticator interacting with an 802.1X compliant supplicant (PC or industrial device) through the use of the EAPOL protocol. Authentication will be granted/denied through an external RADIUS server. RADIUS assigned VLAN IETF 64 (Tunnel Type) IETF 65 (Tunnel Medium Type) IETF 81 (Tunnel Private Group ID) Guest VLAN and Restricted VLANs are supported For non-802.1X devices found in industrial applications, the switch can use the client MAC address for authorization through the use if MAB (MAC Authentication Bypass) Switch can also be configured as an 802.1X supplicant (edge switch) that authenticates with an 802.1x-aware upstream switch.
Login Banner and MOTD	A login message banner presented during sign-on can be configured by the network administrator. A Message Of The Day can also be created for presentation to an authenticated user.
Password Strength Checking	Many organizations require stringent management over the strength level of their passwords. When enabled, Perle extends this capability to local passwords stored on the switch enforcing strong passwords to be used.
Port Security – Secure MAC Addresses	This port security feature provides the ability to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port (Access or Trunk) and will take specific actions when violations occur.
Management ACL	Restricting access to management functions can be configured by protocol or IP address selection are provided. This enables administrators to allow only specific workstations using particular protocols to be able to access the management functions of the switch.
RADIUS Management Access Authentication	AAA support for RADIUS servers that Authenticate, Authorize and Account management sessions.
TACACS+ Management Access Authentication	AAA support for TACACS+ servers that Authenticate, Authorize and Account management sessions.
Secure Socket Layer (SSL)	SSL provided for secure browser sessions using HTTPS
Secure Shell (SSH)	SSH provided for secure SSH session for CLI and SCP file transfer sessions.
SNMPV3	Support provided for secure version 3 of SNMP
Quality of Service (QoS) and Class of Service (CoS) Features	
Classification	IP ToS/DSCP and IEEE 802.1p CoS
Congestion Avoidance	Weighted Fair Queuing or Strict Queuing

Egress Queues and scheduling	4 traffic class queues per port output queue mapping DSCP to output queue mapping
Monitoring Features	
Port Mirroring	N:1 Port Mirroring is a method of monitoring network traffic. With port mirroring enabled, the switch sends a copy of one or more ports to a predefined destination port. Selection of Transmit, Receive frames or both can be made
RMON	RMON statistics provided for statistics, history, alarms and events for network monitoring and traffic analysis
Syslog	Facility for logging systems messages to an external SYSLOG server
Alert Log	Facility for logging systems messages locally
Traceroute	Layer 2 traceroute to identify the path that a frame takes from source to destination
Virtual cable test	A test that enables the detection of potential copper cabling issues such as pair polarity pair swaps and excessive pair skew as well as any opens, shorts or any impedance mismatch. Will report the distance in the cable to the open or short.
Power Supply Monitoring	Provides the status of power supplies of the switch
Internal Temperature Monitoring	The internal ambient temperature of the switch can be obtained from the management interfaces.
Alarm Processing	The switch can monitor global switch conditions as well as individual ports. These alarms can be configured to send messages to ; an internal log file external Syslog server SNMP trap server An external alarm device such as a bell, light or other signaling device via the switch’s built-in dry contact alarm relay Global Status Monitoring Alarms Dual power supply alarm Port Status Monitoring Alarms Link Fault Alarm (IE loss of signal) Port not forwarding alarm Port not operating alarm (failure upon start up tests) FCS Bit error rate alarm
Alarm Relay	When enabled, energizes the built-alarm relay triggering an external alarm circuit such as a bell, light or other signaling device according to alarm conditions set

1.2 - Software

Licensing

All Perle software pre-installed in Perle Products or downloaded from any other source or media is governed by Perle's End User License Agreement. USING THIS PERLE PRODUCT CONSTITUTES ACCEPTANCE OF THIS AGREEMENT. Please review the country specific End User License Agreement located at the following location prior to usage;

http://www.perle.com/EULA.shtml

http://www.perle.com/EULA-Germany.shtml

You also agree that Perle may collect, use, or disclose customer information in the course of fulfilling its obligations under the End User License Agreement, and such collection, use, and disclosure will be in accordance with Perle's privacy policy available at http://www.perle.com/privacy.shtml

IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, You have no right to use the Perle Software and You should return the purchased product to Perle or the applicable reseller or distributor from whom You obtained the product.

Universal Image

Perle IDS ethernet switch products share the same firmware image. Specific functions and features are enabled depending on the model purchased. The benefit of this type of approach is that models can share a single firmware file that may be loaded onto a central file server (IE TFTP). This greatly simplifies updates for the user when multiple Perle IDS model types exist in the same network.

1.3 - Configuring

Configuration

The Perle Industrial Ethernet Managed Switches (IDS) support the following methods of configuration:

- Fast Setup - Available when the IDS is in factory default configuration
- Device Web Manager - Accessible from a Web Browser
- CLI - Command Line Interface
- SNMP - Using a Network Management System

The switch is delivered with a factory default configuration.

To obtain a list of all default values for various features (in factory default mode), connect to the serial console and perform a **"#show running-config all"** CLI command.

Fast Setup

Fast Setup is used as a simple method for configuring the unit for first time installation. Used in Factory Default Configuration Mode, it provides the simplest network setup.

Fast Setup via Internet Browser in factory default mode
Fast Setup mode simply requires a PC Ethernet connection and browser software. Other methods to configure the IDS Switch can be found in the IDS Switch User's guide.

1. Your PC must be set to obtain a DHCP address from the IDS switch (For Windows users, see Control Panel ->Network and Sharing Center -> Change adapter settings ->Local Area Connection Properties ->Internet Protocol Version (TCP/IPv4) ->Properties ->Select Obtain an IP address automatically.

2. To initiate Fast Setup mode, press and hold the "Reset/FS" button located near the bottom of the unit for 4 seconds. Both LEDs on one of the empty Ethernet RJ-45 connectors will rapidly flash to direct you to plug in the Ethernet cable from your PC's Ethernet port to this port. If there are no empty RJ-45 ports on the IDS switch then you will need to make one available.

3. The IDS switch will assign an IP address of 169.254.0.1 to itself and it will assign your PC an address of 169.254.0.2

4. Launch your favorite Internet browser and select any url or simply type in 169.254.0.1 to be directed to the IDS Switch Get Started screen. Select the Get Started button to be directed to the configuration screen.

5. Configure the necessary parameters for your network ;

- **System Name**: Enter the name of the switch. Spaces are not allowed.
- **Settings for VLAN1**: Enter a static VLAN interface IP address or select that a DHCP server will assign.
    - If required, enter the optional default gateway address. This enables any switch management application to be able to communicate to a device on another network via this gateway router. The gateway address will also be reachable from any VLAN on the switch.
- **Administration**: Set an Administrative password for the CLI (Privileged EXEC), create an Administrative User ID for the Web Manager and CLI, create a community to manage the switch using SNMP and set the date and time.

press the Apply button to save and exit Fast Setup.

Fast Setup via CLI in factory default mode
As alternative to using an Internet browser, Fast Setup can also be performed via the CLI interface on the switch serial console. This is done by hitting "return" after the switch has completed booting.

Fast Setup via Internet Browser after initial configuration
A Fast Setup page is provided in the switch web manager to view or change the basic switch parameters that were entered by the user during the initial Fast Setup interview process

CLI

A familiar text-based Command Line Interface based on accepted industry standard syntax and structure is provided. This interface which is ideal for network industry certified engineers, is available via in-band IE Telnet/SSH sessions or the out-band serial console port.

The CLI is structured as follows:

- User EXEC mode
- Privilege EXEC mode
- Global Configuration mode
- Interface Configuration mode
- VLAN configuration mode
- Line configuration mode

For detailed information on the CLI, please refer to the Perle IDS Command Reference Guide available for download from the Perle web site (www.perle.com)

Web Manager

The Perle Web Device Manager is an embedded Web based application that provides an easy to use browser interface for managing the switch.

Navigation Tree

On the left side of all pages resides a structured navigation tree grouped by the following areas;

- Dashboard
- Configure
- Monitor (displayed in green text)
- Administration
- Diagnostic Tools
- Fast Setup
- Command line

This navigation tree can be expanded or collapsed as required. A navigation tree search is also provided to assist in directing the user to the pages that most relate to the search term entered.

Search Navigation

A search tool is provided on the top of the navigation tree to assist user looking for a specific term in the navigation tree. As you begin typing your search term, the navigation tree will filter accordingly until the search you are looking for appears.

Alarms

In the top right quadrant, the total number of alarms that require attention are displayed.

Device Status

A graphical representation of the IDS switch is on the right hand side of the browser window. This device Status window can also be minimized to maximize the size of the middle window if required.

The following elements of the graphic are active and presents their status. Clicking on a port will direct the user to the port monitoring page for a detailed view.

Ethernet RJ/Fiber ports

- A green port color represents a port with an active link. The LED portions, like the real hardware indicate the negotiated speed.
- A black port color represents an enabled port but with no link. This would occur if no device is actively connected.
- A grey shaded port represents a port that has been manually disabled by the administrator.
- A red port color represents a port that has been placed in an error-disabled state by the switch software due to a user pre-defined error condition.
- Activity LEDs will not display as blinking.

Console port

- When a serial device is connected to a console port, a green color on the RJ port is presented indicating that the console port is active. When not present, the port color is black.

Hardware switches

- If hardware switches exist, the direction of the DIP switches are correctly represented. *Refer to the IDS Hardware Installation Guide for details*.

Status LEDs

- The status of all LEDs at the top of the unit are correctly represented. Whenever a LED is blinking, the LED will be represented as a glowing "star" shape.

SD card

- For those models with SD card slots, a black colored slot indicates that an SD card is not present. A green colored slot indicates that an SD card is present.

Unit Configuration

When using the web Manager, details displayed reflect what is contained in the switch's running-config. When changes are made using the web manager, the operation that is performed during an "Apply" is that the change is automatically applied to the Running-config which is then saved in its entirety to the Startup-config file.

This means that when using both web manager and CLI at the same time, some caution is required. Changes made via the CLI are immediately updated to the running-config. Therefore any changes that are subsequently made by the web manager (and "applied") will incorporate all changes previously made via CLI and automatically saved to the startup-config .

To show the state of the synchronization between running-config and startup-config can be found through the web manager under Monitor/System/General Information or under CLI with #show sysinfo

Startup-Configuration state................... In Sync with Running-configuration

Web User Privilege

Authenticated users using the Web Manager operate at the admin (Privileged EXEC) level.

Secure Web Manager

Overview

The Perle Web Manager is an embedded Web based application that provides an easy to use browser interface for managing the switch. Some IDS managed switch models have the capability of running the web manager using secure HTTPS protocol utilizing up-to-date TLS 1.2 or better encryption cipher suites

Operation of the web manager running in a secure environment is the same as described in “Web Manager”

Key and certificate management is found in “Keys and Certificates”

Pre-requisites

- IDS Switch and a browser

Restrictions / Limitations

- None

Terminology

- None

Feature details / Application notes

When using the secure web manager, the switch's IP address must be preceded by "*https://*"

The HTTPS port number can also be modified from the standard default of 443. See below

Configuration
Change HTTP port number

Activity	Web Manager	CLI Command(s)	Comments
Change HTTPS port number	Configure/System/System General Settings	(config)#ip http secure-port	If required, change the standard HTTPS port number from 443 to a different value (1024 to 65535)

Monitoring and Maintaining

- None

2 - Basic Operation

Digital Inputs

Overview

- There are two basic types of digital inputs (dry contact sensing and wet contact sensing). These can be used for the generation of alarms (SNMP trap, energizing of on-board Alarm Relay, etc).
  - One example is the monitoring of a dry contact closure on the equipment enclosure door. Alarms can be generated when the door is sensed open and/or closed.

Pre-requisites

- Availability of Digital Inputs is model Dependant.
- Please see the IDS Hardware Installation Guide for your specific model to determine which digital inputs are available on your switch.

Restrictions / Limitations

- None

Terminology

- Dry contact sensors: using this type of sensor, the switch applies a small amount of voltage across the contacts and senses when the circuit is completed . IE door contact closure completing the circuit
- Wet contact sensors: using this type of circuit, the switch senses the presence of current flowing across the contacts

Feature details / Application notes

- IDS Hardware installation Guide

Configuration

Step	Activity	Web Manager	CLI Command(s)	Comments

1	Configure input contact	configure/alarms/facilities	(config)#alarm contact n	-assign a description for contact n -Set the severity level x (major, minor or none)for contact n · Set whether input is triggered when an open or closed condition occurs
2	Configure where the notification goes when triggered	configure/alarms/facilities	(config)#alarm facility input-alarm n	· For input contact n, set notification to be sent to syslog, as an snmp trap and/or energize the relay

Monitoring and Maintaining

- Display the settings for Input contacts

Activity	Web Manager	CLI Command(s)	Comments
Display Global status of monitoring conditions	Monitor/System/IO and Sensors	#show sysinfo	-Displays the status of; · Power supplies · Digital inputs (open or closed) state · DIP switch settings

Display Global status of monitoring conditions	Monitor/System/IO and Sensors	#show env all	Displays the status of ; · Internal temperature · Power supplies · Digital inputs (asserted or not asserted)

The IDS Hardware Installation Guide provides details on connecting unit power, ethernet devices, SFPs and consoles. This section assists the user with any software configuration and operational considerations that may be required.

2.1 - Connecting Power

The Hardware Installation Guide for your specific model will contain information on the units power requirements as well as help you ensure proper connection.

All models will come equipped with Power Status LED(s). Refer to the specific Installation Guide for details.

2.2 - Connecting Devices

RJ45 Ethernet Ports

By default all of the 10/100/1000 ports will automatically set themselves up to match the speeds of all attached devices. If autonegotiation is not support by one or more of the attached devices, the ports can each re-configured to operate fix speeds and duplex settings. See “Port Setup” for details on how to configure individual ports.

SFP slots

For those models with SFP slots, 100/1000/2500Base-X SFP modules supplied by Perle, Cisco or other manufacturers of MSA compliant SFPs are supported. The port will detect the speed of the SFP and auto-configure the port accordingly.

- Fiber SFP SERDES
    - Depending on the switch model, the following speeds are supported;
        - 100Base-FX

  - 1000Base-X
  - 2500Base-X SFPs running SERDES

- Fiber SGMII SFP
  - There are some non-standard SFPs such as Cisco's GLC-GE-100FX (version 1 and 2) that operate over SGMII (Serial Gigabit Media Independent interface). Perle IDS switches provides the configuration to support this SFP

- Copper SGMII, RJ45 SFP
  - Another type of SFP supported by the switch is Cisco's GLC-T SFP. This is an SFP that has an RJ45 port supprting 10/100/1000Base-T devices. They can be configured to use “auto-negotiation” or fixed speeds.

See “Port Setup” for details on how to configure SFP ports.

Fixed Fiber Transceivers

Some switch models have fiber ports In order to provide fiber connections specific to your fiber cabling needs and come in the following configurations;

- 100Base-x or 1000Base-x
- Multi-mode or single mode
- Duplex or Simplex (two or one fiber strand)
- Distances ranging from 500 meters to 160 Kilometers
- SC or ST connector type

See “Port Setup” for details on how to configure Fixed Fiber ports.

2.3 - SFPs

Overview

An IDS switch will accept any brand of MSA compliant SFP. This provides the user with a wide choice of brands to choose from including Perle's own brand of Cisco compatible SFPs.

Pre-requisites

- Switch models with SFP or Combo ports

Restrictions / Limitations

- None.

Terminology

- None.

Feature details / Application notes

- An IDS switch will accept any brand of MSA compliant SFP. This provides the user with a wide choice of brands to choose from including Perle's own brand of Cisco compatible SFPs.
- Auto speed detection of 100base-x and 1000base-x SFPs
- Display the SFP diagnostic information such as brand, serial number and power levels
  - If SFP vendor specified thresholds are exceeded, SNMP traps are initiated.
- Support for GLC-GE-100FX an SGMII-based fiber SFP (operating 100base-X)
- Support for the GLC-T, a 1000Base-T (SERDES mode)

Configuration

Some switch models don’t require any configuration for SFPs, however in the event that the SFP that is inserted operates under SGMII versus SERDES, the switchport for the SFP must be configured for SGMII.

In the case of the IDS 610 or 710 models, the mode (SGMII or SERDES) as well as the speed of the SFP needs to be configured.

Activity	Web Manager	CLI Command(s)	Comments
Configure a switch SFP port to accept an SFP operating under SGMII	Configure/Ports/Switchport settings	(config-if)#sgmii	Select the "Enable SGMII" checkbox

Monitoring and Maintaining

Display the standard informational and diagnostic information that is provided by the inserted SFP on a ports.

Activity	Web Manager	CLI Command(s)	Comments
Select an SFP port and view the SFP's informational and diagnostic data.	Monitor/Ports/ Port Status/SFP	#show Interfaces *interface-id* transceiver [a0 | a2 | ac] ac is applicable for SFPs that provide PHY register information	**This will display the following information from the SFP**. Product name Vendor name Serial number Connector Nominal Signaling Rate This is the bit rate including encoding information required to carry the data. Link reach for 9/125 single mode fiber. Link reach for 50/125 OM2 mode fiber Fiber wavelength **Alarm and Warning Thresholds (if provided by SFP)** Module Temperature Transceiver Transmit supply voltage Transceiver Transmit bias current Transceiver Transmit power Transceiver receive optical power

2.4 - Combo Ports

Overview

- A dual-purpose Combo port available on some IDS switch models, operate as a single port but with two interfaces, an RJ-45 10/100/1000Base-T cable and a fiber SFP. This provides flexibility in environments where the type of connection (copper or fiber) may change. Only one of the two interfaces can be active at a time with the SFP given priority. Configuration is provided that enables users to manage how the combo ports are to be used.

Pre-requisites

- Switch models with dual purpose combo ports

Restrictions / Limitations

- None.

Terminology

- None.

Feature details / Application notes

Specific to combo port configuration. For all other port configuration features please refer to “Port Setup”

- **Auto** : This is the default setting which will automatically pick the first interface which has a link. Once a port is selected (based on having a signal or link), no auto detection will take place until the link is lost. The other interface is disabled until such time as the link is lost on the on the other interface.
- **RJ45**: The RJ45 is the exclusive interface for the Combo port. The SFP interface is disabled
- **SFP**: The SFP is the exclusive interface for the Combo port. The RJ45 interface is disabled
- **Present / Not Present status**: If neither combo port interfaces have link, then the combo port status will show "not present". If an RJ45 copper connection is made, the combo port will show "10/100/1000base-TX". If the SFP is inserted and established link, the combo port will show "100Base-X" or "1000Base-X"

Configuration

Activity	Web Manager	CLI Command(s)	Comments
Select combo port media settings	Configure/Ports/ Switchport settings	(config-if)#media-type {auto-select | rj45 | sfp}	**Auto** : This is the default setting which will automatically pick the first interface which has a link. Once a port is selected (based on having a signal or link), no auto detection will take place until the link is lost. The other interface is disabled until such time as the link is lost on the on the other interface. **RJ45**: The RJ45 is the exclusive interface for the Combo port. The SFP interface is disabled **SFP**: The SFP is the exclusive interface for the Combo port. The RJ45 interface is disabled

Monitoring and Maintaining

Show combo port settings

Activity	Web Manager	CLI Command(s)	Comments
Show combo port settings	Monitor/Ports/Port Status	#show interfaces *interface-id* status	Displays the status of the port and which interface is assigned to the combo port

2.5 - LEDs

All models come equipped with Status LED(s). Please refer to the specific Installation Guide for details.

2.6 - Logging

Overview

The IDS switch has the ability to communicate and log event messages such as monitored alarms and other notable activity to its local volatile "buffered" memory log, to a file stored on the switch's non-volatile flash memory or to an external Syslog server, Telnet sessions, or the serial console port.

Pre-requisites

- None.

Restrictions / Limitations

- None.

Terminology

The Internal log stored in volatile memory can be viewed by the web manager or CLI.

If enabled, the local file stored in non-volatile flash memory will receive the switch logging information. This file can be copied off platform.

Syslog Source Interface: the VLAN interface used to send log messages to Syslog

Syslog facility

Syslog Facility is one information field associated with a syslog message and is defined by the syslog protocol. It is meant to provide a very rough clue from what part of a system the message originated from. Traditionally, under UNIX, there are facilities like KERN (the OS kernel itself), LPD (the line printer daemon) and so on. The "LOCAL_7" default facility which is traditionally reserved for administrator and application use is the default used by the switch. The user can however change the facility to a wide range of choices.

Origin ID Source: Select which origin ID will be inserted into the syslog messages. Selections can IP address, host (switch) name or a customizable string

Feature details / Application notes

A wide of options are provided to manage where events are communicated.

General settings

- Enable/disable logging
- Whether or not to include sequence numbers in the log messages
- Control the log rate limit in messages/second with the option of filtering based on severity

Timestamp

- Whether or not to include a timestamp in the log message based on date/time or by switch uptime.
- The default date format is Month/Day/ Hour/Minutes/Seconds. Additionally, milliseconds, year and time zone can be added
- Select whether to use local time or UTC (Universal Time Coordinated)

Syslog

- Enable/disable the sending of messages to one or more IPv4 or IPv6 syslog servers

Console and Telnet sessions

- Enable/disable the sending of messages to the serial console port and to authenticated Telnet sessions

Buffered and File

- Select whether to send log messages to the switch's internal buffered memory or to a non-volatile file on the switch's flash

Configuration

General Settings

Activity	Web Manager	CLI Command(s)	Comments
Enable/disable logging	Configure/System/Logging/general	(config)#logging on	Enable logging (default)
Sequence numbers	Configure/System/Logging/general	(config)#service sequence-numbers	Select that sequence numbers be added to the log messages

Maximum log message rate limit	Configure/System/Logging/general	(config)#logging rate-limit	Set the maximum logging rate in messages per second (1 to 10000) optionally filter by minimum severity level : Emergency Alert Critical Error Warning Notification Informational Debugging

Timestamp

Activity	Web Manager	CLI Command(s)	Comments
Include timestamp in messages	Configure/System/Logging/timestamp	(config)#service timestamps log	Select Date and Time or Switch uptime and whether to include, milliseconds, year, time zone, use the local time on the switch or UTC (Universal Time Coordinated) time

Syslog

Activity	Web Manager	CLI Command(s)	Comments
Enable log messages to be sent to Syslog server(s) and severity level	Configure/System/Logging/Syslog	(config)#logging trap or disable with (config)#no logging trap	Enable/disable log messages to Syslog and filter by severity level: · Emergency · Alert · Critical · Error · Warning · Notification · Informational · debugging
Add one or more Syslog server(s)	Configure/System/Logging/Syslog	(config)#logging host <*host name/IP Address* >	Add Syslog server(s) by host name via qualified domain name or IP address specifying a transport of UDP (default) or TCP. The port number and also be changed (default is 514 for UDP and 601 for TCP)
Delete Syslog Server	Configure/System/Logging/Syslog	(config)#no logging host <*host name/IP Address* >	Delete Syslog server by host name via qualified domain name or IP address

Select Syslog Source VLAN interface	Configure/System/Logging/Syslog	(config)#logging source-interface vlan	Specify the source of the management VLAN interface (1-4096) for sending messages to Syslog

Configure Syslog Facility identifier	Configure/System/Logging/Syslog	(config)#logging facility	Identify the Unix Syslog facility identifier. Choose from one of; · kernel messages · user-level messages · mail system · system daemons · security/ authorization messages · messages generated internally by syslogd · line printer subsystem · network news subsystem · UUCP subsystem · clock daemon · security/ authorization messages · FTP daemon · NTP subsystem · log audit · log alert · clock daemon · local use 0 (local0) · local use 1 (local1) · local use 2 (local2)

Select origin-ID source	Configure/System/Logging/Syslog	(config)#logging origin-ID	Select origin ID from one of the following; hostname as ID · ip (Use IP address as ID) · ipv6 (Use IPv6 address as ID) · Custom (configurable unique text string as ID) · None (default)
Select append a line feed delimiter to syslog messages over TCP	Configure/System/Logging/Syslog	(config)#logging delimiter tcp	

Console/Telnet

Activity	Web Manager	CLI Command(s)	Comments

Enable log messages to the serial console port	Configure/System/Logging/console	(config)#logging console	Enable/disable log messages to the console and filter by severity level: · Emergency · Alert · Critical · Error · Warning · Notification · Informational · debugging

Enable log messages to Telnet sessions	Configure/System/Logging/Telnet	(config)#logging monitor	Enable/disable log messages to Telnet sessions and filter by severity level: · Emergency · Alert · Critical · Error · Warning · Notification · Informational · Debugging Note the following EXEC CLI command " #terminal monitor" is required to begin log messages appearing during the terminal session. "#no terminal monitor" will turn it off.

Enable log messages to Buffered memory	Configure/System/Logging/Buffered	(config)#logging buffered	Enable/disable log messages to internal buffered memory. and filter by severity level values <0-7> or keyword · Emergency · Alert · Critical · Error · Warning · Notification · Informational · Debugging Optionally set the maximum size in bytes of the internal RAM buffer. Valid values are < 4096-32768 > (Default is 4096 bytes.)

Enable log messages to a file in non-volatile flash	Configure/System/Logging/File	(config)#logging file flash:*<filename>*	Enable/disable log messages to flash memory *<filename>* and filter by severity level values <0-7> or keyword · Emergency · Alert · Critical · Error · Warning · Notification · Informational · Debugging Optionally set the maximum and minimum size of the cyclical logging file. Valid maximum range is <4096-2147483647> (default 4096.). The minimum logging file size range is <1024-2147483647> (default 2048.) *Users with IDS switch models that have an SD card installed, can copy the log file from the switch's internal flash to the SD flash card.*

Monitoring and Maintaining

- **Display logging settings**

Activity	Web Manager	CLI Command(s)	Comments
Display all of the configuration settings for logging	Configure/System/Logging	#show logging	CLI shows all of the settings related to logging and includes a view of the buffered log. Under Web Manager, the buffered log can be viewed under Monitor/system/View Log

2.7 - Alarms

Overview

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

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

Port Status Monitoring Alarms

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

Global Status Monitoring Alarms

- Dual power supply alarm
- Internal temperature alarm
- SD card (model dependent)

Pre-requisites

- For additional details regarding the alarm relay, please refer to the IDS Hardware Installation Guide

Restrictions / Limitations

- none

Feature details / Application notes

Alarm Relay

The alarm relay is an additional method for indicating that an alarm condition exists. Utilizing the switch's built-in dry contact alarm relay, a circuit can be designed that drives a light or speaker when the contacts on the alarm are open or closed. The switch's contact relay has a default alarm state which is either a normally open or closed condition. Please refer to the hardware installation guide for your particular model. The Ethernet switch upon power up, remains in this default alarm state until the boot process has completed. Once the boot cycle has completed and finds that no error conditions exist, the switch OS "energizes" the relay. Should an alarm condition occur, the switch OS will "de-energize" the relay. The user also has the ability to change the setting of the default alarm condition to either "de-energize" (default) or "energize".

Alarm Levels

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

- Critical
  - Severity 1
  - Syslog equivalent is "Emergency"
-
- Major
  - Severity 2
  - Syslog equivalent is "Error"
- Minor
  - Severity 3
  - Syslog equivalent is "Warning"
- Informational
  - Severity 4
  - Syslog equivalent is "Informational"

Configuration of Alarm Common Settings

Activity	Web Manager	CLI Command(s)	Comments
Set the alarm relay mode	Configure/System/alarms/common settings	(config)#alarm relay-mode	The default for the alarm relay is to de-energize the relay. However should the user's alarm circuit require a contact closure to invoke an alarm, select "energize"
Set Syslog Alarm Level	Configure/System/alarms/common settings	(config)#logging alarm	Set the Syslog alarm level to "none" (default), "Major Only " for alarms that are Major and above or "Minor and Major " for all levels
Set SNMP trap level	Configure/System/alarms/common settings	(config)#logging trap	Set the SNMP trap alarm level to "none" (default), "Major Only " for alarms that are Major and above or "Minor and Major " for all levels.
Enable the monitoring of dual power inputs	Configure/System/alarms/common settings	(config)# power-supply dual	Provides the ability for an alarm condition to occur should one of the two power inputs become absent. This is not enabled by default

Port Status Monitoring Alarms

Port monitoring is provided through the use of port profiles. Port profiles are created to identify which port related alarm conditions are to be reported and where to send the alert message to. A Port Profile can be assigned to all or individual ports.

Port Profiles can configured to monitor one or more of the following conditions;

- Link fault
    - This condition exists when the link is not up.
    - Alarm severity = MAJOR
- Port not forwarding
    - Whenever a port is blocked (Spanning Tree, Ring, etc) the port goes into a "none forwarding" mode.
    - Alarm severity = MINOR
- Port not operational
    - This is a detected hardware issue discovered by the switch software for the port.
    - Alarm severity = MAJOR

A default port profile called "*defaultPort"* is provided and assigned to all ports. This profile can either be edited if required or additional profiles can be created and assigned to individual ports. This default port profile cannot be deleted.

Configuration of Port Profiles

Activity	Web Manager	CLI Command(s)	Comments
Edit the default port profile	Configure/System/alarms/port profiles	(config)#alarm profile <*defaultPort*>	Select port condition(s) for alarm processing
Add a new port profile	Configure/System/alarms/port profiles	(config)#alarm profile <*profile name*>	Create new profile name of choice and select port condition(s) for alarm processing
Assign port profile to port	Configure/System/alarms/port profiles	(config-if)#alarm profile <*profile name*>	Assign individual ports with a port profile

Global Status Monitoring Alarms

Global status monitoring is provided for the various environmental facilities provided by the switch such as temperature, SD card presence (model dependent) and dual power supply status.

The switch provides the ability to set high and low temperature thresholds for two separate temperature ranges. The default Primary temperature range is set to -20C to 95C. When enabled, a major alarm is generated whenever the temperature is outside of this range. These threshold can be adjusted according to the local environmental conditions. A secondary temperature range, disabled by default can be enabled to generate a minor alarm. This can be used as a "warning" range if set to a temperature range that is within the primary range, but beyond the expected normal operating range.

Configuration of Global Status Monitoring Alarms

Activity	Web Manager	CLI Command(s)	Comments
Configure environmental facilities monitoring for dual power supply	Configure/System/alarms/facilities	(config)#alarm facility power-supply rps	Select set notification to be sent to syslog, as an snmp trap and/or energize the relay should one of the dual power supplies fail
Configure environmental facilities monitoring for SD card (model dependent)	Configure/System/alarms/facilities	(config)#alarm facility sd-card	Select set notification to be sent to syslog, as an snmp trap and/or energize the relay when an SD card is inserted or removed from the switch
Configure environmental facilities monitoring primary internal temperature (model dependent)	Configure/System/alarms/facilities	(config)#alarm facility temperature primary	Set the high and low primary temperature threshold along with the notification to be sent (to syslog, as an snmp trap and/or energize the relay) should the temperature exceed these thresholds Default temperature thresholds are a high of 95C and a low of -20C.

Configure environmental facilities monitoring secondary internal temperature (model dependent)	Configure/System/alarms/facilities	(config)#alarm facility temperature secondary	Enable and set the high and low secondary temperature threshold along with the notification to be sent to (syslog, as an snmp trap and/or energize the relay) should the temperature exceed these thresholds

Monitoring and Maintaining

Activity	Web Manager	CLI Command(s)	Comments
Display status of alarm settings	Configure/System/alarms/facilities	#show alarm settings	Displays the alarm settings for the global monitoring alarms
Display alarm profile settings	Configure/System/alarms/facilities	#show alarm profile *<port profile name>*	Displays the port profile settings of the selected port profile

DIP Switch Settings

Overview

The DIP switches on the IDS switch provide a quick and easy way to setup a Ring connection in order to achieve improved network reliability and faster recovery times from network faults. A ring can also be setup and configured from any of the software configuration methods. Software configuration methods provide access to addition parameters as well as the more advanced ring features.

DIP Switch				**Ring Feature**
S1	**S2**	**Ring Role**	**Coupling Mode**	**Description**
On	On	--	--	Software control - Ring Manager functionality will be controlled by the configuration setup in software configuration.
On	Off	Master	Active	Ring Feature is enabled, IDS is Ring Master, Port 4 will be used as the active coupling port.
Off	On	Client	Backup	Ring Feature is enabled, IDS is a Client device on the ring, Port 4 of this IDS will be the backup coupling port.
Off	Off	Client	Off	Ring Feature is enabled, IDS is a Client device on the ring. No coupling features on this IDS

For further details, please refer to the IDS Hardware Installation Guide

Pre-requisites

- Available on 409/509 including 509 PoE models

Restrictions / Limitations

- None

Configuration

- None

Monitoring and Maintaining

Activity	Web Manager	CLI Command(s)	Comments
Display the position of the DIP switches	Monitor/System/ IO and Sensors	#show sysinfo	Displays on/off position of hardware DIP switches
View physical DIP switch positions on unit	Graphic of unit will correctly position the switches as monitored by the switch	None	Displays physical positions of hardware DIP switches

2.8 - Micro SD card

Overview

- A MicroSD card can be used for configuration files and firmware backup and restoration. Files can also be copied to or from the SD card.

Pre-requisites

- MicroSD cards are supported on the 306 and 409/509 series models. Check your IDS Hardware Installation Guide for details.

Restrictions / Limitations

- none

Feature details / Application notes

- IDS Hardware installation Guide

Configuration

There is no configuration required for using an SD card

Monitoring and Maintaining

Displays whether there is a **microSD card present** in the card slot

Activity	Web Manager	CLI Command(s)	Comments
Displays whether there is a microSD card present in the card slot	Dashboard	#show sysinfo Shows how much space is available on the SD card	Displays whether an SD card is present.

To safely **removing an SD card**, the card must first be ejected

Activity	Web Manager	CLI Command(s)	Comments
Safely eject the SD card prior to removal	Administration/File Management/SD card/Eject SD card	#eject	The user can now safely remove the microSD card from the switch.

2.9 - RJ and USB Serial Consoles

Overview

- All IDS switches have a console port. Some models come with an RJ45, RS232 serial console port and some have USB console port. In conjunction with a terminal-emulation program on the PC such as HyperTerminal or PuTTY, this port enables an out of band session to perform CLI commands.
- Some IDS switches come with both an RJ45 serial RS232 and a USB console port. Only one console port can be active at one time.

Pre-requisites

- PC with terminal emulation software such as PUTTY or Hyperterminal.

Restrictions / Limitations

- The IDS 409 and IDS 509 series models have an RJ45, RS232 and a USB serial console port.
- The IDS 610/710 switches only have the USB console port.

Terminology

- none

Feature details / Application notes

- The IDS switch can be fully configured and managed from a console port providing direct access to the Command Line Interface (CLI).
- Configuration provides connection flexibility
- For those models which have both and RJ45 and a USB console port, the USB console port if connected, takes precedent over the RJ console port. Configuration is provided to enable the RJ port to be the preferred console port over the USB. An inactivity timeout value can be configured on the USB port which upon expiry, will direct the console to the RJ serial port
- If enabled, logging messages can be directed to the console port. Logging messages will arrive on both the RJ45 and USB console ports

Configuration

Activity	Web Manager	CLI Command(s)	Comments
Set speed on RJ console	Configure/Ports/Console	(config-line)#speed	Select speed matching the device you are connecting to. 9600, 19200, 38400, 57600, 115200, default: 9600
Set number of data bits on RJ console	Configure/Ports/Console	(config-line)#databits	Select the number of data bits required; Data bits: 7, 8, Default: 8
Set number of stop bits on RJ console	Configure/Ports/Console	(config-line)#stop-bits	Select the number of stop bits required; 1 or 2, default: 1
Set parity on RJ console	Configure/Ports/Console	(config-line)#parity	Select the parity required; None, Even, Odd, Default: None
Select the RJ console as the preferred console port	Configure/Ports/Console	(config-line)#media-type rj45	Select "Prefer RJ-45 console" if the RJ console if preferred when both console ports are connected

Specify USB inactivity timeout	Configure/Ports/Console	(config-line)#usb-inactivity-timeout	Select whether to apply a USB inactivity timeout. If selected, a range of 1 to 240 minutes is available

Monitoring and Maintaining

Show console port settings

Activity	Web Manager	CLI Command(s)	Comments
Display console port settings	Configure/Ports/Console	#show line console *linenumber* *Normally select 0 for linenumber*	Displays console port settings including whether the RJ has been selected as preferred or not.

2.10 - Reset

Overview

- A reset will cause the software to re-start.

Pre-requisites

- None

Restrictions / Limitations

- None

Feature details / Application notes

- When a reset is performed on the switch, the following action takes place;
  - All tasks running on the switch are terminated.
  - All interfaces are turned off (until the switch re-starts).
- A reset is not the same as a power down. Powering down the unit resets all hardware in the switch where as a reset, only re-loads and re-starts the software.
- A reset can be performed via software or via hardware.
  - Hardware
    - Press the "Reset/FS" switch and let it go. (if you press it for longer than 2 sec-

onds, instead of a reset, you will activate the "Password recovery" mode).

- Software
  - Using the CLI, issue the command "#reload"
  - Using the Web manager, select "Reboot" under the "Administration" menu item.

- Using the "Software" option to reset the switch, the user has the following additional options;
  - Reset immediately
    - #reload<CR>
  - Reset in nnn minutes or in hh:mm hours and minutes
    - #reload in 12 (will reset in 12 minutes)
  - Reset at a specific time
    - #reload at 11:45 (will reset at 11:45)
- A timed reset can be canceled by the user by issuing the command;
  - #reload cancel
- Same capabilities can be found in the Web Manager under the "Reboot" menu.

2.11 - Restoring to Factory Configuration

Overview

- Restoring to factory default will erase all user files in the flash.

Pre-requisites

- Requires physical switch access.

Restrictions / Limitations

- Will not modify the current version of software on the switch. User can revert back to previously loaded software. See “Software Image Management”

Terminology

Flash

- Non-volatile memory which exists on the switch. Any information stored in this volume is not lost when power is removed from the switch.

Feature details / Application notes

- In order to reset a switch to "factory default", the operator must have physical access to the switch.   This is done as an added security measure.
- All user created files will be removed during a "reset to factory" operation. This includes the following;
  - Startup configuration.
  - Log files.
  - Any keys or certificates downloaded to the switch.

  - o Any files manually copied to the flash volume .

Configuration/Operation

- Steps for “Resetting to factory default”.
  1. Remove the power from the switch
  2. Press and hold the "Reset/FS" button.
  3. While keeping the button pressed, connect the power to the switch and let it power up.
  4. When the "power LED" changes from "Red" to "Orange", release the "Reset/FS" button.
  5. Switch will boot up in factory default state. This state will be maintained until such time as the user configures the switch.

Monitoring and Maintaining

- Reasons for "resetting to factory default"
  - o When powering up the switch, the boot up sequence does not progress past the initialization (system LED continues flashing forever).
    - This is an indication that something in the existing start-up configuration file is preventing the switch from booting.
  - o You wish to go back to a clean starting point with the switch configuration.
- When the switch is in factory default, it will attempt to obtain an IP address via DHCP. Until such time as it gets an IP address, the only way to manage the switch is via the console port or "Fast-setup". (see “Fast Setup”)

2.12 - Password Recovery

Overview

- A method of gaining access to the switch if you forget the login information.

Pre-requisites

- Requires physical access to the switch.

Restrictions / Limitations

- Feature can be disabled via configuration.

Terminology

Fast Setup

- o A specific mode of operation of the switch triggered by a 4 second press of the "Reset/FS" button.

Feature details / Application notes

- This feature allows a user who has physical access to the switch to gain management access when they have forgotten their login credentials.
- The feature is on by default but can be disabled via configuration.

Configuration / Operation

Step	Activity	Comments
1	Put the switch in "Fast Setup mode"	· Press and hold button for about 4 seconds. · LEDs on first available port will flash. At this point, release the button.
2	Plug the PC into flashing port.	· Make sure that the connecting PC is set for DHCP.
3	Bring up your browser.	· Browse to any site or you can also browse to 169.254.0.1 · When initial screen comes up, press "continue".
4	Change the username and password	· You are now able to define a user and a password for that user.

Monitoring and Maintaining

- **Disabling the "password recovery" feature.**

Activity	Web Manager	CLI Command(s)	Comments
Disable the feature	Password Recovery	(config)#no service password-recovery	· With this configuration in place, the only way to access the switch if credentials are forgotten is to reset it back to factory default.

3 - Network Settings

Network Settings enables the user to configure the IP address for the Management VLAN interfaces as well as DNS Servers and the local Host table.

3.1 - IP

Overview

- To access the switch via the network, at least one IP address is required. Perle IDS switches provide the ability to manage the unit via separate Management VLAN interfaces having individual IP addresses.

Pre-requisites

- None

Restrictions / Limitations

- None

Terminology

Feature details / Application notes

- IP addresses can be configured manually or via an external DHCP server. Supports separate DHCP servers per VLAN.
- Configuration of optional advanced DHCP settings
- IPV4 and IPV6 addressing supported
- IPV6 is disabled by default and must be enabled if required
- Address Conflict Detection for both IPv4 and IPv6, can be enabled if desired.

Configuration

- During initial setup, the switch's standard management VLAN interface under VLAN ID 1 can be configured using the "Fast Setup" feature.
- To **edit Management VLAN interfaces**, the following steps are required

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Edit VLAN description	Configure/System/ Network/Settings/IP	(config)#interface vlan <*vlanid*> (config-if)#description	Edit the description of VLAN interface for vlanid.

2	Disable VLAN interface Enable VLAN interface	Configure/System/ Network Settings/IP	(config)#interface vlan <*vlanid*> (config-if)#shutdown (config-if)#no shutdown	Disable VLAN interface for vlanid. Enable VLAN interface ID for vlanid
3	Enable DHCP for VLAN interface	Configure/System/ Network Settings/IP Configure/System/ Network Settings/IP	(config)#interface vlan <*vlanid*> (config-if)#ip address dhcp (config-if)#interface vlan <*vlanid*> (config-if)#no ip address dhcp	Enable DHCP on VLAN interface for vlanid (default) Disable DHCP on VLAN interface for vlanid
4	Set a static IP address versus using a DHCP server for a Management VLAN Interface	Configure/System/ Network Settings/IP	(config)#interface vlan <*vlanid*> (config-if)#ip address ip-address mask	Set the IP address and mask for the management VLAN interface.
Note	IP address for Management VLAN interface set to “none”	Configure/System/ Network Settings/IP		The check on the “none” box will reflect the creation of a management VLAN interface that does not have an IP address.

- Enable IPV6

Activity	Web Manager	CLI Command(s)	Comments
Enable/Disable IPV6	Configure/System/ Network Settings/IP	(config)#sdm prefer dual-ipv4-and-ipv6 (config)#no sdm prefer	Enable IPV6 Disable IPV6 (default)

Address Conflict Detection

This feature will ensure that the IP address assigned to the VLAN is not currently in use by a different device on the network.

Applies to both IPv4 and IPv6 addresses. IPv6 refers to the feature as "Duplicate Address Detection"

Applies to both static and DHCP address assignment.

- With DHCP, if the address is already in use the switch will return a "DCHPDECLINE" to the DHCP server.
- In the case of a static configuration, the following error will be displayed. "IP address already in use by another device on Network"

When an address conflict is detected, the alarm LED will be turned on. A log entry will also be made to indicate this condition was detected. This is not configurable.

Activity	Web Manager	CLI Command(s)	Comments
Enable Address Conflict Detect	Configure/System/ Network Settings/IP	(config)#ip service address-conflict-detection	Enables the IP address conflict detection logic. This is a global command and applies to all VLAN interfaces
Display feature status.	Monitor/System/ Network/IP Conflict Status	#show address-conflict-detection status	If a conflict exists, this will provide the IP address which has the conflict.

Monitoring and Maintaining

Activity	Web Manager	CLI Command(s)	Comments
Display the management VLAN interface status.	Monitor/System/ Network/IP Status	#show interfaces	Displays information on all the interfaces including the VLAN interfaces
Display IPV6 status.		#show sdm prefer	

3.2 - DNS Server and Host Table

Overview

The DNS (Domain Name Service) protocol controls the Domain Name System (DNS), a distributed database with which you can map hostnames to IP addresses. This enables the user to substitute the hostname for the IP address within all local IP commands, such as ping and telnet.

The IP address of the DNS server can be obtained from either a DHCP server or manually configured on the switch.

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

Pre-requisites

- None

Restrictions / Limitations

- None

Terminology

Feature details / Application notes

- Configure an external DNS server to resolve name to IP address
- Configure a local host table with a database of names to IPV4 addresses
- The host table is examined before doing a lookup via a DNS server

Configuration

Configure DNS Servers

Activity	Web Manager	CLI Command(s)	Comments

Enable DNS Server	Configure/System/ Network Settings/ DNS/DNS Settings	(config)#ip domain lookup (config)#no ip domain lookup	Enable IP address lookup via a DNS server (Default is enabled) Disable IP address lookup via a DNS server
Configure default domain name (optional)	Configure/System/ Network Settings/ DNS/DNS Settings	(config)#ip domain-name <*name*> (config)#no ip domain-name	Configure the default domain name used to complete unqualified host names when entering IP host names on the switch. For example, if you set the domain name to "sample.com," and specify a syslog server by the unqualified name of "Jupiter," then the switch qualifies the name to "jupiter.sample.com." Delete default domain name.
Add DNS Server	Configure/System/ Network Settings/ DNS/DNS Settings	(config)#ip name-server *server-address1 [server-address2…server-address6]* (config)#no ip name-server *server-address1 [server-address2…server-address6]*	Add IP addresses for one or more DNS Servers. There is no limit imposed to the number of DNS servers that users can configure. Delete DNS server address.

Configure Local Host Table

Activity	Web Manager	CLI Command(s)	Comments

Add a host and IP address to the local host table	Configure/System/ Network Settings/ DNS/IPV4 Host Table	(config)#ip host *<host-name, IP Address>* (config)#no ip host *<hostname>*	Add a host name and IP address to the host table. Delete host.

Monitoring and Maintaining

Activity	Web Manager	CLI Command(s)	Comments
Display host table and DNS Server	Configure/System/ Network Settings/ DNS/DNS Settings Configure/System/ Network Settings/ DNS/IPV4 Host Table	#show hosts	

3.3 - DHCP (Client)

Overview

- This is the ability to enable the switch to use DHCP to obtain IP related information from a DHCP / Bootp server.

Pre-requisites

- The network must have a DHCP server or DCHP relay agent which is accessible to the switch via broadcasts.

Restrictions / Limitations

- None.

Terminology

- **DHCP** – Dynamic Host Configuration Protocol
  - A client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet

mask and default gateway.

- **DHCP Server**
  - The program responsible for managing and assigning IP addresses to IP devices in the network. A single network may contain multiple DHCP servers.
- **DHCP Client**
  - The IP device which is attempting to obtain IP information from the DHCP server(s).
- **Bootp – Bootstrap Protocol**
  - A networking protocol used in Internet Protocol networks to automatically assign an IP address to network devices from a configuration server. Bootp was the predecessor to DHCP.
- **DHCP Relay Agent**
  - A program that relays DHCP/BOOTP messages between clients and servers on different subnets.
- **DHCP Lease**
  - This defines the duration for which the IP address provided to the client by a DHCP server is valid.

Feature details / Application notes

- In order to manage the switch, the management interface must be assigned an IP address. This can be done manually via a configuration command or dynamically via DHCP. If DHCP is used, the network must include a DHCP or Bootp server whose job it is to manage the assignments of IP addresses to the various IP devices in the network.
- In some cases, the client can provide the DHCP server with a “hint” which will help the server determine which IP address to give the client. This hint can include any or all of the following
  - Client-id
    - This can be configured to be the MAC address of an interface name, an ASCII text or hex string.
  - Class-id
    - Hex string or ASCII text. This same hex string or text would be configured on the server side and associated with an address to give the client.
  - Host name
    - This can be any string. By default, this is the switch name.

- The DHCP client can request the following attributes from the DHCP server;
  - Specific lease terms.
  - Which of the following options they would like to receive.
    - DNS name server
    - Domain name
    - Default router
    - TFTP server
    - Time zone string
    - Time zone offset
    -

Configuration

- **Set the DHCP client parameters and configure vlan interface to use DHCP.**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Select the VLAN interface you wish to set up.	IP Connections	(config)#int vlan nnn	Select the vlan interface
2	Set to use DHCP	IP Connections	(config-if)#ip address dhcp	Use DHCP to get an IP address for this interface
3	Configure DHCP operation parameters	Advanced DHCP Settings	(config)#ip dhcp client…	Set class-id, client-id, hostname, lease and options.
4	Repeat for each VLAN interface as needed.			

Monitoring and Maintaining

- **Monitoring MAC addresses**

Activity	Web Manager	CLI Command(s)	Comments
Display VLAN status	IP Connection Status	#show int vlan 1	Shows the status of vlan 1
Display lease info	IP Connection Status	#show dhcp lease	Provide details on the IP lease.
Renew lease	IP Connection Status	#renew dhcp vlan 1	Attempt to renew the lease for vlan 1.
Release lease	IP Connection Status	#release dhcp vlan 1	Give up the IP address provided to the switch.

4 - Basic Configuration

Basic Configuration covers the fundamental aspects of the switch's general settings along with its Ethernet ports.

4.1 - Port Setup

Overview

The IDS switch will come with copper, fiber or SFP ports depending on the specific model.

Terminology

Port: Actual Port number as viewed on the unit.

Interface: Port Interface name. Used in various CLI commands.

Enabled: Disabling a port will ensure that no link can be established on that port. This can be done without the loss of any of the configuration information for that port.

Description: An optional Description for the port can be entered. This can be anything that is meaningful.

Speed Negotiation: Copper Ethernet connections virtually always use Auto-negotiation. When Auto-negotiation is used you may select which of the supported communication speeds will be advertised during the negotiation process.

Advertise Speed: Depending on the interface type Advertised speeds will be available to used with the A.

Speed and Duplex: Allow you to select the fixed speed and duplex settings if Speed Negotiation has been set to fixed.

Gigabit Master Slave: Determines which of the two link partners will be designated as the master. By default this is negotiated between the two link partners. Normally multi-port devices such as switches and routers will take on the Master role. If two such devices are connected the IEEE802.3ab specification defines the methods of establishing priority using seed bits.

Flow Control: Permits the IDS to effectively regulate traffic. These ports can generate flow control frames when their receive queues reach pre-defined limits. This signals the transmitter to slow the transmission. In turn these ports will react to receiving flow control frames by pausing packet transmission for the time specified in the flow control frame.

Crossover: When wiring cables for twisted pair copper-based Ethernet, there are two pin-outs, one for each end. These are referred to as MDI and MDI-X (medium dependent interface – crossover). You can use a straight through cable when connecting an MDI to an MDI-X port. Typically MDI ports are used on end devices and MDI-X ports are used on switches. If connecting two like ports you would be required to either use a crossover cable, configure the ports such that they are different or use the Auto crossover feature which will detect the need for a crossover and activate it in the switch hardware.

ATU – Address Translation Unit

- The ATU is a set of tables which are maintained in the switch. Each table is associated with a specific port on the switch. It holds the MAC addresses for all devices which may be connected on the port. Addresses are categorized within VLANs.

Age-out

- The term is used to describe the process whereby an ATU entry

Feature details / Application notes

- None

Configuration

- Adding static MAC addresses

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Determine which MAC addresses will reside on each port.			· Should include all MAC address you wish to associate with a port or ports. · Also include any MAC addresses you wish to disallow.

2	Add the static entry	Static MAC Addresses	(config)#mac address-table static	· An entry is required for each unique VLAN and MAC address combination.

Monitoring and Maintaining

- **Monitoring MAC addresses**

Activity	Web Manager	CLI Command(s)	Comments
Display static MAC addresses	MAC Address Table	#show mac address-table static	· In Web Manager, use the filtering capability to display "static" entries.

4.2 - System General Settings

Overview

System General Settings enables the user to configure the identification, manual date and time and management access filtering.

Pre-requisites

- none

Restrictions / Limitations

- none

Terminology

- Date is in MM/DD/YYYY format
- Time is represented as a 24hr clock
- Time zone is displayed as an offset to UTC (Coordinated Universal Time)

Feature Details / Application Notes

- Identification

  - Configure a unique system name for the switch. This is used on the title of all web manager pages, CLI command prompt and syslog messages
  - Location (SNMP)
  - Contact (SNMP)
- Date, Time and Time Zone
  - Time can be set through the use of external services such as NTP servers or can be manually set via the web manager or CLI commands
    - Time and Time Zone can be manually keyed-in or can be obtained directly from the web browser connected PC workstation
- Management Access
  - Select which management access method are allowed to be used with the switch. Choices are Telnet, (SSH), console, HTTP, HTTPS, and SNMP.
- Idle Timeout for web manager sessions (range 1 to 1440 seconds). When no activity occurs during the web session over the course of the timeout period, the web session is terminated
- The HTTPS port number can also be modified from the standard default of 443.

Configuration

Activity	Web Manager	CLI Command(s)	Comments
Set system Name	Configure/System/System General Settings	(config)#hostname <hostname>	Configure a host name. Spaces are not allowed
Set location	Configure/System/System General Settings	(config)#snmp-server location	Configure the location field for SNMP server
Set contact name	Configure/System/System General Settings	(config)#snmp-server contact	Configure the contact field for SNMP server
Manually set time and date	Configure/System/System General Settings	#clock set hh:mm:ss { day month | month day } year	Manually set time and date Can also derive date and time from PC via web manager

Manually set timezone	Configure/System/System General Settings	(config)clock timezone	Manually set timezone from drop down menu Can also derive timezone from PC via web manager
Select methods for management access	Configure/System/System General Settings	(config)#snmp-server Or (config)#no snmp-server (config)#ip telnet server or (config)#no ip telnet server (config)#ip ssh server or (config)#no ip ssh server (config)#line console 0 (config-line)#no (config)#ip http server or (config)#no ip http server (config)#ip http secure-server or (config)#no ip http secure-server	Select which methods for management access are allowed; · SNMP · Telnet · SSH · Console · HTTP · HTTPS *By default all access methods are allowed*
Change HTTPS port number	Configure/System/System General Settings	(config)#ip http secure-port	If required, change the standard HTTPS port number from 443 to a different value (1024 to 65535)
Set an idle timeout value for all web sessions	Configure/System/System General Settings	(config)#ip http session-idle-timeout	Set idle time for web manager sessions. Range is between 1 and 1440. Default is 1440 (24 hours).

Monitoring and Maintaining

Activity	Web Manager	CLI Command(s)	Comments
Show the status of SNMP	Configure/System/System General Settings	#show snmp	Displays the status of SNMP
Show status of the Telnet server	Configure/System/System General Settings	#no ip telnet server command displayed in running-config	Displays status of the Telnet server
Show the status of the console	Configure/System/System General Settings	#show line console 0	Displays the status and information on the console port(s)
Show the status of the HTTP server		#show IP http server status	Displays HTTP and HTTPS server status.
Show the status of the SSH server		#show IP ssh	Displays information on the SSH server

4.3 - Switch General Settings

Overview

Jumbo frames are Ethernet frames with a payload greater than 1518 bytes. Some networks require jumbo frame traffic and others do not want this type of traffic flowing. Switch General Settings enables the user to select whether jumbo frames are allowed to pass through the switch.

Pre-requisites

- none

Restrictions / Limitations

- Frames to and from the switch's management interface are defaulted to a maximum frame size of 1518 bytes and is not affected by the enabling of jumbo frames for normal switch port traffic.

Terminology

Jumbo frames are Ethernet frames with a payload greater than 1518 bytes.

The size of the jumbo frames will vary across various switch models. To identify the jumbo frame size for your particular model, please refer to the product hardware specifications on the Perle web site

Feature details / Application notes

- The ability to support jumbo frames across the IDS switch ports can be enabled or disabled globally. If jumbo frames are disabled, a maximum frame size of 1522 bytes is adopted. Any frames received above the maximum frame size are discarded

Configuration

Activity	Web Manager	CLI Command(s)	Comments
Enable or disabled jumbo frame support	Configure/switch/switch general settings	(config)#system mtu jumbo Or (config)#no system mtu jumbo	· Enable or disabled jumbo frame sizes · · If jumbo frames are disabled, a maximum frame size of 1522 bytes is adopted. Any frames received above the maximum frame size are discarded

Monitoring and Maintaining

Activity	Web Manager	CLI Command(s)	Comments
View whether jumbo frames are supported or not	Configure/switch/switch general settings	#show system mtu	· Will display “jumbo” (for jumbo frames) or “normal” when jumbo frames are disabled

5 - File Management

The Perle IDS switch line provides a comprehensive range of services to manage files on the IDS switch line. These include using a web browser, external file servers such as TFTP or using the removable SD flash card available on some models.

5.1 - Software Image Management

Overview

This section describes how to manage software image files, which contain the system software for Perle IDS switches

Images can be downloaded from an external TFTP, SFTP, FTP, HTTP, HTTPS or SCP server. If none of these external services exist on the network, a software image file downloaded from the Perle web site, can be downloaded using the IDS Switch Web Manager.

If the IDS model has an SD cardflash capability, a firmware image can also be loaded onto a microSD card and inserted into the switch for direct copying.

The current image can be replaced with a new one or kept in flash memory after a download as a backup. It is also possible to upload a switch image file to a TFTP, FTP or SCP server for backup purposes.

PerleView, an enterprise-grade centralized Microsoft Server-based management program can also be used to manage software downloads across a large number of IDS Managed Switches. Refer to "PerleView" Chapter for details.

All Perle IDS Ethernet switch models share the same universal firmware image. Specific functions and features are enabled depending on the model purchased. The benefit of this type of approach is that all models can share a single firmware file that may be loaded onto a central file server (ie TFTP). This greatly simplifies updates for the user when multiple Perle IDSmodel types exist in the same network.

Pre-requisites

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

Terminology

- "Startup" image is the firmware that is stored in flash and executed upon reboot
- "Running" image is the actual firmware image that is executing on the switch.

- "Backup" image is the firmware that was replaced during an upload and archived should that version be required to be restored.
- SCP (Secure Copy Protocol) uses Secure Shell (SSH) for data transfer, authentication and encryption.
- TFTP (Trivial File Transfer Protocol is a common File Transfer Protocol which allows a client to get a file from or put a file onto a remote host)
- SFTP (Secure File Transfer Protocol is a common File Transfer Protocol which allows a client to get a file from or put a file onto a remote host.
- FTP is similar to TFTP, but requires user authentication

Feature details / Application notes

- Software Information on Startup, Running and Backup images
  - Version
  - Date created
  - Size of the software file
  - Source (where it was loaded from)
  - Date downloaded (installed)
- Software update : update the switch with new software and backing up the existing firmware.
- Revert to Backup: change software to the Backup software stored locally on the switch
- Backup and Restore with external file services such as TFTP
- The firmware can also be restored from a microSD on those IDS switch models with SD card capability

Configuration

Software Update

Activity	Web Manager	CLI Command(s)	Comments

Update switch software using a browser	Administration/File Management/ Software/Software Update/Browser	N/A	After downloading the latest software from the Perle web site @ https:// www.perle.com/ downloads/ , the user can use their browser to download to the switch by clicking the "Update Software" button on the Software Update page. The replaced "Startup" software will then be saved as the "Backup" which can be used to revert back to this version if required. The "Running" image will remain at the existing version until a reboot is performed at which time it will load the new "Startup" software
Update switch software posted on an external FTP server	Administration/File Management/ Software/Software Update/FTP	#archive download-sw |*ftp:[[// username[:password]@location]/ directory]/perle-image-name.img}*	On FTP tab on web manager page enter; · host name or IP address of the FTP server on the network · path name · user name and password credentials

Update switch software posted on an external HTTP server	Administration/File Management/ Software/Software Update/HTTP	#archive download-sw |http:// [[username:password]@][hostname | host-ip [directory] /perle-image-name.img	On HTTP tab on web manager page enter; · host name or IP address of the HTTP server on the network · path name · user name and password credentials
Update switch software posted on an external HTTPS server	Administration/File Management/ Software/Software Update/HTTPS	#archive download-sw |https:// [[username:password]@][hostname | host-ip [directory] /perle-image-name.img	On HTTPS tab on web manager page enter; · host name or IP address of the HTTPS server on the network · path name · user name and password credentials
Update switch software posted on an external SCP server	Administration/File Management/ Software/Software Update/SCP	#archive download-sw |scp:[[username@location]/directory]/perle-image-name.img	On SCP tab on web manager page enter; · host name or IP address of the SCP server on the network · path name · user name and password credentials
Update switch software posted on an external SFTP server	Administration/File Management/ Software/Software Update/SFTP	#archive download-sw |sftp:[[//username[:password]@location]/directory]/perle-image-name.img	On SFTP tab on web manager page enter; · host name or IP address of the SFTP server on the network · path name · user name and password credentials

Update switch software posted on an external TFTP server	Administration/File Management/ Software/Software Update/TFTP	#archive download-sw |tftp:[[//location]/directory]/perle-image-name.img	On TFTP tab on web manager page enter; · host name or IP address of the TFTP server on the network · path name
Update switch software posted on an SD card	Administration/File Management/ Software/Software Update/SD	#archive download-sw |sdflash:[//directory]/perle-image-name.img	On SD tab on web manager page enter; · path name on SD card

Revert to Backup Software

Activity	Web Manager	CLI Command(s)	Comments
Revert to Backup software	Administration/File Management/ Software/Software Information	#boot system backup	This action will cause the "Backup" software stored locally on the switch to overwrite the "Startup" firmware. After confirmation, a reboot is required

Backup and Restore Software

Activity	Web Manager	CLI Command(s)	Comments

Backup and restore software using a browser	Administration/File Management/ Software/Backup / Restore Software/ Browser	N/A	Software on the switch can be backed to a PC workstation using an internet browser by providing a path to where the software image file is to be stored and then clicking on the "Backup Software" button on the Administration/File Management/Software/Backup / Restore Software/Browser page Restoration is performed by providing a path to where the backed up software image is located on the PC workstation and then clicking on the "Restore Software" button

Backup and restore Software with an external FTP server	Administration/File Management/ Software/Backup / Restore Software/FTP	#archive upload-sw *|ftp:[[// username[:password] @location]/directory]/ perle-image-name.img}*
		
		#archive download-sw *|ftp:[[// username[:password] @location]/directory]/ perle-image-name.img}*
			On FTP tab on web manager page enter;
			Backup
			· host name or IP address of the FTP server on the network
			· path name
			· user name and password credentials
			· Click "Backup Software" button
			
			Restore
			· host name or IP address of the FTP server on the network
			· path name
			· user name and password credentials
			· Click "Restore Software" button

Backup and restore Software with an external HTTP server	Administration/File Management/ Software/Backup / Restore Software/ HTTP	#archive upload-sw |http:// [[username:password] @][hostname | host-ip [directory] /perle-image-name.img #archive download-sw |http:// [[username:password] @][hostname | host-ip [directory] /perle-image-name.img	On HTTP tab on web manager page enter; **Backup** · host name or IP address of the HTTP server on the network · path name · user name and password credentials · Click "Backup Software" button **Restore** · host name or IP address of the HTTP server on the network · path name · user name and password credentials · Click "Restore Software" button

Backup and restore Software with an external HTTP server	Administration/File Management/ Software/Backup / Restore Software/ HTTPS	#archive upload-sw |https://[[username:password]@][hostname | host-ip [directory]/perle-image-name.img #archive download-sw |https://[[username:password]@][hostname | host-ip [directory]/perle-image-name.img	On HTTPS tab on web manager page enter; **Backup** · host name or IP address of the HTTPS server on the network · path name · user name and password credentials · Click "Backup Software" button **Restore** · host name or IP address of the HTTPS server on the network · path name · user name and password credentials · Click "Restore Software" button

Backup and restore Software with an external SCP server	Administration/File Management/ Software/Backup / Restore Software/SCP	#archive upload-sw |scp:[[username@location]/directory]/ perle-image-name.img #archive download-sw |scp:[[username@location]/directory]/ perle-image-name.img	On SCP tab on web manager page enter; **Backup** · host name or IP address of the SCP server on the network · path name · user name and password credentials · Click "Backup Software" button **Restore** · host name or IP address of the SCP server on the network · path name · user name and password credentials · Click "Restore Software" button

Backup and restore Software with an external SFTP server	Administration/File Management/ Software/Backup / Restore Software/ SFTP	#archive upload-sw |sftp:[[//username[:password]@location]/directory]/perle-image-name.img #archive download-sw |sftp:[[//username[:password]@location]/directory]/perle-image-name.img	On SFTP tab on web manager page enter; **Backup** · host name or IP address of the SFTP server on the network · path name · user name and password credentials · Click "Backup Software" button **Restore** · host name or IP address of the SFTP server on the network · path name · user name and password credentials · Click "Restore Software" button
Backup and restore Software with an external TFTP server	Administration/File Management/ Software/Backup / Restore Software/ TFTP	#archive upload-sw |tftp:[[//location]/directory]/perle-image-name.img #archive download-sw |tftp:[[//location]/directory]/perle-image-name.img	On TFTP tab on web manager page enter; **Backup** · host name or IP address of the TFTP server on the network · path name · Click "Backup Software" button **Restore** · host name or IP address of the TFTP server on the network · path name · Click "Restore Software" button

Backup and restore Software with an SD card	Administration/File Management/ Software/Backup / Restore Software/SD	#archive upload-sw |sdflash:[//directory]/ perle-image-name.img #archive download-sw |sdflash:[//directory]/ perle-image-name.img	On SD tab on web manager page enter; **Backup** · path name on SD card · Click "Backup Software" button **Restore** · path name on SD card · Click "Restore Software" button *This capability is available on the IDS-306, all IDS-409 and IDS-509 series models and the IDS-509PP series*

Monitoring and Maintaining

Activity	Web Manager	CLI Command(s)	Comments
Show software information	Administration/File Management/ Software/Software Information	#show sysinfo	· Displays the version and build dates for the Startup, Running and Backup software images
Show software version of Startup Software	Administration/File Management/ Software/Software Information	#show version	· Displays the version and build date for the Startup software image and whether the password-recovery mechanism is enabled or not

5.2 - Configuration Management

Overview

This section describes how to manage configuration files on Perle IDS switches.

The “startup-config” file is the file used to load the switch configuration details at boot time. This file which is text-based, can be modified using common text editors and then downloaded directly to the switch. This file can also be retrieved from an external TFTP, SFTP, FTP, HTTP, HTTPS or SCP server.

If the IDS model has an SD flash capability, the “startup-config” file can also be loaded onto a microSD card and inserted into the switch for direct copying.

PerleView, an enterprise-grade centralized Microsoft Server-based management program can also be used to manage config file downloads across a large number of IDS Managed Switches. See “PerleView” for details

Pre-requisites

- TFTP, SFTP, FTP, HTTP, HTTPS or SCP server for downloading/uploading files
-

Restrictions / Limitations

- None

Terminology

- SCP (Secure Copy Protocol) uses Secure Shell (SSH) for data transfer, authentication and encryption.
- TFTP (Trivial File Transfer Protocol is a common File Transfer Protocol which allows a client to get a file from or put a file onto a remote host.
- SFTP (Secure File Transfer Protocol) is a common File Transfer Protocol which allows a client to get a file from or put a file onto a remote host
- FTP is similar to TFTP, but requires user authentication.
- “running-config” is the configuration file that is executing on the switch.

Feature details / Application notes

- Backup and restore configuration file
- Merge configuration: Merge a file to configuration. Both running configuration and startup configuration will be updated.
- Configuration archiving
- Auto-Configuration Rollback:used to restore the switch to a previously known operating environment after a running-config change
- Replace configuration: replace the existing configuration file and then rollback on condition of an error or after a specified period of time.
- Lock Configuration
- Boot DHCP configuration file

Configuration

Backup and Restore configuration file

Activity	Web Manager	CLI Command(s)	Comments
Backup and restore configuration using a browser	Administration/File Management/ Configuration/ Backup / Restore / Browser	N/A	Configuration on the switch can be backed to a PC workstation using an internet browser by providing a path to where the file is to be stored and then clicking on the "Backup Configuration" button on the Administration/File Management/Configuration/ Backup / Restore Software/ Browser page Restoration is performed by providing a path to where the backed up configuration file is located on the PC workstation and then clicking on the "Restore Configuration" button

Backup and restore Configuration with an external FTP server	Administration/File Management/ Configuration/ Backup / Restore/ FTP	#copy startup-config |*ftp:[[//username[:password]@location]/directory]/configfilename* #copy |*ftp:[[//username[:password]@location]/directory]/configfilename* startup-config	On FTP tab on web manager page enter; **Backup** · host name or IP address of the FTP server on the network · path name · user name and password credentials · Click "Backup Configuration" button **Restore** · host name or IP address of the FTP server on the network · path name · user name and password credentials · Click "Restore Configuration" button

Backup and restore Configuration with an external HTTP server	Administration/File Management/ Configuration/ Backup / Restore/ HTTP	#copy startup-config |http:// [[username:password]@] [hostname | host-ip [directory] /*configfilename* #copy |http:// [[username:password]@] [hostname | host-ip [directory] /*configfilename* startup-config	On HTTP tab on web manager page enter; **Backup** · host name or IP address of the HTTP server on the network · path name · user name and password credentials · Click "Backup Configuration" button **Restore** · host name or IP address of the HTTP server on the network · path name · user name and password credentials · Click "Restore Configuration" button

Backup and restore Configuration with an external HTTPS server	Administration/File Management/ Configuration/ Backup / Restore/ HTTPS	#copy startup-config |https:// [[username:password]@] [hostname | host-ip [directory] */configfilename* #copy |https:// [[username:password]@] [hostname | host-ip [directory] */configfilename* startup-config	On HTTPS tab on web manager page enter; **Backup** · host name or IP address of the HTTPS server on the network · path name · user name and password credentials · Click "Backup Configuration" button **Restore** · host name or IP address of the HTTPS server on the network · path name · user name and password credentials · Click "Restore Configuration" button

Backup and restore Configuration with an external SCP server	Administration/File Management/ Configuration/ Backup / Restore/ SCP	#copy startup-config |scp:[[username @location]/directory]/ *configfilename* #copy |scp:[[username@location]/directory]/ *configfilename* startup-config	On SCP tab on web manager page enter; **Backup** · host name or IP address of the SCP server on the network · path name · user name and password credentials · Click "Backup Configuration" button **Restore** · host name or IP address of the SCP server on the network · path name · user name and password credentials · Click "Restore Configuration" button

Backup and restore Configuration with an external SFTP server	Administration/File Management/ Configuration/ Backup / Restore/ SFTP	#copy startup-config |sftp:[[//username[:password]@location]/directory]/ *configfilename* #copy |sftp:[[//username[:password]@location]/directory]/ *configfilename* startup-config	On SFTP tab on web manager page enter; **Backup** · host name or IP address of the SFTP server on the network · path name · user name and password credentials · Click "Backup Configuration" button **Restore** · host name or IP address of the SFTP server on the network · path name · user name and password credentials · Click "Restore Configuration" button

Backup and restore Configuration with an external TFTP server	Administration/File Management/ Configuration/ Backup / Restore/ TFTP	#copy startup-config |tftp:[[//location]/ directory]/ *configfilename* #copy |tftp:[[//location]/ directory]/ *configfilename* startup-config	On TFTP tab on web manager page enter; **Backup** · host name or IP address of the TFTP server on the network · path name · Click "Backup Configuration" button **Restore** · host name or IP address of the TFTP server on the network · path name · Click "Restore Configuration" button
Backup and restore Configuration with an SD card	Administration/File Management/ Configuration/ Backup / Restore/ SD	#copy startup-config |sdflash:[//directory]/ *configfilename* #copy |sdflash:[//directory]/ *configfilename* startup-config	On SD tab on web manager page enter; **Backup** · path name on SD card · Click "Backup Configuration" button **Restore** · path name on SD card · Click "Restore Configuration" button

Merge Configuration

Activity	Web Manager	CLI Command(s)	Comments

Merge a file to configuration using a browser. Both running configuration and startup configuration will be updated	Administration/File Management/ Configuration/Merge Configuration/Browser	N/A	Click "Merge Configuration" button to merge a file to configuration. Both running configuration and startup configuration will be updated.
Merge a file from an external FTP server to configuration . Both running configuration and startup configuration will be updated	Administration/File Management/ Configuration/Merge Configuration/FTP	#config replace |*ftp:[[// username[:password]@location]/directory]/ configfilename* # copy running-config startup-config	On FTP tab on web manager page enter; · host name or IP address of the FTP server on the network · path name · user name and password credentials · Click "Merge Configuration" button
Merge a file from an external HTTP server to configuration . Both running configuration and startup configuration will be updated	Administration/File Management/ Configuration/Merge Configuration/HTTP	#config replace |*http:[[// username[:password]@location]/directory]/ configfilename* # copy running-config startup-config	On HTTP tab on web manager page enter; · host name or IP address of the HTTP server on the network · path name · user name and password credentials · Click "Merge Configuration" button

Merge a file from an external HTTPS server to configuration . Both running configuration and startup configuration will be updated	Administration/File Management/ Configuration/Merge Configuration/HTTPS	#config replace |*https:[[// username[:password]@location]/directory]/ configfilename* # copy running-config startup-config	On HTTPS tab on web manager page enter; · host name or IP address of the HTTPS server on the network · path name · user name and password credentials · Click "Merge Configuration" button
Merge a file from an external SCP server to configuration . Both running configuration and startup configuration will be updated	Administration/File Management/ Configuration/Merge Configuration/SCP	#config replace |*scp:[[// username[:password]@location]/directory]/ configfilename* # copy running-config startup-config	On SCP tab on web manager page enter; · host name or IP address of the SCP server on the network · path name · user name and password credentials · Click "Merge Configuration" button
Merge a file from an external SFTP server to configuration . Both running configuration and startup configuration will be updated	Administration/File Management/ Configuration/Merge Configuration/SFTP	#config replace |*sftp:[[// username[:password]@location]/directory]/ configfilename* # copy running-config startup-config	On SFTP tab on web manager page enter; · host name or IP address of the SFTP server on the network · path name · user name and password credentials · Click "Merge Configuration" button

Merge a file from an external TFTP server to configuration . Both running configuration and startup configuration will be updated	Administration/File Management/ Configuration/Merge Configuration/TFTP	#config replace |tftp:[[//location]/ directory]/*configfilename* # copy running-config startup-config	On TFTP tab on web manager page enter; · host name or IP address of the TFTP server on the network · path name · Click "Merge Configuration" button
Merge a file from the internal flash on the switch to configuration . Both running configuration and startup configuration will be updated	Administration/File Management/ Configuration/Merge Configuration/Internal Flash	#config replace |flash:[[//location]/ directory]/*configfilename* # copy running-config startup-config	On Internal Flash tab on web manager page enter; · path name on flash: · Click "Merge Configuration" button
Merge a file from the internal SD card on the switch to configuration . Both running configuration and startup configuration will be updated	Administration/File Management/ Configuration/Merge Configuration/SD card	#config replace |sdflash:[[//location]/ directory]/*configfilename* # copy running-config startup-config	On SD Card tab on web manager page enter; · path name on SDflash: · Click "Merge Configuration" button

Configuration Archiving

This feature enables the user to make changes to the running config and have these changes archived automatically.

To retrieve and use a specific archived file, use the "restore config" file function detailed above

Activity	Web Manager	CLI Command(s)	Comments

Enable configuration archive creation and direct to a file location	Administration/File Management/ Configuration/Archives	(config-archive)#path	After checking "Enable configuration archive creation" box, specify a path and filename. Path choices are; · flash: · ftp: · http: · https: · scp: · sftp: · tftp:
Set maximum number of saved configurations	Administration/File Management/ Configuration/Archives	(config-archive)#maximum	Set maximum number of saved configurations (1 to 14). The default is 10
Set the frequency of configuration saves	Administration/File Management/ Configuration/Archives	(config-archive)#time-period	Set the frequency of configuration saves in minutes (0 to 525600). The default is 0
Create archive when running configuration is saved	Administration/File Management/ Configuration/Archives	(config-archive)#path	Archives the running-config file each time is saved

Auto-Configuration Rollback

This feature is used to restore the switch to a previously known operating environment in the event that the new configuration change to the running-config prevents the administrator from accessing the unit (i.e. change the IP address to an address that is not reachable from the location the administrator is at).

Activity	Web Manager	CLI Command(s)	Comments

Set Rollback configuration	Administration/File Management/ Configuration/Rollback	#configure terminal revert timer Or #configure terminal revert idle	Check the Rollback configuration timer in minutes (1 to 120). Default has no value Or Check the Rollback configuration based on an idle timer of the existing user:admin
Lock Configuration	Administration/File Management/ Configuration/Rollback	#configure terminal lock	Lock - will prevent other users from being able to go into configuration mode.

Replace Configuration

Allows the user to replace the existing running configuration with a version which was previously saved using the archive function or one that was created

Activity	Web Manager	CLI Command(s)	Comments
Replace configuration using an internet browser	Administration/File Management/Replace/ Browser	N/A	Replace the configuration file with another via the internet browser
Replace configuration from an FTP server	Administration/File Management/Replace/ FTP	#configure replace |ftp:filename revert trigger error #configure replace |ftp:filename revert trigger timer <1-120>	Replace configuration file with file from an FTP server and rollback if there is a an during configuration processing Replace configuration file with file from an FTP server and rollback when timer expires (1 to 120 minutes)

Replace configuration from an HTTP server	Administration/File Management/Replace/ HTTP	#configure replace |http:filename revert trigger error #configure replace |http:filename revert trigger timer <1-120>	Replace configuration file with file from an HTTP server and rollback if there is a an during configuration processing Replace configuration file with file from an HTTP server and rollback when timer expires (1 to 120 minutes)
Replace configuration from an HTTPS server	Administration/File Management/Replace/ HTTPS	#configure replace |https:filename revert trigger error #configure replace |https:filename revert trigger timer <1-120>	Replace configuration file with file from an HTTPS server and rollback if there is a an during configuration processing Replace configuration file with file from an HTTPS server and rollback when timer expires (1 to 120 minutes)
Replace configuration from an SCP server	Administration/File Management/Replace/ SCP	#configure replace |scp:filename revert trigger error #configure replace |scp:filename revert trigger timer <1-120>	Replace configuration file with file from an SCP server and rollback if there is a an during configuration processing Replace configuration file with file from an SCP server and rollback when timer expires (1 to 120 minutes)
Replace configuration from an SFTP server	Administration/File Management/Replace/ SFTP	#configure replace |sftp:filename revert trigger error #configure replace |sftp:filename revert trigger timer <1-120>	Replace configuration file with file from an SFTP server and rollback if there is a an during configuration processing Replace configuration file with file from an SFTP server and rollback when timer expires (1 to 120 minutes)

Replace configuration from an TFTP server	Administration/File Management/Replace/ TFTP	#configure replace |tftp:filename revert trigger error #configure replace |tftp:filename revert trigger timer <1-120>	Replace configuration file with file from an TFTP server and rollback if there is a an during configuration processing Replace configuration file with file from an TFTP server and rollback when timer expires (1 to 120 minutes)
Replace configuration from the internal flash	Administration/File Management/Replace/ Internal Flash	#configure replace |flash:filename revert trigger error #configure replace |flash:filename revert trigger timer <1-120>	Replace configuration file with file from the switch's internal flash and rollback if there is a an during configuration processing Replace configuration file with file from the switch's internal flash and rollback when timer expires (1 to 120 minutes)
Replace configuration from the SD card	Administration/File Management/Replace/ SD Card	#configure replace |sdflash:filename revert trigger error #configure replace |sdflash:filename revert trigger timer <1-120>	Replace configuration file with file from the switch's SD card and rollback if there is a an during configuration processing Replace configuration file with file from the switch's SD card and rollback when timer expires (1 to 120 minutes) *SD card slots are provided on IDS Switch on the IDS-306 and all IDS-409/509 including IDS-509 PoE models*

Lock

Lock - will prevent other users from being able to go into configuration mode.

Activity	Web Manager	CLI Command(s)	Comments

Lock out all other users from configuring the switch	Administration/File Management/Lock	#configure terminal lock	Click the "Lock Configuration" button
Unlock	Administration/File Management/Lock	Exit configure mode	Click the "Unlock Configuration" button

Boot File

Enable the downloading of the configuration file using DHCP/BOOTP on the next reboot

Activity	Web Manager	CLI Command(s)	Comments
Enable the downloading of the configuration file using DHCP/BOOTP on the next reboot	Administration/File Management/Boot File	(config)#boot host dhcp (config)#no boot host dhcp (config)#boot host retry timeout	Enable loading of the config file via DHCP on the next reboot. Disable loading of the config file via DHCP on the next reboot. Specifies the amount of time between retries; valid values are between 60 and 65,535 seconds.

5.3 - File Transfer Settings

Overview

- Enables the user to configure global file transfer parameters for use with external file servers.

Pre-requisites

- None

Restrictions / Limitations

- None

Terminology

Feature details / Application notes

- Configure parameters for FTP server
- Configure parameters for HTTP server
- Configure parameters for HTTPS server

- Configure parameters for SCP server
- Configure parameters for SFTP server

Configuration

Activity	Web Manager	CLI Command(s)	Comments
Configure FTP client	Administration/File Transfer Settings/FTP	(config)#ip ftp username (config)#ip ftp password (config)#ip ftp passive	· Configure FTP Username · Configure FTP Password · Indicate to the FTP server that the client will be opening the file transfer session (default)
Configure HTTP client	Administration/File Transfer Settings/HTTP	(config)#ip http client username (config)#ip http client password (config)# ip http client proxy-server *proxy-name* proxy-port *port-number*	· Configure HTTP Username · Configure HTTP Password · Configure an HTTP proxy server (port number range is 1 - 65535)

Configure HTTPS client	Administration/File Transfer Settings/HTTP/ HTTPS	(config)#ip http client username (config)#ip http client password (config)# ip http client proxy-server *proxy-name* proxy-port *port-number* | secure trustpoint *name*	· Configure HTTP Username · Configure HTTP Password · Configure an HTTP proxy server (port number range is 1 - 65535) · For HTTPS, specific secure trustpoint (refer to “Keys and Certificates” "
Configure SCP client	Administration/File Transfer Settings/SCP	(config)#ip scp username (config)#ip scp password	· Configure SCP Username · Configure SCP Password
Configure SFTP client	Administration/File Transfer Settings/SFTP	(config)#ip sftp username (config)#ip sftp password	· Configure SFTP Username · Configure SFTP Password

5.4 - Exporting Flash Files

Overview

Files such as the archived config and logging files stored on the switch's flash can be exported for viewing or posterity purposes.

Pre-requisites

- TFTP, FTP, HTTP, SFTP, HTTPS or SCP server for exporting files (if not using the “browser” option).

Restrictions / Limitations

- None.

Features details / Application notes

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

Configuration

Activity	Web Manager	CLI Command(s)	Comments
Export flash file to PC via web browser	Administration/File Management/Export Flash Files/Browser	N/A	Export a file that resides in the switch's flash: to a workstation using an internet browser
Export flash file to FTP server	Administration/File Management/Export Flash Files/FTP	#copy flash:*flashfilename* |*ftp:[[// username[:password]@location]/directory]/flashfilename*	On FTP tab on web manager page enter ; · host name or IP address of the FTP server on the network · path name · user name and password credentials · Click "Export from flash" button
Export flash file to HTTP server	Administration/File Management/Export Flash Files/HTTP	#copy flash:*flashfilename* |*http:[[// username[:password]@location]/directory]/flashfilename*	On HTTP tab on web manager page enter ; · host name or IP address of the HTTP server on the network · path name · user name and password credentials · Click "Export from flash" button

Export flash file to HTTPS server	Administration/File Management/Export Flash Files/HTTPS	#copy flash:*flashfilename* |*https:[[//username[:password]@location]/directory]/flashfilename*	On HTTPS tab on web manager page enter ; · host name or IP address of the HTTPS server on the network · path name · user name and password credentials · Click "Export from flash" button
Export flash file to SCP server	Administration/File Management/Export Flash Files/SCP	#copy flash:*flashfilename* |*scp:[[//username[:password]@location]/directory]/flashfilename*	On SCP tab on web manager page enter ; · host name or IP address of the SCP server on the network · path name · user name and password credentials · Click "Export from flash" button
Export flash file to SFTP server	Administration/File Management/Export Flash Files/SFTP	#copy flash:*flashfilename* |*sftp:[[//username[:password]@location]/directory]/flashfilename*	On SFTP tab on web manager page enter ; · host name or IP address of the SFTP server on the network · path name · user name and password credentials · Click "Export from flash" button
Export flash file to TFTP server	Administration/File Management/Export Flash Files/TFTP	#copy flash:*flashfilename* |*tftp:[[//location]/directory]*	On TFTP tab on web manager page enter ; · host name or IP address of the FTP server on the network · path name · Click "Export from flash" button

5.5 - Transfer System Recovery Files to an SD Card

Overview

- This feature is designed for a service/replacement scenario where the user loads an SD card with the System Recovery files for the purposes of replacing the switch with the same configuration and software. Typically the new switch is in a factory default state. By placing the SD card in the replacement switch, the new switch will operate with the same configuration and/or software of the unit that has been replaced.
- Unit has to be operating in order to restore the software and/or configuration.

Pre-requisites

- MicroSD slots are not available on all models. Refer to specifications of the specific model.
- A MicroSD card properly inserted in the SD card slot (refer to the IDS Hardware Installation guide for more details)

Feature details / Application notes

- Create a recovery disk of both configuration and firmware
- Create a recovery disk for firmware only
- Create a recovery disk for configuration only

Configuration

- THIS FEATURE IS NOT INTENDED FOR DISASTER RECOVERY. Unit has to be in proper working order to restore the software and/or configuration.

Activity	Web Manager	CLI Command(s)	Comments
Create a recovery disk including both configuration and firmware files	Administration/File Management/SD Card/ Recovery Disk	#sync flash:sdflash	· Copies both the firmware image and the startup-config file
Create a recovery disk with firmware image	Administration/File Management/SD Card/ Recovery Disk	#sync flash: sdflash: skip config	· Only copies the firmware image
Create a recovery disk with configuration file	Administration/File Management/SD Card/ Recovery Disk	#sync flash: sdflash skip image	· Only copies the startup-config file ·

5.6 - Keys and Certificates

Overview

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

Terminology

Strict Host Checking

- This causes a client attempting to establish an SSH or HTTPS connection to a server to validate the identify of that server using keys or certificates. If the server fails to authenticate using this method, the connection is not established.

Feature details / Application notes

We support the following certificates/keys in the switch

- HTTPS Certificate
  - o This is our Server HTTPS certificate. It identifies us to clients who HTTPS to the switch.
  - o We include a self-signed certificate with the switch.
  - o User can download their own certificate which correctly identifies their switch and may

be signed by a signing authority such as Symantec.

- Server SSH key
    - This key is used to identify the server when a client connects via SSH to the switch.
    - The key is an RSA key.
    - When the switch boots, if there is no SSH server key present, one is automatically generated.
        - We generate an SSH2 and SSH1 key.
        - The SSH1 key cannot be manipulated in the switch (i.e. no ability to delete, export or import the key).
    - The user can optionally import their own key if they wish to.
    - The public portion of the key can be exported from the switch so that it can be put on SSH clients who are using "strict host key checking". This requires them to have a host key for any server they wish to SSH to.
    - The private portion of the key can be exported as well. This can be done to backup this key. If the original switch is reset to factory default or is replaced, this key can be downloaded to the switch so that the SSH clients see the same SSH host as before.
        - Only the private key is saved. The public portion can always be generated from the private portion so it does not need to be saved.
        - To protect the private key, if you export it out of the switch, you must enter a "Passphrase" which is used to encrypt the key. This passphrase is required when restoring the key to the switch and protects if from unauthorized usage.
- SSH Host keys
    - If the switch attempts an SSH session to an SSH server and "strict host checking" is enabled, there needs to be an SSH host key for this host present on the switch.
    - This is the "public" portion of the SSH host key
    - This is used for SSH2
    - The key needs to be an RSA key in OpenSSH format.
- SSH User keys
    - SSH clients can choose "key" authentication. If this is the case, each user needs to have a key on the switch which identifies them.
    - This is used for SSH2 clients.
    - The key needs to be an RSA key in OpenSSH format.
- Server CA Certificate
    - This is used when we perform an HTTPS file transfer to an HTTPS host.
    - It can also be used to identify a Radius authentication server to the switch when the port is acting as an 802.1x supplicant.
    - The CA certificate is used to validate certificates presented by the HTTPS host.
    - The CA certificate is given a name ("trustpoint"). This is the name used to associate the CA with file transfer operations or 802.1x supplicants.
- SSL Client key
    - Used by 802.1x supplicant

- The key is used to encrypt the data exchange between the suppliant and the RADIUS host.
- This is a global client key which is used as the credentials for the switch.
- The user imports the public key into our switch.

- SSL Client Certificate?
  - Used by 802.1x supplicant
  - The certificate is used by the ADIUS host to validate that we are who we say we are.
  - This is a global client certificate which is used as the credentials for the switch.
  - The user imports the certificate into our switch.

Monitoring and Maintaining

- **Managing the HTTPS Certificate.**

  oThis is the certificate which identifies our switch to clients which use HTTPS to access our switch and need the certificate to validate our identity.

  oThe switch is shipped with a generic certificate signed by Perle Systems Limited. This certificate can be replaced by a certificate which contains specific information and is signed by an authorized certificate authority.

Activity	Web Manager	CLI Command(s)	Comments
Import the Server Certificate	HTTPS Certificate	(config)#cryptopki import https <pem | pkcs12> <terminal | url > <password>	· Use the "crypto pki import https ...." command · Indicate the format of the certificate. · Indicate whether you will use the terminal (type or paste the certificate) or file transfer from a url. · If the certificate was encrypted using a passphrase, it must be entered here.
Deleting the server certificate	Only via CLI.	(config)#cryptopki zeroize https	· This will remove the certificate associated the HTTPS server on the switch.

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

Activity	Web Manager	CLI Command(s)	Comments
Export an SSH server key for use on SSH client.	Server SSH Key (export **public** key function)	(config)#icrypto key export rsa public Terminal url	· Pick the public key · Use the CLI terminal session to paste (or type) the key data. · Use a file transfer to obtain the key.
Export an SSH server key for safe keeping.	Server SSH Key (export **private** key function)	(config)#icrypto key export rsa Terminal url <des | 3des> passphrase	· Pick the private key · Select destination as the CLI terminal session · Select file transfer mode for destination · In either case above, the private key must be encrypted to protect its contents from unauthorized access. ·Select algorithm to use to encrypt the private key. ·Select a passphrase. This will be required when restoring the key to the switch.

Restore an SSH server key.	Server SSH Key (import **private** Server SSH key)	(config)#crypto key import ssh-host rsa Terminal url passphrase	· Restore the private SSH server key · Select source as the CLI terminal session · Select file transfer mode for source · If the SSH server key is protected by a passphrase (forced if originally exported from the switch) it must be entered here.
Generate an SSH server key.	Server SSH Key (Gemerate Server SSH key button)	(config)#icrypto key generate rsa modulus <*number of bits*>	· Generate a new SSH server key. · Replaces existing key. · User can specify the length of the key in number of bits. The longer, the more secure.

- **Managing SSH user keys.**

oThis is the ability for the user to import SSH client public keys. If the SSH client chooses "key" authentication, this would be the key which is used to authenticate the client when they SSH to the switch.

Activity	Web Manager	CLI Command(s)	Comments
Import an SSH user key	SSH User Keys	(config)#ip ssh pubkey-chain (config-ssh-pubkey)#user-name <user> (config-ssh-pubkey-user)#key-string (config-ssh-pubkey-data)#<key text> (config-ssh-pubkey-data)#exit (config-ssh-pubkey-user)#	· Go into the public key command tree · Enter the name of the user to which this key is for. · Enter the "key data" entry mode. · Type or paste the actual key text here. · Enter "exit" on a new line to exit key entry mode. · At this point you can enter another user name or exit if done.
Deleting an SSH user key	SSH User Keys	(config)#ip ssh pubkey-chain (config-ssh-pubkey)#no username <user>	· Go into the public key command tree · Use the no option in front of "username" to remove the key associated with this user.

- **Managing SSH host keys.**

oThis is the ability for the user to import SSH host keys of servers which they will be establishing an SSH session with. The keys are used to validate the identify of these servers.

Activity	Web Manager	CLI Command(s)	Comments
Import an SSH host key	SSH Host Keys	(config)#ip ssh pubkey-chain (config-ssh-pub-key)#server <name | ip addr> (config-ssh-pubkey-server)#key-string (config-ssh-pubkey-data)#<key text> (config-ssh-pubkey-data)#exit	· Go into the public key command tree · Enter the name of the host or an IP address. If name is used, it must be resolvable to an IP address via the host table or DNS lookup. · Enter the "key data" entry mode. · Type or paste the actual key text here. · Enter "exit" on a new line to exit key entry mode. · At this point you can enter another server name or exit if done.
Deleting an SSH host key	SSH Host Keys	(config)#ip ssh pubkey-chain (config-ssh-pubkey)#no server <name | ip addr>	· Go into the public key command tree · Use the no option in front of "server" to remove the key associated with this server.

- **Managing Server CA Certificate.**

  oThis is used to validate HTTPS certificates presented by hosts which we perform HTTPS transfers to/from.

  oIt can also be used to validate the Radius authentication server if the switch is acting as an 802.1x supplicant.

Activity	Web Manager	CLI Command(s)	Comments
Import a CA Certificate	Server CA Certificates	(config)#crypto pki import server <ca | trustpoint name> <pem | pkcs12> <terminal | url > <password>	· Use the "crypto pki i mport server ...." command · Enter the name "Trustpoint" which will be used to reference this certificate in the switch. · Indicate the format of the certificate. · Indicate whether you will use the terminal (type or paste the certificate) or file transfer from a url. · If the certificate was encrypted using a passphrase, it must be entered here.

Associating a trustpoint with the HTTPS client	File Transfer Settings <HTTP/HTTPS tab> "Secure Trustpoint"	(config)#ip http client secure-trustpoint <trustpoint>	· Enter the trustpoint name (certificate) you wish to user for HTTPS file transfers. · This is global to all HTTPS file transfers.
Enable server validation	File Transfer Settings <HTTP/HTTPS tab> "Validate server certificate"	(config)#ip http client verify-server	· Enabling this option will cause the switch to validate the certificate presented by the HTTPS host we are performing the file transfer with.
Deleting a trustpoint	Server CA Certificates	(config)#crypto pki zeroize server <trustpoint>	· This will remove the CA certificate associated with the named trustpoint.

- **Managing SSL Client Keys.**

oKey pair is generated externally to the switch and the public portion of the key is imported to the switch.

Activity	Web Manager	CLI Command(s)	Comments
Import a Client SSL key	SSL Client Key	(config)#crypto key import client rsa <pem | pkcs12> <terminal | url > <password>	· Use the "crypto pki import client ...." command · Indicate the format of the key. · Indicate whether you will use the terminal (type or paste the key) or file transfer from a url. · If the key was encrypted using a passphrase, it must be entered here.
Deleting a Client SSL Key			· Can't delete a client SSL key. Can only overwrite an existing one.

- **Managing SSL Client Certificate.**

oThe certificate is imported to the switch from an external source.

Activity	Web Manager	CLI Command(s)	Comments
Import an SSL Client Certificate	SSL Client Certificate	(config)#cryptopki import client <pem | pkcs12> <terminal | url > <password>	· Use the "crypto pki import client ...." command · Indicate the format of the certificate. · Indicate whether you will use the terminal (type or paste the certificate) or file transfer from a url. · If the certifciate was encrypted using a passphrase, it must be entered here.

Deleting a Client SSL Certificate			· Can't delete a client SSL certificate. Can only overwrite an existing one.

6 - SNMP

6.1 - Overview

- Simple Network Management Protocol is a standard management protocol which can be used to monitor or configure all aspects of the switch.

6.2 - Pre-requisites

- None

6.3 - Restrictions / Limitations

- None

6.4 - Terminology

- **Communities**
  - These are used to define the access level to different groups.
- **Traps**
  - This is the message which SNMP uses to inform management software when an event has occurred on a managed entity.
    - Inform traps are traps which require acknowledgment from the receiver.
- **Inform**
  - Since SNMP operates over UDP, there is usually no guarantee that a message has been received by the intended recipient. Inform is a type of SNMP trap which requires the receiving host to acknowledge the fact that it has been received and therefore giving the sending entity a confirmation that the message was correctly received.
- **MIB**
- Management Information Base. This defines the parameters which SNMP can operate on.
  - o
-

6.5 - Configuration

- Configuring the SNMP parameters.

Activity	Web Manager	CLI Command(s)	Comments
Enable SNMP	System General Settings	(config)#snmp-server	Use the “no” version of the CLI command to disable SNMP. SNMP is enabled by default.

Set up the “Location” and “Contact” information	System General Settings	(config)#snmp-server Location contact	· SNMP-server command is used to configure SNMP attributes. · Defines the SNMP text string describing the SNMP location of the switch. · Max length = 32 characters · Defines the SNMP text string describing the SNMP contact of the switch. · Max length = 14 characters
Define the SNMP communities	SNMP Settings	(config)#snmp-server Community Name {IP access list | Extended IP access list} ro rw	· Define a community and its associated parameters. · Name of the community. · Max length = 63 characters. · Optionally can associate an IP access list with this community to control access via IP addresses. The access list can be a number or name. Extended is the same function as IP access, just uses a different range of numbers. · Give this community Read Only rights. · Give this community Read/ Write rights.
Configure trap information	SNMP Notifications	(config)#snmp-server enable traps	· Individually enable/disable what conditions would generate an SNMP trap. · Some notifications (i.e. authentication) also need to be enabled at the source before they will generate. · For authentication that would be the “(config)#login on-failure/on-success traps” command).
Enable link status trap	Switchport Settings	(config-if)#snmp trap link-status	· Turn on or off the sending of traps when a link on a port goes up/down.

Set trap host information	SNMP Notifications (host tab)	(config)#snmp-server host IP address Community UDP port Traps/informs Version	· Define the SNMP hosts to send traps to. · IPv4 or IPv6 address of host. · Community name to use. · UDP port the trap host is listening on. (default is 162) · Type of notification trap or inform. · Version of trap (v1 or v2c)
Set inform parameters	SNMP Notifications (Advanced tab)	(config)#snmp-server inform Retries Timeout	· Define the inform parameters. · · Number of time to re-try the inform if not acknowledged by the host. · Time to wait for host to acknowledge the inform.
Set maximum number of traps	SNMP Notifications (Advanced tab)	(config)#snmp-server queue-length	· Define the number of SNMP traps/informs which can be queued up for each trap host. · Range is 1 – 5000 · Default is 10

Define the SNMP V3 users	SNMPv3 Users	(config)#snmp-server user	· Add/modify an SNMP v3 user. ·
		<name>	· Name of the user on the SNMP host.
		<group>	· V3 Users must belong to a group.
		Remote	· Optional. Can specify the IP address or name of the host the user belongs to.
		Udp-port	· Can specify the UDP port number. Default is 162.
		V3	· Define the v3 security model.
		Encrypted	· Optional, specifies whether the passwords appear in encrypted format. This is the format in which they will be stored in the configuration files.
		Auth	· Define authentication method (MD5 or SHA) followed by the authentication password.
		Priv	· Define the encryption method as either AES or DES followed by the privacy password.
		access	· Associate an access list with this user.

Define an SNMP group	SNMPv3 Groups	(config)#snmp-server group <name> Access v3 { noauth | auth | priv} Notify Read Write	· Add/modify an SNMP group. · · Name of the group · Optionally can associate an IP access list with this group. · Indicates this is a v3 group using a V3 security model. · Defines the authentication scheme for the group. o noauth – No Authentication, no Privacy o auth – Authentication, no Privacy o priv – Authentication and Privacy · Assign a “notify” view to group. · Assign a “read” view to group. · Assign a “write” view to group.
Define an SNMP v3 view	SNMPv3 Views	(config)#snmp-server view <name> {Include | exclude} OIDs	· Add/modify an SNMP view. · · Name of this view. · One or more OIDs which can be included or excluded from the view.

Define an Engine ID	SNMP Engine ID	(config)#snmp-server engineID remote	· Used to define the local and remote engine IDs. · A remote engine ID is required when an SNMP version 3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.
		local	· The local SNMP engine ID is a unique string used to identify this device. You do not need to specify an engine ID for the device. A default string is generated using Perle’s enterprise number and the mac address of the switch.

7 - Security

7.1 - General

Security on the switch boils down to two main categories.

- Management access
  - Preventing unauthorized access to the switch management functions.
- Switch port access
  - Preventing unauthorized access to the network.

Management access security

- Involve securing the switch against unauthorized attempts to configure the operating parameters of the switch or to even monitor the current status of various aspects of the switch.
- Controlling access via;
  - Console port
    - Switch can be configured to require a login on the console.
  - Switch ports
    - To access management functions on the switch via an Ethernet port the user must use one of the following protocols;
      - Telnet
      - SSH
      - HTTP
      - HTTPS
      - SNMP
    - All of the above have configurable parameters which define what access is granted for each.

Switch port access

- For ways on how to limit/protect switch ports from unauthorized access see the following features;
  - Port Security
  - 802.1x

Authentication

- Authentication can be performed via any of the following methods;
  - Local user database
  - External TACACS+ server
  - External RADIUS server
- User can configure “strong password” option which enforces the configuration of passwords which are more complex and therefore deemed safer.

7.2 - Password Security

Overview

- This is the ability to define users and passwords in the switch.

Terminology

- **Secret**
  - Another word for password.
- **VTY** -Virtual TTY
  - This is a generic notation for Telnet or SSH sessions.
- **RADIUS**
  - Remote Authentication Dial-In User Services
- **TACACS+**
  - Terminal Controller Access Control System

Feature details / Application notes

- In order to manage the Perle IDS Switch, users have to login to the switch. One of the methods which can be used to login involve a username and password. The user database on the switch
- The user will be assigned one of two authorization levels.
  - User EXEC - Able to perform most monitoring functions but not allowed to perform configuration of switch.
  - Privileged EXEC - Is able to perform all supported operations on the switch.
- Passwords can be up to 25 characters long. Blank passwords are also supported.
- Passwords will be stored in the local database using MD5 encryption. This is a one way encryption scheme. There is no way to extract the clear password from the stored value. User password validation is performed by taking the password supplied by the user and encrypting it using the MD5 algorithm and comparing the result to the value stored in the database.
- When viewing the text configuration of the switch, the password will be displayed in its encrypted form in ASCII printable characters. A user can cut and past this information into the configuration of another switch. This allow the administrator to copy users from one switch to another without knowing what their passwords are.
- Password recovery
  - In cases where the user has forgotten the password, there is a procedure which allows them to recover/re-set the password without needing to go back to factory default. This allows the user to maintain the existing configuration of the switch.
  - In order to use this feature;
    - User must have physical access to the unit
    - "Password Recovery" has not been disabled via configuration.
      - If feature is disabled, the only recovery would be a reset to factory default.
  - The procedure is initiated exactly the same as "fast setup" See --> Fast Setup for details on how to initiate this process.

- Once the password recovery process has been initiated, user will be prompted for;
  - Enable password
  - Username
  - Password
- The username entered will be setup as a "Privileged EXEC" user.
- This information can be entered via the web browser or the console port.
- At this point, the new username, password and enable password can be used to gain full access to the unit.

- User lockout
  - The switch can be configured to "lockout" a user after a configured number of failed login attempts have occurred.
  - Once locked out, it required manual intervention by a "privileged EXEC" user to unlock the user.
  - Only "user EXEC" level users can get locked out.

Configuration

- **Setting up user authentication.**

Activity	Web Manager	CLI Command(s)	Comments
Set .Set requirement for users to login	AAA Settings	(config)#aaa authentication	
Optionally set authentication method for specific access.	Management Access --> method.	(config)#line {console | vty} exec	Select method. Requires authentication. Use the *no* version of the command to not require authentication.
Add users.	User Accounts	(config)#username	Define the username, password and authorization level.

- **Setting up login parameters.**

Activity	Web Manager	CLI Command(s)	Comments

Set login reporting	Login Setting	(config)#login {on-success on-failure CR log trap every	Define the action to take on successful and failed logins. Configure action for successful login. Configure action for failed login. Next parameter defines the action to be taken for above. This will cause both a log and snmp trap to be generated every time the above occurs. Indicates a log message will be generated. Indicates an “snmp trap” will be sent. Optionally, the user can enter how often this will be done using the “every” parameter. This will cause the action to be performed every xxx occurrences.
Set number of retries.	Login Settings	(config)#aaa authentication attempts login	Once this number is exceeded, the session will be dropped. Valid range is 1 to 25. Default value is 3.
Enable user lockout.	Login Settings	(config)#aaa local authentication attempts max-fail	When enabled, after configured number of failed attempts, the user will be prevented from logging into the switch. A successful login resets this counter. Valid range is 1-65535. Feature is disabled by default.

- **Setting up the Password Recovery feature.**
- This feature is enabled by default.

Step	Activity	Web Manager	CLI Command(s)	Comments

1	Disable the password recover feature.	Login Settings.	(config)#no service password-recovery	This disables the "password recovery" feature. If the username/password is not known, the only way to gain access to the switch when this feature is disabled is by resetting the switch to factory default.

Monitoring and Maintaining

- **Managing the lockout feature**

Activity	Web Manager	CLI Command(s)	Comments
Displaying locked out users	Locked-out Local Users	#show aaa local user lockout	Display all users which have been locked out of the switch
Resetting the number of unsuccessful attempts.	Locked-out Local Users	#clear aaa local user failed-attempts {Username | All}	Will reset the number of unsuccessful login attempts to 0. Can only be done by a "Privileged EXEC" user. Can be applied to a specific user. Can be applied to all users.
Unlocking locked out users	Locked-out Local Users	#clear aaa local user lockout {Username | All}	Will unlock and reset the unsuccessful login count to 0. Can only be done by a "Privileged EXEC" user. Unlock a specific user. Unlock all locked out users.

- **Managing external authentication**

Radius info	RADIUS Statistics	#show radius statistics	Authentication statistics for the RADIUS server(s)
TACACS info	TACACS+ Statistics	#show tacacs statistics	Authentication statistics for the TACACS server(s)

7.3 - Login Banners

Overview

- Login banners are messages displayed at various stages of the login process. They are used for VTY and console connections.

Feature details / Application notes

- The switch supports the following banners;
    - Login
        - Login Timeout
            - This would be displayed if the user does not complete the login within a configurable number of Seconds.
            - The default is 30 seconds.
            - When the timer expires, the session is terminated (i.e. does not retry like it would if you typed the wrong username or password).
            - On console, the port is reset.
        - Failed login
            - Applies to Telnet and console.
            - If the user fails to login successfully, the following message will be displayed;
                - % Authentication failed! - when you try to sign in with the wrong username/password.
        - % Access denied - when attempting to elevate to privileged EXEC.
    - Web
        - Displayed on the Web Manager login screen.
        - Displayed on authentication result screen.

Configuration

- **Configuring the " login " banner.**

Step	Activity	Web Manager	CLI Command(s)	Comments

1	Configure the prompt to display before the login prompt.	Login Settings	(config)#banner login *text*	This applies to all VTY and console sessions.

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Configure the Message of the Day	Login Settings	(config)#banner motd *text*	This applies to all VTY and console sessions

Step	Activity	Web Manager	CLI Commands(s)	Comments
1	Configure the "login Timeout" banner.	Login Settings	(config)#banner prompt-timeout *text*	· This applies to all VTY and console sessions. · Should include all MAC address you wish to associate with a port or ports. · Also include any MAC addresses you wish to disallow.
2	Configure the login timeout.	Telnet/SSH Console	(config)#line vty 0 15 (config-line)#timeout login response *time*	· Select the port to configure. · Set the login timeout. Valid range is 1-300 seconds.

7.4 - AAA

Overview

- This section describes how you set up AAA on the switch.
- This involves defining the various servers and methods which will be used to achieve AAA and then assigning these to the various access methods available on the switch.

Pre-requisites

- None.

Restrictions / Limitations

- None.

Terminology

- **AAA**
  - Stands for Authentication, Authorization and Accounting. The three functions which are associated with security.
- **Authentication**
  - The act of verifying that a user is who they say they are.
- **Authorization**
  - The act of assigning a valid user with a privilege level.
- **Accounting**
  - The act of recording when users access the switch to manage it. It also involves recording when the switch is re-booted.
- **RADIUS** – Remote Authentication Dial-In User Service
  - A network protocol which provides AAA management for users or devices that connect to the switch.
- **TACACS+** - Terminal Access Controller Access-Control System Plus
  - A network protocol developed by Cisco which provides AAA management for users or devices that connect to the switch.

Feature details / Application notes

- AAA involves the following steps;
  - Defining methods for performing authentication, authorization and accounting.
  - Assigning which methods will be used for each management access method. Specifically;
    - Console
    - Telnet/SSH (VTY access)
    - Web browser

Configuration

- Configurating AAA for user login / logout

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Define method lists	AAA Settings (Authentication tab) (Authorization tab) (Accounting tab)	(config)#aaa authentication login methodlist (config)#aaa authorization exec methodlist (config)#aaa accounting exec listname Type start-stop stop-only none Method broadcast group	Configure authentication method list(s) Configure authorization method list(s) Configure accounting method list(s) Name of list being created. Accounting message will be sent; On login and logout. On logout No message will be sent All servers in "group" will get message. Else, first available serve in group will get message. Name of server group to add to list.

2	Assign authentication method lists to access methods.	Telnet/SSH and Console HTTP/HTTPS	(config-line)#login authentication listname (config-line)#aaa authentication {console | vty } (config)#ip http authentication aaa login-authentication listname Uses local database.	CLI done at the "line vty" or "line con" level. Assign method(s) when Web browser is used.
3	Assign authorization method lists to access methods. For Web Browser	Telnet/SSH and Console	(config-line)#authorization exec listname (config-line)#aaa authorization {console | vty }	CLI done at the "line vty" or "line con" level. Authorization always required. Will use authentication method to obtain authorization. Use local database.
4	Assign accounting method lists to access methods.	Telnet/SSH and Console HTTP/HTTPS	(config-line)#accounting exec listname (config)#ip http accounting exec listname	CLI done at the "line vty" or "line con" level. Configure accounting for http/https.

- Configuring Accounting for system re-boots

1	Assign accounting for system start/stop.	AAA (system tab)	(config)#aaa accounting system default {type} {method} {group} Type Start-stop None Method Broadcast Group	Configure accounting for system reboots. Message will be send on reboot. No message will be sent on reboot All servers in "group" will get message. Else, first available serve in group will get message. Name of server group.

- Configuring AAA for 802.1x

1	Assign Authentication method.	AAA (802.1x tab)	(config)#aaa authentication dot1x default group	Group must be Radius servers.
1	Assign Accounting method.	AAA (802.1x tab)	(config)#aaa accounting dot1x default start-stop group	Group can be Radius or TACACS+ servers.

7.5 - RADIUS

Overview

- A RADIUS server can be used to provide external security to the switch.

Pre-requisites

- Basic AAA has been configured on the switch.

Restrictions / Limitations

- None

Terminology

- **RADIUS** - Remote Authentication Dial-In User Service
    - A network protocol which provides AAA management for users or devices that connect to the switch.

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

Feature details / Application notes

- RADIUS can be used with the switch to provide the following functions
    - Authenticate users logging into the switch.
    - Provide authorization information for users logging into the switch.
        - Returned via attribute "Service-Type"
            - 1 (login) = User Exec
            - 6 (administrative) = Privileged Exec
            - Any other value is deemed as User Exec.
    - Provide accounting information for users and or devices logging in and out of the switch.
    - Provide AAA functions for devices accessing a port configured for 802.1x.
- The following ports are used by default;
    - Authentication = 1812
    - Accounting = 1813
    - These can be changed on a per RADIUS host basis via configuration.
- User can assign different servers (if desired) for authentication, authorization and accounting.

Configuration

- **Configure the RADIUS Settings**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Configure global settings for ALL RADIUS hosts	RADIUS	(config)#radius-server deadtime Key Retransmit timeout	How long to we ignore non-responsive server. Encryption key shared with RADIUS hosts. Number of attempts to reach host. Delay between unresponsive attempts.
2	Define IP source address for all RADIUS messages.	RADIUS	(config)#ip radius source-interface vlan *vlan#* (config)#ipv6 radius source-interface *int*	Defines which IP address will be used when originating RADIUS messages from this switch. The interface must be a management interface (i.e. has an IP address assigned).

3	Define individual RADIUS servers	RADIUS (Servers)	(config)#radius server RAD1 (config-radius-server)# address key retransmit timeout	Configure RADIUS host “RAD1” The IP address of the host. Can be followed up by the authentication and accounting UDP port numbers. You can override the global settings for the following three parameters for this RADIUS host.
4	Define a group of RADIUS servers (optional)	RADIUS (server Groups)	(config)#aaa group server radius GroupR1 (config-sg-radius)#server name	Configure a group of RADIUS servers called “GroupR1” Add one or more RADIUS server(s) to the group. Group can be assigned to authentication, authorization and/or accounting functions.

Monitoring and Maintaining

- **RADIUS statistics**

Activity	Web Manager	CLI Command(s)	Comments
Display RADIUS Statistics	RADIUS Statistics	#show radius statistics	Add the keyword details for a more detailed output.
Clear RADIUS Statistics	RADIUS Statistics	#clear radius statistics	Reset all the statistics to zero.

7.6 - TACACS+

Overview

- A TACACS+ server can be used to provide external security to the switch.

Pre-requisites

- Basic AAA has been configured on the switch.

Restrictions / Limitations

- None

Terminology

TACACS - Terminal Access Controller Access-Control System

- A network protocol developed by Cisco which provides Authentication services for users or devices that connect to the switch.

TACACS+ - Terminal Access Controller Access-Control System Plus

- A network protocol developed by Cisco which provides Authentication, Authorization and Accounting services for users or devices that connect to the switch.
  - TACACS+ is not backwards compatible with the much older TACACS protocol.
  - In this document "TACACS" is synonymous with "TACACS+"

AAA

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

Feature details / Application notes

- TACACS+ can be used with the switch to provide the following functions
  - Authenticate users logging into the switch.
  - Provide authorization information for users logging into the switch.
  - Provide accounting information for users logging in and out of the switch.
  - Provide accounting for devices connecting on 802.1x ports.
- The following ports are used by default;
  - Authentication = 1812
  - Accounting = 1813
  - These can be changed on a per TACACS host basis via configuration.

Configuration

- **Configure the TACACS Settings**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Configure global settings for ALL TACACS+ hosts	TACACS+	(config)#tacacs-server deadtime key timeout	How long to we ignore non-responsive server. Encryption key shared with TACACS+ hosts. Delay between unresponsive attempts.

2	Define IP source address for all TACACS+ messages.	TACACS+	(config)#ip tacacs source-interface vlan *vlan#* (config)#ipv6 tacacs source-interface *int*	Defines which IP address will be used when originating TACACS+ messages from this switch. The interface must be a management interface. (i.e. has an IP address assigned).
3	Define individual TACACS+ servers	TACACS+ (Servers)	(config)#tacacs server TAC1 (config-tacacs-server)# address key timeout	Configure TACACS+ host “TAC1” The IP address of the host. Can be followed up by the authentication and accounting UDP port numbers. You an override the global settings for the following two parameters for this host.
4	Define a group of TACACS+ servers. (optional)	TACACS+ (Server Groups)	(config)#aaa group server tacacs GroupR1 (config-sg-tacacs)#server name	Configure a group of tacacs servers called “GroupR1” Add one or more TACACS+ server(s) to the group. Group can be assigned to authentication, authorization and/or accounting functions.

Monitoring and Maintaining

- **TACACS+ statistics**

Activity	Web Manager	CLI Command(s)	Comments
Display TACACS+ Statistics	TACACS+ Statistics	#show tacacs statistics	Add the keyword details for a more detailed output.
Clear TACACS+ Statistics	TACACS+ Statistics	#clear tacacs statistics	Reset all the statistics to zero.

7.7 - Port Security

Overview

- Port Security allows the user to restrict port access to specific devices. It also allows the user to limit the number of devices which can connect to a port.

Restrictions / Limitations

- Port security can only be enabled on an access or Trunk port
- User can't enable port security if "static addresses" are currently defined in the switch
- If the port is part of a port-channel, the user can't enable port security on the port. It must be done at the port-channel level.

Terminology

- **ATU** - Address Translation Unit
  - The ATU is a set of tables which are maintained in the switch. Each table is associated with a specific port on the switch. It holds the MAC addresses for all devices which may be connected on the port. Addresses are categorized within VLANs.
- **Age-out**
  - The term is used to describe the process whereby an ATU entry is removed after some period of inactivity. This does not apply to static entries.
- **MAC move violation**
  - This is a condition where a MAC address which is configured on a secure port is seen on another port in the same vlan.

Feature details / Application notes

- This feature allows the user to specify which devices (via MAC address) will be allowed to access a port on a switch by having the user manually configure the "Secure MAC addresses" allowed.
- The switch can also dynamically learn MAC addresses which may later be converted to secure addresses. These dynamically learned address **don't age**. These addresses will get deleted if the link goes down or if port security is turned off on the port.
- The security feature also allow the user to limit the number of addresses that can be learned by the switch (per port, per vlan).
- Dynamic MACs allowed = Maximum devices allowed - Statically configured devices.
- At the point that port security is enabled (as well as disabled), all addresses are deleted from the chip.
- If a security violation occurs (i.e. unauthorized device attempts to access the switch, number of devices attempting to connect exceeds the maximum number of devices configured, etc…), the user can configure what action to take as follows;
  - Protect
    - Drops all packets from the unauthorized device but does not increment the security-violation count and does not generate a security violation condition.
  - Restrict
    - Drops all packets from the unauthorized device. The security-violation count is

incremented, an SNMP trap is sent and a syslog message is issued.

- Shutdown (default)
  - Interface becomes error-disabled and shuts down. Link is taken down and link led turns off.
- Shutdown vlan
  - Similar to shutdown but on a per-VLAN basis.

Configuration

- **Configuring port security on the switch.**

Activity	Web Manager	CLI Command(s)	Comments
Enable port security	Port Security	(config)#int gi 1/1 (config-if)#switchport port-security	Select the port to enable security on. Enable port security on the port. At this point, any existing learned addresses are removed from the switch. Port security is disabled by default.
Define number of devices allowed on port	Port Security (Settings) tab	(config-if)#switchport port-security maximum <number>	Command for specifying maximum number of devices. Enter the maximum number of devices allowed on the port.
Define number of devices allowed per vlan	Port Security (Settings) tab	(config-if)#switchport port-security maximum <number> Vlan <num | access | voice>	Command for defining the number of devices allowed on a vlan. Enter the maximum number of devices allowed on the vlan. For “access” port, specify “access” or “voice” vlan. For “Trunk” port, specify the vlan number or vlan range.
Define how dynamically addresses are stored	Port Security (Settings) tab	(config-if)#switchport port-security mac-address sticky	Command for defining port security parameters. Indicate that any dynamically learned address will now be saved in configuration.

Define how security violations will be treated.	Port Security (Settings) tab	(config-if)#switchport port-security Violations Protect Restrict Shutdown Shutdown vlan	Command for defining port security parameters. Select action to take on violations. Drop all packets from unauthorized devices. Does not increment the security violation count. Drop all packets from unauthorized devices. Increment the security violation count. Sends out traps and syslogs. Interface becomes “error disabled”. Offending vlan becomes “error disabled”.
Add “secure addresses”	Port Security (Secure MAC Addresses) tab	(config-if)#switchport port-security mac-address <mac address> Vlan <access | voice>	Command for adding secure MAC addresses. Enter the device MAC address in hhhh.hhhh.hhhh notation. Specify if vlan is access or voice. This is optional and default is the access vlan.

Monitoring and Maintaining

- **Monitoring secure MAC addresses.**

Activity	Web Manager	CLI Command(s)	Comments
Display secure MAC addresses	Port Security Status	#show mac address-table secure Address Interface Vlan CR	Command to display MAC table information. Can specify a specific secure MAC address to display. Can request all secure addresses for an interface. Can request all secure addresses for a vlan. Request all secure addresses on the switch.

Display high level port security information	Port Security Status	#show port-security Address Interface CR	Command to display high level port security information. Can hit CR after address to see all or further qualify with a vlan number. Display port security info only for the specified interface. Display high level port security information for all interfaces.
Clear port security functionality	Port Security Status (disable)	#clear port-security All Configured Dynamic Sticky Address | interface	Command to disable port security and clear the following secure addresses. Will clear configured, dynamic and sticky secure addresses. Clear only configuredsecure addresses. Clear only dynamic secure addresses. Clear only sticky secure addresses. In all cases above, you can further specify whether this should be applied to a specific address (on all interfaces) or to a specific interface.

7.8 - 802.1X

Overview

- This feature provides a way of forcing devices connecting to the switch to authenticate themselves before they are granted access to the switch, other devices on the switch or the network.

Pre-requisites

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

Restrictions / Limitations

- 802.1x is only supported on access ports.
    - Not supported on trunks or port-channels

Terminology

- **dot1x**
    - This is a term that is used to refers to the 802.1x feature.
- **Supplicant**
    - This refers to the device which is requesting access to the network.
- **Authenticator**
    - This refers to the switch which the supplicant is attempting to connect to. The switch will act as the intermediary between the "supplicant" and the "authenticating server".
- **Authenticating Server**

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

- **EAP - Extensible Authentication Protocol**
  - This is the protocol that is used to perform the basic authentication function.
  - For messages between the supplicant and the authenticator, this is encapsulated in EAPoL. (EAP over LAN)
  - For messages between the authenticator and the authenticating server, the EAP is encapsulated within the RADIUS messages.
  - This protocol is defined by RFC 3748.
- **MAB - MAC Authentication Bypass**
  - This feature allows devices which do not support 802.1x to be authenticated on the switch. The authentication is done by using the MAC address of the device as both the username and password. The authenticating server would need to have this information configured as a valid user.

Feature details / Application notes

- The switch supports a Radius host as the "authenticating server". The Radius host needs to support EAP extensions in order to perform the 802.1x authentication function.
- The switch can act as both a "supplicant" or an "authenticator". This is configurable on a port basis.
- Modes of operation supported by the switch for 802.1x
  - Single host
    - Only one device can authenticate and connect on the port.
    - This is the default mode of operation.
  - Multiple host
    - Unlimited number of devices can connect on the port once a single device has been authenticated on the port. This single device must be a "data" (as opposed to voice) device.
  - Multiple authentication
    - Each device connecting to the switch is required to authenticate.
    - No limit as to the number of devices which can authenticate on the port.
- The port is in an "unauthorized" state if the device attempting access has not authenticated. In this state the following applies;
  - The port does not allow any traffic except for STP (Spanning Tree Protocol) and EAPOL.
  - If the port is configured as a VOICE VLAN port, the port allows VoIP traffic as well.
  - Any static addresses configured are not written to the switch chip until the port is authorized.

Configuration

- **Selecting the 802.1x role for a port.**
  - 802.1x enabled ports can perform one of two roles;
    - Authenticator
      - Port will authenticate 802.1x supplicants which are connected to it.
    - Supplicant

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

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Select the port.	802.1x Settings --> Port Settings	(config)#int gi 1/3	Select the switch port. On Web manager, select the desired port and hit the "Edit" button.
2	Select the 802.1x role for this port.	802.1x Settings --> Port Settings	(config-if)#dot1x pae supplicant Authenticator	Supplicant – Port will authenticate with peer which is the authenticator. Authenticator – Port will authenticate the device/ devices (supplicants) connecting on the port.

- **Configuring a port as a supplicant.**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Select a "credential" profile.	802.1x Settings --> Port Settings	(config)#int gi 1/3 (config-if)#dot1x credentials<profile name>	Select the switch port. On Web manager, check the "Enable 802.1x authentication" box and select "Supplicant" for PAE mode. Assign the desired credentials profile to this supplicant. See "Creating a credential profile" below.
2	Select an "EAP" profile.	802.1x Settings --> Port Settings	(config#)#int gi 1/3 (config-if)#dot1x supplicant eap <profile name>	On Web manager, check the "Enable 802.1x authentication" box and select "Supplicant" for PAE mode. Select the switch port. Assign the desired EAP profile to this supplicant. See "Creating an EPA profile" below.

- **Creating a credential profile.**
  - Credential profiles are just a username and password which will be used by supplicants to authenticate on 802.1x authenticators. Creating a profile allows the user to assign this

profile to individual ports as needed.

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Create a “credential” profile.	802.1x Credential Profiles	(config)#dot1x credentials <profile name> (config-dot1x-creden)#username (config-dot1x-creden)#password	Select the name for the profile. Spaces are not allowed in the name. Define the username. Define the password for this user.

- **Creating an EAP profile.**
  - An EAP profile is similar to a Credential profile but is used to define the authentication methods to be used by and 802.1x supplicant. Creating a profile allows the user to assign this profile to individual ports as needed.

Step	Activity	Web Manager	CLI Command(s)	Comments

1	Create an “EAP” profile.	802.1x EAP Profiles	(config)#eap profile <profile name> (config-eap-profile)#method (config-eap-profile)#pki-trustpoint	Select the name for the profile. Spaces are not allowed in the name. Select the authentication method to be used. For some methods (i.e. ttls, this specifies the basic authentication method and requires a second parameter to define the sub authentication method under ttls). This refers to the name of an authenticator certificate which was downloaded to the switch. (see “Server CA Certificates” under “Administration”). It is only required if the supplicant is required to validate that he is communicating with the desired authenticator and not an imposter.

- **Configuring a port as an "authenticator".**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Select the port to configure.	802.1x Settings	(config)#int gi 1/1	Each port is configured individually.

2	MAB	802.1x Settings --> Port Settings.	(config-if)#mab {eap}	Enable MAB if supplicant does not support 802.1x. The switch will use the supplicants MAC address as username and password. MAB uses “normal” radius protocol to authenticate the supplicant. If the parameter {eap} is included, the switch will use EAP protocol embedded within the radius message. The radius server must be configured to expect this message format.
3	Select the 802.1x mode of operation.	802.1x Settings --> Port Settings.	(config-if)#authentication host-mode multi-host single-host multi-auth	Allows unlimited number of data and voice devices to connect to port after a single 802.1x supplicant has been authenticated. Allows one supplicant on the port. The supplicant can be a data or voice device. Allows multiple data and voice devices on port. Each supplicant must be individually authenticated.
4	Port control	802.1x Settings --> Port Settings	(config-if)#dot1x port-control auto force-authorized force-unauthorized	Places port in unauthorized state until such time as a supplicant authenticates. Disables 802.1x authentication and places the port in an “authorized” state. Causes the port to remain in an “unauthorized” state. Port does not attempt to authorize supplicant and port is blocked to all data.
5	Periodic re-authentication	802.1x Settings --> Port Settings	(config-if)#authentication periodic	When enabled, the supplicant will be asked to periodically re-authenticate. To set re-authentication period, see “Advanced 802.1x settings” below.

6	Authentication violation mode	802.1x Settings --> Port Settings	(config-if)#authentication violation protect restrict shutdown	Define action to take when a security violation occurs. Drop data from offending device. Generate a syslog indicating violation occurred. Error disable the port.
7	Authentication no response action	802.1x Settings --> Port Settings	(config-if)#authentication event fail action authorize vlan nnnn	If desired, the supplicant can be assigned to a "guest" vlan if no 802.1x response is received from it. Usually this is used to allow the supplicant to download an 802.1x client. In order to allow this, you must enable this feature globally using this command.
8	Enable guest vlan feature.	802.1x Settings --> Advanced tab	(config)#dot1x guest-vlan supplicant	In order to support the guest vlan, you must enable this feature globally using this command.
9	Authentication failure action	802.1x Settings --> Port Settings	(config-if)#authentication event no-response action authorize vlan nnnn (config-if)#authentication event fail retry	If desired, the supplicant can be assigned to a "restricted" vlan if it fails the 802.1x authentication. This provides the supplicant with some restricted access to the network. Configures the number of times authentication will be tried before sending the supplicant to the restricted vlan.

- **Configuring Advanced 802.1x settings**
    - Allows for the setting of the various timers and re-try counters. These timers are set on a per port basis.

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Setting the "supplicant response timeout"	802.1x Port Settings --> Advanced tab	(config-if)#dot1x timeout supp-timeout	Sets the amount of time that the authenticator will wait for the supplicant to reply to all 802.1x messages other than the EAP ID request. The valid range is 1 – 65535 seconds.

2	Setting the “transmit timeout”	802.1x Port Settings --> Advanced tab	(config-if)#dot1x timeout tx-period	Configures the interval, in seconds, between two successive EAP request ID messages. This is the first message sent by 802.1x, trying to identify the supplicant. The valid range is 1 – 65535 seconds.
3	Setting the “quiet period timeout”.	802.1x Port Settings --> Advanced tab	(config-if)#dot1x timeout quiet-period	Sets the amount of time that the authenticator will remain “quiet” after a failed authentication attempt. The valid range is 1-65535 seconds.
4	Setting the “re-authentication timeout”.	802.1x Port Settings --> Advanced tab	(config-if)#authentication timer reauthenticate {server}	Sets the amount of time after which the authenticator must re-authenticate the supplicant. The valid range is 1 - 65535 seconds. If the parameter “server” is specified, the time is derived from the “Session-Timeout value” (RADIUS Attribute 27)
5	Setting the “restart timeout”	802.1x Port Settings --> Advanced tab	(config-if)#authentication timer restart	Interval in seconds after which an attempt should be made to authenticate an unauthorized port. The valid range is 0-65535 seconds.
6	Setting the “Authentication re-tries”	802.1x Port Settings --> Advanced tab	(config-if)#dot1x max-req	Sets the number of times the authenticator will re-transmit an EAP message to the supplicant. The valid range is 1 – 10 re-tries.
7	Setting the “re-authentication re-tries”	802.1x Port Settings --> Advanced tab	(config-if)#dot1x max-reauth-req	Sets the number of times the authenticator will try to re-authenticate a supplicant. The valid range is 1 – 10 re-tries.

Monitoring and Maintaining

- **Running the 802.1x readiness test.**
  - This test checks whether an 802.1x capable device is connected to the port under test.
  - If the test is successful, a message is sent to the system log. If the test fails, no messages are generated.

Step	Activity	Web Manager	CLI Command(s)	Comments

1	Define the time-out for test	802.1x Port Settings --> Advanced tab	(config)#dot1x test timeout	Set the length of time to wait for the device to respond to the test messages. Valid range is 1 – 65535 seconds.
2	Run the test.	802.1x Port Settings	#dot1x test eapol-capable Interface gi 1/6	Run on a specific interface. If interface parameter is omitted, the test is run on all 802.1x enabled ports.

- **Manually controlling the state of an 802.1x port.**
  - This allows the user control the 802.1x by issuing manual commands.
  - User can cause the port to become "unauthorized". This will force the port to attempt to re-authenticate the supplicant(s).
  - User can also force a port to -re-authenticate a port or ports. This manually kicks off the re-authenticate process.

Activity	Web Manager	CLI Command(s)	Comments
Re-initialize a port.	802.1x Port Settings	#dot1x initialize int gi 1/6	This will re-initialize the port to an unauthorized state and attempt to authenticate the device(s) on the port. If interface is omitted, this will apply to all the 802.1x enabled ports.
Re-authenticate a supplicant.	802.1x Port Settings	#dot1x re-authenticate int gi 1/6	This will initiate a re-authentication process. If interface is omitted, this will apply to all the 802.1x enabled ports.

7.9 - Management Access Filter

Overview

- Ability to limit who can get management access to the IDS switch.

Pre-requisites

- none

Restrictions / Limitations

- None

Terminology

- **Switch Management Access**

  - This is the ability to access the switch in order to configure or administer the switch or to obtain status information. This is not to be confused with devices which are connected to the switch ports and are simply passing frames between themselves and other devices connected to the switch.

- **Telnet**
  - A user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access a computer remotely.
- **SSH**
  - SSH stands for "Secure Shell". It is similar to Telnet but information sent and received over this TCP/IP connection is encrypted preventing anyone listening in from being able to decipher the data being exchanged.
- **HTTP/HTTPS -**Hypertext Transfer Protocol.
  - This protocol is used by browsers when communicating with Web Servers. The HTTPS is the secure / encrypted version of the protocol. The IDS switch has an embedded web server which allows users to access the management functions of the switch using a web browser.
- **VTY** - Virtual Terminal
  - These refer to terminal sessions which are established by Telnet or SSH. Each VTY session is numbered in the order in which the connection was established. There can be 16 simulatneous VTY sessions established (0 to 15).
- **Console**
  - The switch supports the ability to connect a terminal to the "console" serial port. This is an RJ45 connection. On some models, there is also a Micro USB connector for the console.
- **Access-list**
  - A list of IP addresses each of which can be associated with an "allow" or a "deny" directive. This list can be assigned to various functions to control which device can access the function.

Feature details / Application notes

- Typical management access control involves the need for the user to login to the switch before they are allowed to manage it. This can be done using a local database or an external authentication server such as Radius or a Tacacs server.
- In addition to the requirement to login, the switch allows for restricting switch management access by protocol or specific IP address.
  - For IP address restriction, the user assigns an access-list to the function. Processing of access-lists is as follows;
    - The list is processed from the top down. As soon as a match is found on the IP

address attempting access, the processing of the list stops and the corresponding "allow" or "deny" is applied. If the list is fully processed and no match is found for the IP address in question, the action taken will be to deny access.

Configuration

- **Controlling access to specific protocols**

Activity	Web Manager	CLI Command(s)	Comments
Limit access to Specific VTY protocols	System General Settings	(config)#line vty 0 – 15 (config-line)#transport input (config)#ip http server (config)#ip http secure-server	Used to restrict access to Telnet, SSH, or both. Allow HTTP access. Allow HTTPS access.
Limit access to Specific browser protocols	System General Settings	(config)#ip http server (config)#ip http secure-server	Allow HTTP access. Allow HTTPS access.

- **Using Access Lists**

Activity	Web Manager	CLI Command(s)	Comments
Define the access list	Access Control Lists	(config)#ip access-list standard 1 (config-std-nacl)#[permit | deny] [any | host] [hostname | ip address] (config-std-nacl)#exit	Start definition of standard list 1. Define condition. Can have multiple conditions in the list. Exit list definition.
Assign list to function	HTTP/HTTPS VTY	(config)#ip http access-class 1 (config)#line vty 0 – 15 (config-line)#access-class 1	Assigns access list 1 to http/https protocols. Assign access list 1 to VTY protocols.

- **Controlling console access**

Activity	Web Manager	CLI Command(s)	Comments

Enable/Disable management access via console	Console access	(config)#line console 0 (config-line)#no exec	Prevent management access from console.

Monitoring and Maintaining

- **Monitoring currently connected management sessions**

Activity	Web Manager	CLI Command(s)	Comments
Display current management sessions	Management Access Info	#show users all #show users web	Display all management sessions. This includes VTY and Web sessions. Displays only connected Web sessions.

- **Disconnecting a VTY management session.**

Activity	Web Manager	CLI Command(s)	Comments
Drop connection for a currently active session.	Management Access Info	#clear line x	A “show users all” can provide you with a listing of all VTY sessions and their associated line number.

- **Disconnecting a Web management session.**

Activity	Web Manager	CLI Command(s)	Comments
Drop connection for a currently active Web session.	Management Access Info	#clear user web {username, ip}	Can be done by username alone or can be qualified with an IP address. The username alone will disconnect all sessions associated with the specified username.

8 - MAC Address Management

8.1 - Static MAC addresses

Overview

- Ability to pre-define the MAC address of devices connected to specific ports.

Pre-requisites

- **None**

Restrictions / Limitations

- **None**

Terminology / Acronyms

- **ATU** - Address Translation Unit
  - The ATU is a set of tables which are maintained in the switch. Each table is associated with a specific port on the switch. It holds the MAC addresses for all devices which may be connected on the port. Addresses are categorized within VLANs.
- **Age-out**
  - The term is used to describe the process whereby an ATU entry is removed after some period of inactivity. This does not apply to static entries.

Feature details/Application notes

- Static entries can be used to;
  - Reserve a spot in the ATU table for a specific device. In cases where we limit the number of devices which can be connected to a port, this will ensure this devices ability to connect to the port.
  - Put an entry into the ATU table for devices which may never send any messages to the switch.
- Static MAC addresses;
  - Must be associated with a specific VLAN.
  - Can be **Unicast** or **Multicast** addresses.
  - Can be assigned to more than one port (even in the case of unicast MAC addresses).
- Static entries are more of an optimization feature. Without the entry in place, a packet destined to a MAC address not found in the switch would simply flood to all ports.
- Static entries do not age out.
- Static MAC addresses can also be used to define which MAC addresses will be ignored by the switch. This is done by using the "drop" option. When used, frames received by the switch with

the specified MAC address will be silently dropped.

Configuration

- **Adding static MAC addresses**

Ste p	Activity	Web Manager	CLI Command(s)	Comments
1	Determine which MAC addresses will reside on each port.			Should include all MAC address you wish to associate with a port or ports. Also include any MAC addresses you wish to disallow.
2	Add the static entry.	Static MAC Addresses	(config)#mac address-table static	An entry is required for each unique VLAN and MAC address combination.

- **Deleting static MAC addresses**

Ste p	Activity	Web Manager	CLI Command(s)	Comments
1	Delete the desired MAC address.	Static MAC Addresses	(config)#no mac address-table static	Need to specify the MAC address to be deleted and its associated VLAN.

Monitoring and Maintenance

- **Monitoring MAC addresses.**

Activity	Web Manager	CLI Command(s)	Comments
Display static MAC addresses	MAC Address Table	#show mac address-table static	In Web Manager, use the filtering capability to display “static” entries.

8.2 - Quick Port Disconnect

Overview

- This feature causes all dynamically learned MAC address on a switch port to be deleted when the port link drops.

Pre-requisites

- None

Restrictions / Limitations

- If 802.1x security is enabled on the port, we would immediately delete the entries associated with this port when a link down condition is detected. We would do this regardless of whether the "quick port disconnect" feature is enabled. This will force the devices connecting on this port to re-authenticate after a link down condition.

Terminology

- **ATU** - Address Translation Unit
    - The ATU is a set of tables which are maintained in the switch. Each table is associated with a specific port on the switch. It holds the MAC addresses for all devices which may be connected on the port. Addresses are categorized within VLANs.
- **Age-out**
    - The term is used to describe the process whereby an ATU entry is removed after some period of inactivity (activity is defined as packets received from the device). This does not apply to static entries.

Feature details / Application notes

- This feature can be enabled on a specific switch port interface basis.
    - By default, this feature is disabled on all ports.
- When the link on a port changes from a "link up" to a "link down" state, the switch will normally allow all MAC addresses dynamically learned on this port to slowly age out. This comes in handy when a cable is accidently removed from a port and then re-inserted. With this feature in place, the port will maintain all the MAC addresses which were previously learned on the port and continue to direct traffic destined to one of these addresses, to that port.

- With "Quick Port Disconnect" enabled, as soon as the link drops on the port, all dynamically learned addresses on that port are immediately deleted.

Configuration

- **Enabling the feature on port 5 and 7**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Enable the feature for switch port 5	MAC Address Settings	(config)#mac address-table quick-disconnect interface gi 1/5	Enables feature on switch port 5. In Web manager, this is found under the “Port” tab.
2	Enable the feature for switch port 7	MAC Address Settings	(config)#mac address-table quick-disconnect interface gi 1/7	All other ports maintain the default setting of not having this feature enabled.

Monitoring and Maintaining

Activity	Web Manager	CLI Command(s)	Comments
Display the status of quick disconnect feature.	MAC Address Table	#show mac address-table quick-disconnect	Displays the status of all the switch ports.

9 - Traffic Management

9.1 - IGMP

Overview

- IGMP is a protocol which allows nodes on a network to advertise and discover what IP multicast addresses their peers are interested in.

Pre-requisites

- None

Restrictions / Limitations

- IGMP cannot co-exist with GMRP on the same port. If GMRP is enabled on a port, IGMP cannot be enabled on that port.

Terminology

- **IGMP** - Internet Group Management Protocol
  - A communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. IGMP is an integral part of IP multicast.
- **IGMP Snooping** - The act of capturing IGMP messages
  - The IDS layer 2 switch has the ability to listen in on IGMP (layer 3 messages) and extract information from these packets while still delivering them to their intended destinations. This activity is referred to as "IGMP Snooping"
- **IGMP Querier** -Node which will query all other nodes in network with regards to multicasts.
  - The IGMP querier node is the node responsible for querying all other nodes on the VLAN with regards to which multicasts they are interested in. There is only one IGMP querier per VLAN.

Feature details / Application notes

- There are three versions of the IGMP protocol
  - RFC 1112-IGMP v1 (Aug. 1989)
  - RFC 2236-IGMP v2 (Nov. 1997)
  - RFC 4604-IGMP v3/MLDv2 (Aug. 2006)
  - The Perle IDS switch supports all three versions.
- IGMP acts at a layer 3 level. The Perle IDS switch is a layer 2 switch. There is a mapping from Layer 3 multicast addresses to a layer 2 (MAC) multicast addresses but it is not a one to one. This means that multiple layer 3 multicasts may map to the same layer 2 multicast.
  - Layer 3 multicast address range is;

§ 224.0.0.0 - 239.255.255.255

- 224.0.0.0 - 224.0.0.255 is reserved for routing protocols. **NOT CONSTRAINED** by IGMP snooping.

§ E0 (224) to EF (239)

o The mapping between layer 3 and layer 2 really only looks at the 23 least significant bits of the multicast address. This leaves 9 bits which are not looked at (i.e. **32 different addresses layer 3 addresses which would all map into the same layer 2 MAC address**).

§ 01 00 5E (24 bits) + 0 (1 bit) + 23 bits from IP multicast address = 48 bit MAC address.

- When IGMP is enabled, the port setting for blocking unknown multicasts is ignored. If IGMP has not associated a multicast group with a given port, that multicast is not sent out that port regardless of the "Block Unknown Multicast" setting.

Configuration

- **Enable IGMP Snooping**

Activity	Web Manager	CLI Command(s)	Comments
Enable IGMP globally.	IGMP	(config)#ip igmp snooping	Globally enable IGMP snooping.
Enable IGMP on a VLAN	IGMP	(config)#ip igmp snooping vlan 1.	Enable IGMP snooping on VLAN 1. VLAN does not have to be a management VLAN.
Enable IGMP on a port.	IGMP	(config)#int gi 1/2 (config-if)#ip igmp snooping	Enable IGMP snooping on port 2.

- **Setting IGMP Snooping parameters**

Activity	Web Manager	CLI Command(s)	Comments

Globally.	IGMP	(config)#ip igmp snooping <parameters>	This will set the configured parameters on a global basis.
Enable IGMP on a VLAN.	IGMP	(config)#ip igmp snooping vlan 1 <parameters>	Assign IGMP Snooping parameters to vlan 1. If parameter is settable on a global basis, it will not be settable on a VLAN basis.
Set limit on number of multicast groups (optional).	IGMP	(config)#int gi 1/2 (config-if)#ip igmp max-groups	Defines the maximum number of multicast addresses that can be assigned to this port. Once this number is exceeded, any new multicast group requests will be dropped.

- **Setting the switch up as an IGMP Querier.**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Enable IGMP	IGMP	(config)#ip igmp snooping.	Globally enable IGMP snooping.
2	Enable IGMP querier	IGMP	(config)#ip igmp snooping querier (config)#ip igmp snooping vlan 1 querier.	Enable the querier globally. Enable the querier on vlan 1.
3	Set Querier parameters.	IGMP	(config)#ip igmp snooping querier <parameters>	Configure the parameters associated with the querier function.

Monitoring and Maintaining

- **Monitoring IGMP**

Activity	Web Manager	CLI Command(s)	Comments
Display information about IGMP	IGMP status	#show ip igmp snooping.	Can be global or VLAN specific.
Display information about IGMP querier	IGMP status	#show ip igmp snooping querier	Can be global or VLAN specific.

9.2 - MLD (IPv6)

Overview

- Method of learning about multicast addresses in an IPv6 network.

Pre-requisites

- None

Restrictions / Limitations

- None

Terminology

- **MLD -** Multicast Listener Discovery
  - This is a protocol used to discover multicast listeners in an IPv6 environment. It is embedded in ICMPv6.

Feature details / Application notes

- This feature is very similar to IGMP. Whereas IGMP is used in an IPv4 environment and MLD is used in an IPv6 environment.

- The two features can co-exist within the same switch/port.

- There are two version of MLD (v1 and v2)

  - V1 is described by RFC 2710 (equivalent to IGMPv2)

  - V2 is described by RFC4604 (equivalent to IGMPv3)

  - The Perle IDS switch supports both versions.

Configuration

- **Enable MLD**

Activity	Web Manager	CLI Command(s)	Comments
Enable MLD globally.	IPv6 MLD	(config)#ipv6 mld snooping	Globally enable MLD snooping
Enable MLD on a VLAN.	IPv6 MLD	(config)#ipv6 mld snooping vlan 1.	Enable MLD snooping on VLAN 1. VLAN does not have to be a management VLAN.
Enable MLD on a port.	IPv6 MLD	(config)#int gi 1/2 (config-if)#ipv6 mld snooping	Enable MLD snooping on port 2.

- **Setting MLD Snooping parameters**

Activity	Web Manager	CLI Command(s)	Comments
Globally	IPv6 MLD	(config)#ipv6 mld snooping <parameters>	This will set the configured parameters on a global basis.
Enable MLD on a VLAN.	IPv6 MLD	(config)#ipv6 mld snooping vlan 1 <parameters>	Assign MLD Snooping parameters to vlan 1. If parameter is settable on a global basis, it will not be settable on a VLAN basis.
Set limit on number of multicast groups (optional).	IPv6 MLD	(config)#int gi 1/2 (config-if)#ipv6 mld max-groups	Defines the maximum number of multicast addresses that can be assigned to this port. Once this number is exceeded, any new multicast group requests will be dropped.

- **Setting the switch up as an MLD Querier.**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Enable MLD	IPv6 MLD	(config)#ipv6 mld snooping.	Globally enable MLD Snooping.
2	Enable MLD querier	IPv6 MLD	(config)#ipv6 mld snooping querier (config)#ipv6 mld snooping vlan 1 querier.	Enable the querier globally. Enable the querier on vlan 1.
3	Set Querier parameters.	IPv6 MLD	(config)#ipv6 mld snooping querier <parameters>	Configure the parameters associated with the querier function.

Monitoring and Maintaining

- **Monitoring MAC addresses.**

Activity	Web Manager	CLI Command(s)	Comments
Display static MAC addresses	MAC Address Table	#show mac address-table static	In Web Manager, use the filtering capability to display “static” entries.

9.3 - GMRP

Overview

- GMRP is a protocol which learns about active Multicast groups adds them to their associated interfaces.

Pre-requisites

- None.

Restrictions / Limitations

- GMRP cannot co-exist with IGMP on the same port. If IGMP is enabled on a port, GMRP cannot be enabled on that port.

Terminology

- **GARP - Generic Attribute Registration Protocol**
  - Defined by IEEE 802.1 is a protocol used to register and de-register attribute values like VLAN identifiers and Multicast group membership. The protocol defines the architecture, rules of operation, state machines and messages required to advertise information regarding the specific attributes.
- **GMRP - GARP Multicast Registration Protocol**
  - This is an application which uses GARP to specifically learn and advertise information regarding Multicast group usage on interfaces.
- **Multicast Group - (MC)**
  - Multicast group is an address which is shared by multiple devices. This exists at the layer 2 (MAC) and Layer 3 (IP).
- **Link Aggregation**
  - The logical joining of multiple physical single ports to form one larger logical data pipe.

Feature details / Application notes

- GMRP is a protocol which advertises information about layer 2 Multicast groups.
- When a device is interested in receiving data on a specific multicast address, it can use
- GMRP can co-exist with IGMP (which operates at a Layer 3).
- If a multicast group is received on a port, it is propagated to;
  - Other ports which are members of the original VLAN of the received MC and;
    - have that MC group registered.
    - Or have not set the "filter unknown multicasts" flag
  - If the received MC is not known on the switch it will only get propagated to ports which have the "gmrp service unregistered-groups" configuration option set.

Configuration

- **Setting up the GMRP environment.**
  - GMRP can be enabled globally or on a per interface basis.
  - For individual ports you can specify;
    - All multicast groups which are registered on this switch (on the VLAN to which this port belongs) will be sent out this port.
      - Used for ports connected to a router or network analyzer as an example.
    - What you want the peer to send on this port.

- All-groups
  - Send us groups that you have learned. If this is not specified, the peer will only send us groups that we have specifically requested.
- Unregistered-groups
  - Send us all the groups that we have requested plus any other groups that you receive but don't know about (i.e. unknown or unregistered groups).

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Adjust GARP timers as needed	GMRP	(config)#garp timer Join Leave leaveall	Define the time to wait before advertising a newly-added MC group. The removal of a specific MC. How often to ask peers for their MC information.
2	Define action to take on interface when switch is about to forward a multicast out the interface.	GMRP	(config-if)#gmrp forward-all	Send out this port all multicast addresses registered for the vlan associated with the interface.
3	Define what multicast groups you want the peer to send to this interface.	GMRP	(config-if)#gmrp service all-groups unregistered-groups	Request peer to; Send all groups we asked for and all groups you know about. Send all groups we asked for and any group you don’t know about.
4	Enable GMRP.	GMRP	(config)#gmrp (config-if)#gmrp	Enable GMRP globally. Can be done on individual port basis.

Monitoring and Maintaining

- **Display GMRP statistics**

Activity	Web Manager	CLI Command(s)	Comments
Display GMRP statistics	GMRP Statistics	#show gmrp statistics	Number of messages received and sent for each GMRP packet type.

- **Clear GMRP statistics**

Activity	Web Manager	CLI Command(s)	Comments
Clear GMRP statistics	GMRP Statistics	#clear gmrp statistics {interface}	Can clear all or a specific interface.

9.4 - Blocking Unknown Multicasts and Unicasts

Overview

- This feature controls what action is taken when an unknown mulitcast or unknown unicast is about to be sent out the switch ports.

Pre-requisites

- None

Restrictions / Limitations

- None

Terminology

- **Unknown Multicast**
    - An unknown multicast is a multicast which has not been configured on any vlan/port on the switch. As soon as a multicast is configured on a single vlan/port, it is deemed as "known" by the switch.
- **Unknown Unicast**
    - An unknown unicast is a unicast destination address which has not been learned by the switch (i.e. the switch does not know what port this address is associated with). The can be due to the fact that the switch has not seen any packets from this address or has not

learned this address due to some security or configured limitation.

Feature details / Application notes

- By default, when the switch needs to forward an unknown multicast of unicast, since it does not know which specific port(s) are associated with this address, it will flood the frame to all ports. This behaviour can be modified by the user.
- If the switch is being run in a very controlled environment where each destination is defined in the switch, the user can disable the flooding behaviour by enabling this feature.

Configuration

- **Disabling the flooding of unknown multicasts and/or unicasts**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Disable flooding of desired destinations	Flood control	(config-if)#switchport block {multicast | unicast}	The CLI command is executed under the switchport interface. The NO version of this command will enable the specified frame type.

Monitoring and Maintaining

- **Displaying the current status of the feature**

Activity	Web Manager	CLI Command(s)	Comments
Display whether unknown multicasts/ unicasts are being blocked	Flood control	#show interface switchport	In Web Manager, you look at the configuration.

9.5 - Storm Control

Overview

- Storm control allows the user to configure a traffic limit on a per port basis. Any traffic which exceeds the specified limit is silently discarded by the switch.

Pre-requisites

- None

Restrictions / Limitations

- None

Terminology

- **Ingress**
    - Ingress refers to frames which are entering the switch.
- **Egress**
    - Egress refers to frames which are being sent out the switch port(s).

Feature details / Application notes

- This feature allows the user to put limits on ingress and/or egress traffic
- The limits can be specified as a percentage of the bandwidth or in terms of kbps (kilobytes per second).
- The ingress traffic can be limited by frame type.
- The egress traffic is not limited by frame type. The cut-off level applies to all traffic.
- When the specified threshold is reached, the traffic is silently discarded. No indication is provided that this has occurred and the amount of discarded traffic is not tracked.

Configuration

- **Setting traffic thresholds.**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Select the port to which to apply the storm control.	Storm Control	(config)#int gi 1/4	Storm control settings are set on individual ports.

2	Define the limits.	Storm Control (port dialog box)	(config-if)#storm-control
			{ingress | egress}
			{bc | bc+mc | bc+mc+uuc}
			level
				Select the direction of traffic to control.
				Select the type of frames (only applies to ingress traffic).
				BC – Broadcast
				MC – Multicasts
				UUC – Unknown Unicasts
				Select the cut off in terms of % of bandwidth or kbps.

9.6 - Bandwidth Control

Overview

- Bandwidth Control allows the user to configure a traffic limit on a per port basis. Any traffic which exceeds the specified limit is discarded and notifications are provided to the user that this even has occurred.

Pre-requisites

- None

Restrictions / Limitations

- None

Terminology

- **Ingress**
  - Ingress refers to frames which are entering the switch.
- **Egress**
  - Egress refers to frames which are being sent out the switch port(s).

Feature details / Application notes

- This feature allows the user to put limits on ingress and/or egress traffic
- The limits are specified as pps (packets per second).
- Two limits are set;
  - Rising threshold - This is the point where the specified action is taken.
  - Falling threshold - Once traffic as dropped below this point, the next occurrence of going over the rising threshold will cause the specified action to be taken again.
- When the specified threshold is reached, the specified action is taken. The available options are;
  - Error disable the port

- Issue a trap

- When the specified threshold is reached, the switch takes the action specified in the configuration. If the action was to issue a trap, no frames are not discarded.

Configuration

- **Setting traffic thresholds.**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Select the port to which to apply the Bandwidth control.	Bandwidth Control	(config)#int gi 1/4	Bandwidth control settings are set on individual ports.

2	Define the limits.	Bandwidth Control (port dialog box)	(config-if)#bandwidth-control {ingress | egress}
			traffic {all | bc | bc+mc }
				Select the direction of traffic to control.
				Select the type of frames.
				All – all traffic
				Bc – broadcast
				Mc – multicasts
				Select the level on which to take action.
				Select the level which resets action taken flag.
				Specify action to take;
				Shutdown – Error disable the port
				Trap – send out an SNMP trap.

Monitoring and Maintaining

- **Monitoring Bandwidth Control.**

Activity	Web Manager	CLI Command(s)	Comments
Display status of Bandwidth control	Bandwidth Control Status.	#show bandwidth-control	This will provide information on parameters configured for the feature as well as the current data rate and status.

9.7 - QOS

Overview

- Normally the switch treats all packets with equal priority. With QoS, the switch can be directed to provide preferential treatment to certain types of packets over others. This can be an essential feature particularly on a congested network. The packet designated as higher priority may be delivered ahead of others and would also have a lower probability of being dropped.

Terminology

- **Output Queue**
  - The switch has 4 output queues, one for each physical port. These are pre-assigned priorities 0-3 and can be used for QoS purposes. The higher the output queue number the higher priority it is. The parameters defined in this section determine which queue an outbound packet will be placed in as well as how the switch selects packets from these queues for transmission.
- **Policy – Weighted Fair Queuing**
  - This is implemented using an algorithm that will ensure packets are transmitted from all of the queues but higher priority queues will have a heavier weighting.
- **Policy – Strict**
  - This policy ensures that higher priority packets are always sent out before lower priority ones. Packets will be sent out starting on the highest priority queue (3). When this queue is empty the switch will move on to the next highest priority queue (2) and so on.
- **CoS – Class of Service/802.1P**
  - Refers to a 3 bit field called the Priority Code Point (PCP) located in the Ethernet frame for 802.1Q messages. The priority can have a value of 0 to 7, with 7 being the highest priority. This priority is used to differentiate traffic for QoS purposes.
- **DSCP – Differentiated Services Code Point**
  - This is an 8-bit field in the IP header. This field can have values from 0 to 63, which differentiate traffic for QoS purposes with 63 being the highest priority.

Feature details / Application notes

Egress:
Each port has 4 queues for Egress (output). The switch will select frames from these 4 output queues for transmission. The method by which these frames are selected is the Policy which can be either:

- Weighted fair queueing or
- Strict

The policy setting applies to all ports.

Ingress:
When frames ingress (input) from a port, the frame will be examined to establish its relative priority. This priority will be used to move the frame into an output queue of the egressing port. There are two mapping methods for mapping a frames priority to an output queue. These are “CoS to Queue” and “DSCP to Queue”.

Each input port can be set up to use one of three prioritization schemes (QoS Trust Mode). These determine the prioritization and mapping method.

- **Disabled** – All frames will be assigned the “default priority”. A unique default priority can be assigned to each port. The default priority can be between 0 and 7. The CoS/802.1P mapping method is then used to assign the frames to a particular output queue.
- **DSCP** – If the frame contains a DSCP value, that value is used as the priority. The DSCP to Queue mapping method is used to assign the frame to an output queue. If the frame does not contain a DSCP value, the frame is assigned the default priority and the CoS/802.1p to Queue method is used to assign the frames to a particular output queue.
- **801.1p CoS** – If the frame contains a CoS value, this value is used. Otherwise, the default value is used. If the override priority is set, the default priority will be used and the CoS field in the frame will be changed to the default priority and the frame will egress with this. The CoS/802.1p to Queue mapping will be used to assign the frame to an output queue.

Configuration

- **Setting QoS parameters**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Enable QoS	Quality of Service	(config)#mls qos	
2	Setup CoS/802.1p to Queue Mapping	Quality of Service	(config)#mls qos queue output cos-map	Default Mapping CoS Output Queue 0-1 0 2-3 1 4-5 2 6-7 3

3	Setup DSCP to Queue Mapping	Quality of Service	(config)#mls qos queue output dscp-map	Default Mapping DSCP Ouput Queue 0-15 0 16-31 1 32-47 2 48-63 3
4	Setup QoS Policy	Quality of Service	(config)#fair-queue or (config)#no fair-queue	Weighted fair queue or Strict
5	Setting up a default priority for a port	Quality of Service	(config-if)#mls qos cos	
6	Setting up trust mode and override	Quality of Service	(config-if)#mls qos trust (config-if)#mls qos cos override	

Monitoring and Maintaining

- **Monitoring MAC addresses.**

Activity	Web Manager	CLI Command(s)	Comments
Display QoS Config Status	Quality of Service	#show mls qos	In Web Manager, use the configuration screens.
Display QoS Priority Maps	Quality of Service	#show mls qos maps	
Display Port Settings	Quality of Service	#show mls qos interface	

10 - Time Management

10.1 - Real Time Clock

Overview

- Date and time information is maintained on the switch using a non-volatile Real Time Clock

Pre-requisites

- None

Restrictions / Limitations

- When the switch is physically disconnected from power, the Real Time Clock is able to maintain the correct date and time information for approximately 12 – 24 hours.

Terminology

- **RTC** – Real Time Clock
  - This is specific hardware that is designed to maintain the correct date and time. Typically this type of hardware is more accurate than maintaining this information using software.

Feature Details / Application Notes

- When the switch is powered up for the first time, it typically does not have the correct date and time information. This needs to be set once. Once set, the switch will be able to maintain the correct date and time information as long as power is applied to the unit. It will maintain the correct information even if power is temporarily removed from the switch.
- A soft reset does not cause the switch to lose its date and time information.

Configuration

- Date and time information can be set via any of the following methods;
  - Fast Setup (See --> Fast Setup)
  - Manual Configuration
    - CLI
      - #clock set hh:mm:ss day month year
    - Web Manager
      - System General Settings
    - External Time Servers such as;

        - NTP (See --> NTP/SNTP)
        - PTP (See --> PTP)
- In addition, the switch provides the ability to set the time zone information.
    - CLI
        - (config)#clock timezone
    - Web Manager
        - System General Settings
            - Selecting a time zone from the list provided in the Web Manager also sets the Daylight Savings Time information.
- User can set the Daylight Savings Time information manually using the command;
    - (config)#clock summer-time

Monitoring and Maintaining

- To display the current date and time;
    - CLI
        - Show clock
    - Web Manager
        - Dashboard

10.2 - NTP/SNTP

Overview

- Network Time Protocol (NTP) is used as a method of distributing and maintaining synchronization of time information between nodes in a network.

Pre-requisites

- None.

Restrictions/Limitations

- None.

Terminology

SNTP – Simple Network Time Protocol

- A subset of NTP
- Uses the same protocol

UDP – User Datagram Protocol

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

NTP Server

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

NTP Client

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

Stratum

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

Feature Details / Application Notes

- When initially launched, it can take NTP as much as 5 minutes to obtain an accurate time. This is due to the algorithm used to determine what NTP master(s) the switch should synchronize with. NTP will not synchronize with nodes whose time is significantly different than the other nodes, even if its stratum is lower. During this "settling" period, the switch may not have the correct time.
- NTP can usually achieve time synchronization between two systems in the order of a few milliseconds. This can be achieved with a time transmission rate of as little as one packet per minute.
-
- Your IDS switch is equipped with a Real Time Clocks (RTC). The RTC can work in conjunction with NTP.
    - The RTC will enable the switch to maintain the date and time when powered down.
    - When the switch is initially powered up, the time will be retrieved from the RTC.
    - During the normal operation of the switch, NTP can be used to maintain the accuracy and synchronization of the time with the other nodes in the network as well as dealing with variations in the time due to such factors as daylight saving time.
    - The Perle IDS switch can be both an NTP Server and an NTP client. It can receive its time from another NTP server and provide this time to other NTP client nodes. In order to do this, you must configure both server and client aspects of the NTP feature.
- Time zone information.

- The time zone is not used by NTP. NTP uses UTC (Universal Coordinated Time). Time zone is only used by application displaying information to the user.

Configuration

- **Setting the switch up as an NTP client.**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Enable NTP	NTP Settings	(config)#ntp…	Any NTP command will enable NTP automatically.
2	Define NTP peers	NTP Servers / Peers	(config)#ntp peer (config)#ntp server	Specifically identifies NTP peers and / or servers. Servers and peers can provide time info. Peers can also receive time info from this switch. Allows for use of public key encryption to validate the peer.
3	Enable authentication of peers (optional)	NTP Settings	(config)#ntp authenticate	Will use PKI to authenticate peers. When defining the peer, specify which key will be used to authenticate this peer.
4	Define / enable receipt of NTP broadcasts / Multicasts	NTP Broadcast	(config-if)#ntp broadcast client (config-if)#ntp multicast client	Allow client to receive NTP broadcast. Defines specific NTP multicast addresses for client to listen for.

- **Setting the switch up as an NTP Server.**

Step	Activity	Web Manager	CLI Command(s)	Comments

1	Enable NTP	NTP Settings	(config)#ntp…	Any NTP command will enable NTP automatically
2	Define NTP peers (optional)	NTP Servers / Peers	(config)#ntp peer	Specifically identifies NTP peers. Allows for use of public key encryption to validate the peer.
3	Define broadcast / multicast parameters	NTP Broadcast / Multicast Server	(config-if)#ntp broadcast server (config-if)#ntp multicast server	Define broadcast and multicast address on which to send out the time information.

- **Configuring the switch as an NTP master.**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Enable NTP	NTP Settings	(config)#ntp…	Any NTP command will enable NTP automatically.
2	Define the stratum of the switch	NTP Settings	(config)#ntp master <stratum>	Specify how far the switch is from the “Authoritative Time Source”.

Monitoring and Maintenance

Activity	Web Manager	CLI Command(s)	Comments
NTP status	NTP Status	#show ntp status	General information about the NTP operation.
Associations	NTP Status	#show ntp associations	Information about NTP servers and peers with which the switch is communicating.

10.3 - PTP

Overview

- Precision Time Protocol (PTP) is a Layer 2 protocol (also has IP support) used to synchronize clocks throughout a computer network. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems. This is a much higher accuracy than that which can be achieved via NTP.

Pre-requisites

- None

Restrictions / Limitations

- If NTP and PTP are both enabled on the switch, NTP will take precedence.
- Example;
  - NTP is enabled and PTP is set for Boundary mode.
  - The switch's clock is not updated from the PTP sync messages.
  - Any PTP master ports will send out the system time which was updated by NTP to their PTP slave devices.

Terminology

Grandmaster clock

- A single clock source in the network to which all other clocks synchronize.
- Communicates the difference between UTC and TAI (International Atomic Time which is used by PTP) so that UTC can be computed from the received PTP time.

Boundary clock

- This is a device which receives its clock from a master clock source and then distributes the clock information to other "slave" devices connected on other ports.

Transparent clock

- Comes in two flavors.
- End-to-end and Peer-to-peer.
- Introduced in PTP V2
- Modifies the timestamps in the PTP messages to reflect the time spent traversing this device (residence time) and if peer to peer is being done, calculate the delay introduced by the path.

Feature Details / Application Notes

- PTP is a L2 protocol (also has IP support) used to synchronize clocks throughout a computer network. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems. This is a much higher accuracy than that which can be achieved via NTP. Higher accuracy is achieved if all nodes in a network participate in the protocol, but the mechanism used for delay measurements on various paths, can still achieve the accuracy even if nodes between the boundary clock and simple clock, are not PTP-enabled nodes.

- There are two versions of PTP and they are not backwards compatible.
    - V1 was written in 2002 – IEEE 1588-2002
    - V2 was written in 2008 – IEEE 1588-2008
- PTP operates on the “native” or “access” vlan of a port.
- Time is propagated to all slave ports regardless of the vlan association of the port on which the time was received from the master.
- The Perle Switch supports the following PTP modes of operation.
    - Boundary clock
        - Supported for PTP V1 and V2
        - End to End
            - Used if intermediate nodes do not support PTP
        - Peer to Peer
        - Supported for PTP V1 and V2
        - This mode of operation will elect one port on the switch to be the PTP slave port. This is the port on which the best clock master is determined to exist. The switch will accept time information on this port. The rest of the ports on the switch now become master PTP ports to the PTP slave devices connected to them. The switch will send the time information to all the PTP slave devices. The time sent to the slaves is adjusted by the average end to end or peer to peer delay.
    - Transparent clock
        - Only supported for PTP V2
        - End to End
            - Used if intermediate nodes do not support PTP
        - Peer to Peer
        - This mode of operation attempt to make adjustments to the delay introduced by the switch. The end to end setting and peer to peer setting attempt to account for delays introduced by the path (end to end or peer to peer).
        - In transparent mode of operation, we do use the time information in the PTP frames to set the switch time.
    - Forward

        - Supported for PTP V1 and V2.
        - This mode is used when we want the Perle switch to sit between two switches which are doing PTP but not getting involved in the protocol. By setting this mode, the PTP frames will be propagated through the switch as opposed to being consumed by the switch.

- For each PTP mode of operation, the following logic applies with regards to VLANs.
    - Boundary clock;
        - We receive the PTP time info on the salve port.
        - We ignore the VLAN information on the salve port and forward the PTP time on all master ports.
    - Transparent clock;
        - We record the native or access vlan on the port on which the PTP frame was received.
        - We then forward this information only to ports which have the same native or access vlan.
    - Forward mode;
        - PTP task doesn't process the frames. We just program the switch chip to handle the traffic.
        - PTP frames received on one port end up going out (untagged) on all PTP-enabled ports.

Configuration

- **Select the version of PTP to run.**

Activity	Web Manager	CLI Command(s)	Comments
Select the version of PTP to run	PTP	(config)#ptp version {1 | 2}	The rest of the parameters are dependent on the version selected.

- **PTP Version 1 settings**

Activity	Web Manager	CLI Command(s)	Comments
Set the global PTP mode of operation	PTP	(config_ptp_v1)#mode {boundary | forward}	The mode parameter sets the PTP mode of operation. Select between boundary clock or forward.

Set the PTP domain	PTP	(config ptp v1)#domain <0 – 3>	Set the domain for PTP. The valid domains are 0 – 3. Each domain operates independently of other PTP domains in the network.
Set the PTP sync interval	PTP	(config ptp v1)#sync interval <0 – 5>	Set the frequency which PTP will send out “sync messages. The valid range is 0 – 5 0 = 1 second 1 = 2 seconds 2 = 4 seconds 3 = 8 seconds 4 = 16 seconds 5 = 32 seconds

- **PTP Version 1, switchport settings**
  - The only setting available at the switch port level is the ability to enable or disable PTP on this port.

Activity	Web Manager	CLI Command(s)	Comments
Select the desired port.	PTP	(config)#in gi 1/1	Select the port on which to enable/disable PTP.
Enable/disablePTPon port	PTP	(config-if)#no ptp enable	This will disable PTP on this port.

- **PTP Version 2 settings**

Activity	Web Manager	CLI Command(s)	Comments
Set the global PTP mode of operation	PTP	(config-ptp-v2)#mode {forward | boundary-e2e | boundary-p2p | transparent-e2e [one step | two step] | transparent-p2p}	Select the PTP mode of operation. Choose the desired PTP mode of operation. For transparent-e2e, you need to select between one-step or two-step operation.

Set the PTP domain	PTP	(config-ptp-v2)#domain <0 – 127>	Set the domain for PTP. The valid domains are 0 – 127 Each domain operates independently of other PTP domains in the network.
Set the PTP transport	PTP	(config-ptp-v2)#transport Udp4 Udp6 8023	Not applicable to “forward” mode. Use IP/UDPv4 frames Use IP/UDPv6 frames User Layer 2, 802.3 frames.
Set the PTP clock priority	PTP	(config-ptp-v2)# Priority 1 Priority 2	Priority parameters are used to determine who the best clock is when running in Boundary mode. Priority 1 overrides the clock criteria (clock quality and clock class) to be used when advertising the clock. The lower the value, the more accurate the clock. In cases where there is a tie on the priority 1 value, priority 2 is the tie-breaker. The lowest value would win. If Priority 1 and priority 2 are identical, the MAC address is the tie-breaker. Lower MAC address wins.
Set the PTP clock class	PTP	(config-ptp-v2)#clock-class <0 – 255>	Clock class is used to define the accuracy of the clock based on pre-defined classes. The lower the number, the more accuracy is attributed to the clock. Used in Boundary mode. Default is 248.

- **PTP Version 2, switchport settings**
  - The following PTP parameters can be configured for each of the ports on the switch.

Activity	Web Manager	CLI Command(s)	Comments
Select the port to configure.	PTP	(config)#int gi 1/1	
Enable/disable PTP on port	PTP	(config-if)#no ptp enable	This will disable PTP on this port.

Set the “announce” message settings	PTP	(config-if)#ptp announce Interval Timeout	Announce message are used to determine who the best clock is. Only applies in boundary mode. How often to send the message. 0 = 1 second 1 = 2 seconds 2 = 4 seconds 3 = 8 seconds 4 = 16 seconds Time to wait for replies Valid range is 2 – 10 seconds
Set the “sync” message interval	PTP	(config-if)#ptp sync interval < - 1 to 1 >	Defines how often a “sync” message will be sent out. -1 = 0.5 seconds 0 = 1 second 1 = 2 seconds
Set the “delay request” message interval	PTP	(config-if)#ptp delay-req interval < -1 to 6 >	Defines how often a “sync” message will be sent out. -1 = 0.5 seconds 0 = 1 second 1 = 2 seconds 2 = 4 seconds 3 = 8 seconds 4 = 16 seconds 5 = 32 seconds 6 = 64 seconds

Monitoring and Maintaining

- To obtain information on the status of PTP use;

Activity	Web Manager	CLI Command(s)	Comments
Display PTP status	PTP status	#show ptp Clock Foreign-master-record Parent Port Time-properties	Display information on various aspects of PTP.

11 - VLANS

11.1 - Overview

VLAN (Virtual Local Area Network) is a logical grouping of devices, ports, switches and routers that permitting the segmentation of a physical network into smaller broadcast domains. VLANs are often implemented as a way of separating network traffic along functional, team or departmental lines. It is also common that VLAN's are aligned with IP subnets.

In most implementations, end devices are not aware of what VLAN they are associated with. The edge switch associate a VLAN with the port (access port) that the device is connected to. Once frames from that device enter the switch they will be tagged (assigned a VLAN ID). When they leave the switch via another access port, associated with the same VLAN, the tag will be stripped off. If the frames leave the switch on a trunk port, the tags will be maintained.

IDS switches can support up to 256 different VLAN's. A physical port on the switch can be defined as either an Access port or a Trunk port.

Pre-requisites

None

Supported VLANs

- The switch can support up to 256 VLANs
- Spanning Tree Protocol (STP and RSTP) is implemented as a unique instance on each VLAN and are VLAN unaware. MSTP is VLAN aware.
- VLAN ID 1 is defined in the switch by default. If the network does not require the used of VLANs, then the default configuration will work with all switch ports assigned to this VLAN. VLAN 1 Cannot be deleted
- VLAN ID’s 4091 and above are reserved for internal use.

Terminology

Access Port: An Access port is a physical port that is associated with single VLAN. All frames entering from this port will be tagged with the VLAN ID assigned to this port. All frames exiting this port will have the VLAN tags stripped off before the frame is sent to the connecting device.

Trunk Port: A trunk can send and receive frames from one or more VLANs. Typically frames will be tagged with their associated VLAN ID. Through configuration, you can define which VLANs a trunk port will be associated with.

VLAN ID : VLAN's are designated by a number from 1-4090. If the VLAN is not associated with any Trunk Ports then the VLAN ID can be selected arbitrarily, however if it is used on a Trunk Port, then it must match the VLAN ID used in other switches or devices.

Trunk Allowed VLANs: By default a trunk port will carry traffic from all VLANs. However you can limit the VLANs allowed on a particular Trunk port to a specific range of VLAN IDs.

Management VLAN Interface: Normally the IDS switch will pass traffic on VLANs from access port to access port or to and from Trunk ports. However if there is a need for the IDS management software to communicate to other devices on the networks (such as a Radius Server), it will need to have access to one or more VLANs. This is accomplished by enabling a VLAN interface on a particular VLAN. A VLAN interface will normally have an IP address associated with it.

SwitchPort VLAN: Is a VLAN that has Access Port or Trunk Ports associated with it, but does not have a Management VLAN Interface.

11.2 - Special VLANs

VLAN ID	Comment
1	The IDS switch comes preconfigured with VLAN 1 defined. All ports come defined as Access ports and they are all associated with VLAN 1. The IDS management function has a VLAN interface to VLAN 1.
4091-4094	Reserved for internal use
4095	Reserved for creating a VLAN isolation of the port that the PC is connected to during Fast Setup.

11.3 - Configuration

Setting up a SwitchPort VLAN

Ste p	Activity	Web Manager	CLI Command(s)	Comments
1	Define a new VLAN	VLAN List	(config)#vlan	Add a VLAN and give it a unique ID and name.
2	Associate Ports to the newly defined VLAN	Assign VLANs to Ports	(config)#Interface (config-if)#switch-port mode (config-if)#switch-port access	Include each of the ports you wish to associate to this VLAN as an Access port.

Setting up a VLAN Trunk Port

Ste p	Activity	Web Manager Screen	CLI Command(s)	Comments
1	Define a new VLAN	VLAN List	(config)#vlan	Add all VLANs to be associated with VLAN Trunk Port
2	Associate Ports to the newly-defined VLAN	Assign VLANs to Ports	(config)#Interface (config-if)#switch-port mode (config-if)#switch-port trunk	Define Port as Trunk Port Define Native VLAN ID and Allowed VLANs Note: Allowed VLANs are defined in ranges. All VLANs to be allowed on a port must have already been added in the VLAN List.

Setting up management access to or from a VLAN

Ste p	Activity	Web Manager Screen	CLI Command(s)	Comments
1	Define a new VLAN	VLAN List	(config)#vlan	Add VLANs Enable the Management VLAN Interface Option (CLI only)
2	Define IP address for each Management VLAN Interface	IP Connections	(config)#interface vlan (config-if)#ip address	Edit the selected VLAN Interface to provide IP address information. Note1: If DHCP is selected, the DHCP server must be on the specified VLAN. Note2: All VLAN Interface IP addresses must be in different subnets.

11.4 - Monitoring and Maintaining

Monitoring VLANs.

Activity	Web Manager	CLI Command(s)	Comments
Display VLAN status	VLAN Status	#show vlan	In Web Manager, use the filtering capability to display “static” entries.
Display management VLANs	IP Connections	#show interface vlan	

11.5 - Voice VLANs

Overview

- If a port is going to have a voice device such as an IP Phone attached to one of its ports, the voice information will have to be configured on that port.

Pre-requisites

- None

Restrictions / Limitations

- The switch port will need to be configured as an "Access" port.

Terminology

VVID - Voice VLAN ID

- This is the VLAN number that will be used to carry voice type information from the IP Phone.

QOS - Quality Of Service

- Refers to the attributes which define the priority scheme for packets. Voice data typically needs to be higher priority than "normal" data.

802.1P

- Protocol or specification which defines how priority information can be included in the Media Access Control (MAC) packet headers.

Feature details / Application notes

- The IDS switch supports the ability to connect an IP phone to it. The IP phone may also optionally have a PC attached to it thereby having two devices connected to the single port.
- In order to allow for both devices to operate independently of one another as well as to prioritize the voice traffic over the data traffic, the user needs to explicitly define certain attributes of the switch port.
- Optionally, the user can define a "Network Policy" which is associated with this port. The information in the Network policy will be sent to the IP phone to inform it of the correct operating parameters.

Configuration

- **Configuring the Voice parameters directly on the port**
    - When using this method the following default values are used;
        - Vlan option
            - COS value for voice data = 5
            - DSCP value for voice data = 46
        - Dot1p

- Vlan ID = 0
- COS value for voice data = 5
- DSCP value for voice data = 46

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Define the ports mode of operation.	Assign VLANs to Ports → Mode	(config)#int gi 1/1 (config-if)#switchport mode access	Set the mode to “access”
2	Define the voice vlan parameters	Assign VLANs to Ports → Voice mode	(config-if)#switchport voice vlan Number OR dot1p OR untagged OR none	Specify the voice vlan to be used. Indicate only priority info in packet. VLAN id is 0. Data and voice will use same vlan (access vlan) No voice support on port.

- **Configuring the Voice parameters using a "Network Policy"**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Define the voice application network policy parameters.	Network Policy	(config)#network-policy profile 3 (config-network-policy)#voice vlan Number OR Dot1p OR untagged OR None	Define the “voice application” parameters. Specify voice vlan number, COS priority and DSCP number. Specify COS priority and DSCP number. VLAN id for voice will be 0. Data and voice will use same vlan (access vlan). Don’t send phone any voice info. It will use parameters manually configured on the phone.

2	Optionally define the voice signaling application network policy parameters.	Network Policy	(config-network-policy)#voice-signaling {vlan | dot1p | untagged | none}	Define the voice signaling parameters.
3	Assign the network policy to the port.	Assign VLANs to Ports → Voice mode	(config)#int gi 1/1 (config-if)#network-policy 3	Assign network policy profile 3 to this port.

11.6 - GVRP

Overview

- GVRP is a protocol which learns about active VLANs and adds them to their associated interfaces.

Pre-requisites

- None.

Restrictions / Limitations

- None

Terminology

GARP - Generic Attribute Registration Protocol

- Defined by IEEE 802.1 is a protocol used to register and de-register attribute values like VLAN identifiers and Multicast group membership. The protocol defines the architecture, rules of operation, state machines and messages required to advertise information regarding the specific attributes.

GVRP - GARP Vlan Registration Protocol

- This is an application which uses GARP to specifically learn and advertise information regarding VLAN usage on interfaces.

Trunk

- A port which supports multiple VLANs.

Link Aggregation

- The logical joining of multiple physical single ports to form one larger logical data pipe.

Feature details / Application notes

- GVRP is a protocol which advertises information about VLAN usage on each interface. It also processes the information being sent by peers which enables it to learn about VLAN usage by devices connected to it.
- GVRP adds/removes VLANs from interfaces as the network environment changes.
- GVRP operates on ports which are defined as "trunks" (can support multiple VLANs).
- GVRP can be used with Link Aggregation.
- VLANs which are learned via GVRP are not saved in configuration. They are dynamically maintained on the switch. As a result, the following conditions apply;
    - A power down/up or reset will cause all VLANs learned via GVRP to be lost.
    - A copy running-configuration to startup-configuration will not save any VLAN information learned via GVRP.

Configuration

- **Setting up the GVRP environment.**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Adjust GARP timers as needed	GVRP	(config)#garp timer join leave leaveall	· Define the time to wait before advertising · a newly added vlan. · the removal of a specific VLAN · how often to ask peers for their VLAN information.
2	Define action to take when learning about a new VLAN	GVRP	(config)#gvrp dynamic-vlan-creation (config-if)#gvrp dynamic-vlan-creation	· Enable the ability to add vlans to the switch when they are learned. · Can be done on individual port basis.

3	Enable GVRP	GVRP	(config)#gvrp (config-if)#gvrp	· Enable GVRP globally. · Can be done on individual port basis.

Monitoring and Maintaining

- **Display information about GVRP**

Activity	Web Manager	CLI Command(s)	Comments
Display GVRP statistics	GVRP Statistics	#show gvrp statistics	· Number of messages received and sent for each GVRP packet type.

- **Clear GVRP statistics**

Activity	Web Manager	CLI Command(s)	Comments
Clear GVRP statistics	GVRP Statistics	#clear gvrp statistics {interface}	· Can clear all or a specific interface.

12 - Redundancy

12.1 - P-Ring

Overview

- P-Ring provides a method of connecting multiple switches in a “ring” topology which insures the ability for each switch to connect to all the other switches.

Pre-requisites

- The feature requires switches to be physically connected in a ring topology.
- Ring ports must be set to “trunk” mode of operation. This is because the ring messages use a reserved VLAN (vlan 4094). Since this vlan needs to co-exist with the “normal” VLAN being used on the port, the port must be in “trunk” mode.

Restrictions / Limitations

- P-ring can’t be enabled if MRP-ring is enabled on the same switch.
- P-ring can get its configuration from DIP switches. This method of configuring the feature is only available on the IDS-409x/509x and PoE models. For other models, the feature must be configured using software configuration.

Terminology

- **Ring topology**
  - When the switches are connected in a ring topology, each switch is connected to the two peers immediately adjacent to it. The end result is a complete ring (or circle) connecting all the switches.
- **Ring Manager**
  - This is the one switch on the ring which is in charge of monitoring the status of the ring to determine if the ring is intact or broken.
- **Ring Client**
  - All other switches on the ring aside from the one ring master are ring clients. The clients each monitor the ring to ensure that each has connectivity to all other members of the ring.

Feature Details / Application Notes

- The switches on the ring must be connected in a ring topology. This means that on each switch two ports will be used to connect to the immediate peer switches.
- You can fully configure the P-ring feature using software but you can also enable it using the DIP switch (on models which are equipped with DIP switches). To use the DIP switches to activate the feature, do the following:
  1. Ensure that the switches have been connected in a ring topology. Connection between the switches must use port 1 and port 2 on each switch.

2. On Ring master, set DIP switch S1 (Ring Master) to ON and set S2 (Backup Coupling) to OFF.
3. On Ring clients, set DIP switch S1 (Ring Master) to OFF. S2 (Backup Coupling) can be ON or OFF depending on whether you intend to use the coupling feature. (see Link Standby).

- Once the P-ring has been set up, a device on any switch will be able to connect to a device on any of the other switches. If the connection between any of the switches fails, the ability for the devices to connect will be maintained.
- If more than one link between any two switches fails, there will be some connectivity loss at this point.

Configuration

- Set the mode of the ring ports.

Activity	Web Manager	CLI Command(s)	Comments
Set the mode of the ring port	Assign VLANs to Ports	(config)#int gi 1/1 (config-if)#switchport mode trunk	· Ring ports must be set up in "Trunk" mode. · Repeat for second ring port.

- Configuring the P-ring parameters.

Activity	Web Manager	CLI Command(s)	Comments
Enter P-ring configuration mode	Ring Redundancy	(config)#p-ring	· Takes you to the P-ring configuration level.
Define the switch role	Ring Redundancy	(config-ring)#mode Manager client	· Set the role that this switch will perform on the ring. · Will monitor status of the ring. Will ensure that it has connectivity to all other switches on the ring.

Define the ports used for the ring	Ring Redundancy	(config-ring)#ring-port-1 <interface> (config-ring)#ring-port-2 <interface>	· First port used for ring connection. · Second port used for ring connection.
Enable the ring functionality	Ring Redundancy	(config-ring)#enable	· Enables the ring operation
Complete the ring configuration	Ring Redundancy	(config-ring)#save (config-ring)#exit	· Exit P-ring configuration and save the changes made. · Exit P-ring configuration without saving any of the changes.

Monitoring and Maintaining

- Display information on p-ring operation.

Activity	Web Manager	CLI Command(s)	Comments
Display P-ring status	P-ring Status	#show p-ring	· Will display status of ring as well as each of the ring ports.

12.2 - MRP

Overview

- MRP (Media Redundancy Protocol) provides fast convergence in a ring network toplolgy.

Pre-requisites

- The feature requires switches to be physically connected in a ring topology.

Restrictions/Limitations

- For convergence times of 10ms the maximum number of switches in the ring is 14.
- MRP-ring cannot run with other ring protocols (P-RING) on the same switch.
- Both ring ports must be the same mode (either access or trunk mode).
- If the port is in access mode, the access VLAN must be the same as the MRP-ring VLAN. If they are not, the MRP-ring VLAN will be automatically changed to the access VLAN of the port.
- Port channels can be used for ring ports. Ports that are part of a port channels can’t be selected as a ring port.

Terminology

- **Ring topology**
  - When the switches are connected in a ring topology, each switch is connected to the two peers immediately adjacent to it. The end result is a complete ring (or circle) connecting all the switches.
- **Ring Manager**
  - This is the one switch on the ring which is in charge of monitoring the status of the ring to determine if the ring is intact or broken.
- **Ring Client**
  - All other switches on the ring aside from the one ring master are ring clients. The clients each monitor the ring to ensure that each has connectivity to all other members of the ring.

Feature Details / Application Notes

- The switches on the ring must be connected in a ring topology. This means that on each switch two ports will be used to connect to the immediate peer switches.
- You can fully configure the MRP-ring feature using software but you can also enable it using the DIP switch (on models which are equipped with DIP switches). To use the DIP switches to activate the feature, do the following:
  1. Ensure that the switches have been connected in a ring topology. Connection between the switches must use port 1 and port 2 on each switch.
  2. On Ring master, set DIP switch S1 (Ring Master) to ON and set S2 (Backup Coupling) to OFF.
  3. On Ring clients, set DIP switch S1 (Ring Master) to OFF. S2 (Backup Coupling) can be ON or OFF depending on whether you intend to use the coupling feature. (see Link Standby).
- Once the MRP-ring has been set up, a device on any switch will be able to connect to a device on any of the other switches. If the connection between any of the switches fails, the ability for the devices to connect will be maintained.
- If more than one link between any two switches fails, there will be some connectivity loss at this point.

Autop Manager feature

In an MRP ring, you need to have one manager node and the rest of the switches must be client nodes. If you would like to have the switches figure out on their own who should be the manager node, you can set all switches on the ring to a role of “Auto Manager”.

(this is the default setting). When this is the case, the switches on the ring will arbitrate who the manager should be and elect one of the node to perform this role. The rest of the nodes will assume the client role. If at any time, the manager stops sending beacons on the ring, a new election will take place and a new node will be selected to be the manager.

If you have a ring which includes devices which do not support the “auto manager” setting, you must manually set one node to manager and the rest must be set to client.

If some nodes on the ring support the “auto manager” mode, you must set all nodes that don’t support this role to “client”. Nodes that do support the role can be set to either “auto manager” or “client”.

Autoconfig feature

When using MRP-ring as the ring protocol you are able to automatically detect and configure your switches on your ring network.

- Select one of your switches as your Manager switch
- Configure the two ring ports on that switch
- Connect all your ring ports on your other switches in your ring.
- Before connecting to your Manager Switch, run the “autoconfig” command.
- Connect the final cable to your Manager Switch.
- You will be prompted with all the switches discovered and the ring ports for those switches.

- **Example output of “autoconfig” command;**
  - The following switches were discovered
  - Mac Address: 68c9:bc1:8aad
  - Ring Port 1: Gi2
  - Ring Port 2: Gi3
  -
  - Mac Address: 68c9:bcc:5a56
  - Ring Port 1: Gi2
  - Ring Port 2: Gi3
  -
  - Configure the remote switches as MRP clients [Y/n]? Y

  - Save the config to startup-config on the remote switches [Y/n]?

- Enter Y to both questions. Your discovered switches will now be configured as MRP Clients on your RING and MRP will start running.

Configuration

Activity	Web Manager	CLI Command(s)	Comment
Enter MRP-ring Configuration	Ring Redundancy	(config)#mrp ring 1	Takes you to the MRP-ring configuration level.
Select the role of the node.	Ring Redundancy	(config-mrp)#mode Auto Manager Manager Client	- Will Automatically determine if node is manager or client. Default setting. - Fixes the role to manager - Fixes the role to client.
Define domain-id	Ring Redundancy	(config-mrp-manager)# domain-id <value> OR (config-mrp-client)# domain-id <value>	Value UUID string of 32 hexadecimal digits in five groups separated by hyphens eg. 641d931f-f1aa-50e5-b625-537564531f1f
Define domain-name	Ring Redundancy	(config-mrp-manager)# domain-name <value> OR (config-mrp-client)# domain-name <value>	domain-name can be a string of up to 32 Characters long.
Define Priority	Ring Redundancy	(config-mrp-manager)# priority <value>	Priority is an integer value between 0 - 65535
Define Profile	Ring Redundancy	(config-mrp-manager)# profile <value> OR (config-mrp-client)# profile <value>	Profile determines the maximum recovery time on the ring after a fault has been detected. Option is – 10,30,200 or 500 ms

Define Vlan-ID	Ring Redundancy	(config-mrp-manager)# vlan-id <vlan> OR (config-mrp-client)# vlan-id <vlan>	The VLAN that is used to send MRP-ring messages on the ring.
Configure Ring Port	Ring Redundancy	(config)# int gi 1/1 (config-if)# mrp ring 1	Repeat for the second ring port. When both ports are configured , MRP-ring will start.
Auto Configuration	Ring Redundancy	(config-mrp-manager)# autoconfig <value>	You must be in manager mode and your two ring ports must be configured. All cabling should be connected for the auto configuration to detect and configure your switches.

Monitoring and Maintaining

Display information on MRP Operation

Activity	Web Manager	CLI Command(s)	Comment
Display MRP Ring Status	Ring Redundancy Status	#show mrp ring 1	Displays the status of the MRP-ring
Display MRP Port Status	Ring Redundancy Status	#show mrp ports	Displays the status of the MRP ports in the ring.

DIP SWITCH HANDLING

You can fully configure RING features using the DIP Switches (on models which are equipped with DIP Switches)

Dip switches can use either P-RING or MRP-ring as the Ring protocol.
The default protocol for Dip Switches is MRP.

Activity	Web Manager	CLI Command(s)	Comment
Enable MRP as the Dip Switch Protocol	Ring Redundancy	(Config)# mrp ring 1	Enables MRP as the Dip Switch Protocol.

Enable P_RING as the Dip Switch Protocol	Ring Redundancy	(Config)# p-ring	Enables P-RING as the Dip Switch Protocol.

For a complete description of DIP Switch settings see Chapter 2, Dip Switch Settings.

12.3 - Ring Coupling

Overview

- Ring coupling involves having a ring attached to another ring or network using two links which provides redundancy for the coupling.

Pre-requisites

- None

Restrictions / Limitations

- One of the two sides being coupled must be a ring.
- Ability to enable feature via DIP switches is only available on models which support DIP switches.

Terminology

- **Physical subsystem**
  - This feature allows for the coupling of a ring to a ring or a ring to a network. Within the scope of this feature, the ring or network being coupled will be referred to as a physical subsystem.
- **Primary link**
  - This is the link which is used to couple the two physical subsystems (ring to ring or ring to network). Data transferred between the two travels over this link.
- **Backup link**
  - This is the redundant link. If the primary link fails, this link will become active and will be the link used to transfer data between the two physical subsystems.
- **Control link**
  - A physical link between the two switches on the same physical subsystem which is used to communicate statuses and control between the two switches on the on physical sub-system.

Feature details / Application notes

- This is a two switches to two switches coupling scenario. This means that one switch on one physical subsystem is connected to a switch on the second physical subsystem. A second switch on the first physical subsystem is connected to a second switch on the second physical subsystem.
- The ring ports on the ring act as the control channel to inform the other switch on the ring as to the status of the primary and backup links. Optionally the user can define a different port on the switch to perform this function.
- In the case of a failure on the primary link, all learned addresses on this link will be removed. The backup link will now re-learn the addresses as it sees them.
- When the link comes back up on the primary link, the backup link resumes its role as backup and traffic moves back to the primary link.
- If the DIP switches are used to enable the coupling feature, the coupling port is fixed to port 4. The ring ports are used as the "control port".
- The feature also supports an "extended redundancy mode". This allows the one physical subsystem to detect if the link between the two switches on the other physical subsystem has been broken. If this is the case, both the primary and backup link are used to transfer data to the second physical subsystem.

Configuration

- **Setting up ring coupling.**

Activity	Web Manager	CLI Command(s)	Comments
Define the parameters of the coupling.	Ring Redundancy	(config-if)#switchport backup coupling Active Standby Control-port <int> Extended-redundancy	· Command is executed on the switchport interface which is going to be used to couple to the other physical subsystem. · Indicates this is the "primary" link · Indicates this is the "backup" link. · Optionally specify which port will be used as the "control port". · · Specify "extended redundancy" feature will be used.

Optionally enable mac-move messages.	Ring Redundancy	(config)#mac address-table move update Receive Transmit	· Enables the use of a Perle proprietary message to inform other switch about all MAC address which exist on this link. Both switches must be Perle switches. · Enable processing of a received move message · Enable the sending of a move message.

Monitoring and Maintaining

- **Displaying status of coupling feature**

Activity	Web Manager	CLI Command(s)	Comments
Show the status of the coupling	Ring Coupling Status	#show interfaces switchport backup detail	· Display information on the status of the coupling. · If this keyword is specified, more details are provided.

12.4 - Spanning Tree

Overview

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

Pre-requisites

- None

Restrictions / Limitations

- None

Terminology

STP - Spanning Tree Protocol

- A layer 2 protocol which identifies and eliminates loops in your network. It is detailed in the IEEE 802.1D specification.

RSTP - Rapid Spanning Tree Protocol

  - This is an enhanced version of the STP protocol which allows for faster detection and correction of loop conditions. It is detailed in the IEEE 802.1w specification. It is compatible with switches running the STP protocol.

- Multiple Spanning Tree Protocol
  - This is an enhanced version of the RSTP protocol which allows for handling of multiple VLANs. A separate instance of spanning tree is used for each vlan. It is detailed in the IEEE 802.1Q-2005 specification. It is compatible with switches running the STP or RSTP protocol.

Feature details / Application notes

- RSTP is enabled by default on all ports of the switch.
- Spanning tree implementation based on port type;
  - Access port
    - If all switch ports are on the same VLAN, there will be a single instance of STP/ RSTP against all ports.
    - If switch has more than one vlan defined on different access ports, we will run multiple instances of STP/RSTP. One against each VLAN.
  - Trunk port
    - If switch port is defined as a trunk and user configured STP or RSTP on port, we will actually run "PVST+" on the native trunk vlan
      - PVST+ - Same as STP but uses a different multicast address
        - If the peer is a Perle switch, this will work fine since even if they configure STP or RSTP on the peer, it will actually run PVST+.
        - If the peer is a Cisco switch, this will also work fine since Cisco runs PVST+ on trunk ports.
        - If the peer is a different vendor, they will;
          - Either need to configure the trunk for PVST+ (if they can).
          - We still run STP or RSTP on the native vlan. (PVST+ on native and all other vlans).
        - STP and PVST+ multicasts propagate to all ports on the switch (even if STP is not enabled on the port).
    - If another port has an access vlan which is defined on a trunk, the access port still runs STP.
    - If "MSTP", is configured it will run against all ports in the switch.

- Spanning tree is support on port-channels.

Configuration

- **Global spanning tree settings**

Activity	Web Manager	CLI Command(s)	Comments
Configure the protocol	Spanning Tree Settings	(config)#spanning-tree mode STP RSTP MSTP	- Configure the protocol to use - Spanning Tree Protocol - Rapid Spanning Tree Protocol - Multiple Spanning Tree Protocol
Guard against port-channel misconfiguration	Spanning Tree Settings	(config)#spanning-tree etherchannel guard misconfig	- Turns on detection of getting BPDUs with different MAC addresses in them on a port channel. This is an indication that we are configured for port channel but the peer is not. - If this condition is detected, the port channel will be shut down. - Default is "off"
Set the path cost method	Spanning Tree Settings	(config)#spanning-tree pathcost method Long Short	- Only applicable to STP - All nodes in network need to use the same method. - Uses a calculation to determine path cost. - Uses a build in table to calculate the path cost. - Default is "long".

Set the transmit hold count	Spanning Tree Settings	(config)#spanning-tree transmit hold-count <count>	· Only applicable to RSTP · Configures the number of BPDUs transmitted per second before pausing for 1 second. · Valid range is 1 - 20. Default is 6.
Set the maximum hops	Spanning Tree Settings	(config)#spanning-tree max-hops <count>	· The maximum number of hops that a BPDU is valid for. · Valid range is 6 - 40. Default is 20
Set the maximum aging time	Spanning Tree Settings	(config)#spanning-tree aging -time <count>	· The time in seconds for aging out dynamically learned forwarding information. · Valid range is 10 - 1,000,000 seconds. The default is 300 seconds.
Enable the loopguard feature	Spanning Tree Settings	(config)#spanning-tree loopguard default	· This causes additional checks to be made before a port moves from blocked to listening/learning/ forwarding state. · STP determines that a port is not a candidate for a loop if it does not detect BPDU messages on it for a certain amount of time. With loop guard, when this happens, the port transitions to a "loop-inconsistent blocking" state.

Enable the portfast BPDU filter	Spanning Tree Settings	(config)#spanning-tree portfast Edge Network Normal	· Enabling Portfast immediately puts the interface into spanning tree forwarding mode. · Should only be set on a port directly connected to a server or workstation. · Indicates port is connected to an end node. · Enables "bridge assurance" logic. If the port does not receive a BPDU for a specific time period, it moves to an "inconsistent" state (blocking). · Indicates that the port topology is not configured (could be edge or network). This is the default.
Enable the portfast BPDU guard	Spanning Tree Settings	(config)#spanning-tree edge bpduguard default	· This enables bpduguard on all portfast enabled ports. · When bpduguard is enabled, if a BPDU is received on the port, the port is shut down.

- **Defining MST parameters**
  - Allows the user to define the parameters of a single MST instance.
  - This collection of parameters of the MST instance is identified as a "Region".

Activity	Web Manager	CLI Command(s)	Comments

Enter the MST configuration mode.	Multiple Spanning Tree Settings	(config)#spanning-tree mst configuration	· Takes you to the mst configuration level which is identified with the prompt "(config-mst)#
Define the name of the region	Multiple Spanning Tree Settings	(config-mst)#name	· The name can be 1 - 32 characters long.
Define the revision number for the region	Multiple Spanning Tree Settings	(config-mst)#revision	· A number between 0 – 65535
Define the instance(s) for the region	Multiple Spanning Tree Settings	(config-mst)#instance <number> vlan <range>	· The region can have multiple instances. · Each instance has a vlan or range of vlans which is associated with it.

- **Interface specific spanning tree settings**

Activity	Web Manager	CLI Command(s)	Comments
	Spanning Tree Settings		·
Enable BPDU	Spanning Tree Interface Settings	(config-if)#spanning-tree { enable | disable }	· Enable / Disable the processing of received BPDUs on this port.

Change the "guard" mode	Spanning Tree Settings	(config-if)#spanning-tree guard Loop None Root Topology-change	· Set the spanning tree guard mode for interface. · If BPDUs are not received, the port moves into the "loop-inconsistent" blocking state instead of listening/learning/ forwarding state. · No special guard handling. · Guard against the device attempting to become root. · Restrict the sending of Topology Change Notifications on interface.
Enable auto transition from RSTP to STP	Spanning Tree Interface Settings	(config-if)#spanning-tree mcheck	· When enabled, the port will send out RSTP for 3 seconds. Allows it to identify if the peer is running RSPT or STP.
Set the link type	Spanning Tree Interface Settings	(config-if)#spanning-tree link-type Point-to-point shared	· Identifies the type of connection on this port. · Only a single device is connected. · Multiple devices are connected on this port. · Default is "point-to-point"

Set the port type	Spanning Tree Interface Settings	(config-if)#spanning-tree portfast Disable Edge Network	· Determines which states interface will transition through · Goes through normal learning/forwarding/ blocking states. · Interface goes into forwarding state immediately. Will not send BPDUs out this port. If you add "trunk" after "edge", it will behave similarly · Interface goes into forwarding state immediately. Will send out BPDUs on this interface and may go blocking in the future.
Set the maximum hops	Spanning Tree Settings	(config-if)#spanning-tree max-hops <count>	· The maximum number of hops that a BPDU is valid for. · Valid range is 6 - 40. Default is 20
Set the maximum aging time	Spanning Tree Settings	(config-if)#spanning-tree aging -time <count>	· The time in seconds for aging out dynamically learned forwarding information. · Valid range is 10 - 1,000,000 seconds. The default is 300 seconds.
Set the port priority	Spanning Tree Settings	(config-if)#spanning-tree port-priority (config-if)#spanning-tree vlan port-priority	· Set the priority for the port. · Set the priority for this port on this vlan. · Range is 0 - 240. Default is 128

Set the port path cost	Spanning Tree Settings	(config-if)#spanning-tree cost (config-if)#spanning-tree vlan nnn cost	· Set the path cost for the port. · Set the path cost for this port on this vlan. · Range is 1 - 200,000,000. Default is 2,000,000

Monitoring and Maintaining

12.5 - Link Aggregation

Overview

- Link aggregation is the combining of two or more ports to form one logical pipe. This is typically used to connect two switches. It provides for increased bandwidth.

Pre-requisites

- None

Restrictions / Limitations

- Some features can not be used on link aggregated ports. Refer to the individual features to determine if they support link aggregated ports.
    - Example, ports configured for 802.1x can not be part of a port channel.

Terminology

- **Port Channel**
    - This is the name given to the logical entity which is the aggregation of the individual ports.

- **LACP - Link Aggregation Control Protocol**
    - This is a protocol used between switches to dynamically negotiate whether a port will be part of the port channel.

Feature details / Application notes

- In order to combine ports into a port channel, the individual port must have some common attributes. If a port is included in a port channel but does not have matching attributes to the other port in the port channel, that port will be suspended. The following is a list of attributes that must be the same for all ports which are included in a port channel.
    - VLAN mode (access or Trunk).
    - Access vlan or Native VLAN (trunk mode)

  - Vlan range (trunk mode)
  - Block multicast
  - Block unicast
- Up to 8 ports (if available in your hardware mode) can be included in a port channel.
- The number of port channels a switch can have is equal to;
  - Number of ports(rounded down to even number) / 2
- Port channels can be configured to have one of the following behaviours with regards to negotiating with their peer, the participation in the individual ports within the group;
  - Static
    - No negotiation with peer. The port is always part of the port channel.
  - Active
    - The port will initiate LACP negotiation with peer as well as responding to LACP negotiation initiated by the peer.
  - Passive
    - The port will NOT initiate LACP negotiation with peer but will respond to LACP negotiation initiated by the peer.
- LACP priorities.
  - The LACP system priority is used when two systems are attempting to determine who will be the "master" of the LACP negotiations. The system with the lower "system priority" number will become master. If both switches have the same system priority value, the switch with the lowest MAC address will become the master.
  - The port LACP priority only gets used if we have more ports assigned to a port channel than the maximum number allowed (8). In that case the LACP port priority is used to determine which ports will be included in the port channel. The ports with the lower LACP port priority are selected first.

Configuration

Activity	Web Manager	CLI Command(s)	Comments

Add a port to a new or existing port channel.	Switchport Settings (Add Port Channel) button.	(config)#int gi 1/1 (config-if)#channel-group <1 - 16> Mode Static active passive	· Select the port you wish to add to the port channel. · Select the port channel number · Select the mode · No LACP · Initiate LACP · Respond to LACP · All ports which are included in the same port channel must be set to the same mode.
Configure system LACP priority	Switchport Settings (Add Port Channel) button.	(config)#lacp system-priority <0 - 65535>	· The lower number wins.

- You can set all ports in the channel interface to common settings as follows;

Activity	Web Manager	CLI Command(s)	Comments
Set parameters for all port in port channel	Switchport Settings (Add Port Channel) button. Interface Settings tab.	(config)#int port-channel <#> (config-if)#	· Select the port channel you wish to edit. · Under the port channel interface you will find a number of parameters that can be set for all ports which are members of the port channel. · ? · In Web, you need to go to the actual feature and set the associated parameters under the port channel interface under that feature.

Monitoring and Maintaining

- There are a number of show commands which provide information on the Link Aggregation feature.

Activity	Web Manager	CLI Command(s)	Comments
Display LACP status.	Port Status (Pox interface)	#show lacp <port channel number> {counters | internal | neighbor | sys-id}	· Can display LACP protocol information for a specific port channel.

Display detailed port channel info	Port Status (Pox interface)	#show interface port-channel <port channel number> {accounting | counters | description |flowcontrol | mtu |stats |status | summary | switchport}
		#show etherchannel <port channel number > {detail | port | port-channel | summary}
		#show interface etherchannel
			· Can display detailed information on various aspects of link aggregation for a specific port channel.
			· Can also use these commands to get similar information.

12.6 - Link Standby

Overview

- This features provides for connecting two network segments using two links which provides redundancy in case one of the links fails.

Pre-requisites

- None

Restrictions / Limitations

- None

Terminology

- **Primary link / Active link**
  - This is the link which is used to couple the two network segments. Data transferred between the two travels over this link as long as the link is up.

- **Backup link / Standby link**
    - This is the redundant link. If the primary link fails, this link will become active and will be the link used to transfer data between the two network segments.

Feature details / Application notes

- At any given time, only one of the two port involved (active and standby) is forwarding traffic. The other port is blocked.
- If the "active" link goes down;
    - Port security is not enabled (on active port or backup port).
        - Dynamically learned addresses are copied to the backup port.
        - Static addresses are not copied. User needs to configure the static addresses on both ports.
    - If Port security is enabled on Active port or on Backup port
        - Dynamically learned addresses are not copied to the backup port and are deleted from the active port.
        - Secure Static addresses are not copied. User needs to configure the static addresses on both ports.
    - The switch sends out notification to upstream switches to allow them to learn the new path to the devices on the switch. There are two ways to do this.
        - First method is to send out a multicast with the source address of each MAC address the switch has learned on all of its other ports.
        - The second is to use a "MAC move" message.
            - This uses a proprietary message to relay all the MAC addresses reachable on this port to the upstream switch. This message contains multiple MAC address and vlan information in one message.
            - Advantage of this method is the fact that you can send information on multiple MAC addresses in one message.
            - The method to use is defined by the "mac address-table move…" command.
- After a switchover, if the active link come back up, one of two things can happen;
    - It becomes the "standby" link.
    - It can resume its role as the "active" link.
    - This behavior is controlled by configuring the "pre-emption" mode. See below.
- Fast convergence feature
    - When this is enabled, the backup port sends out an IGMP query reports out on the backup link. When the switchover happens, the upstream switches already know about the multicast addresses.
    - If the feature is not enabled, on a switchover, the switch will issue an IGMP query report at the time of the switchover.
- Preemption
    - This defines the behavior of the switch back from the backup/standby port to the active port.
        - User can configure the delay before switching back.
        - User can delay under what conditions the switchback will occur

- Off
  - Will not switch back until a failure occurs in the backup link
- Forced
  - Will always switch back to the active interface when it is operational
- Bandwidth
  - Prefer the link with the higher bandwidth. If the bandwidth is the same, no switchback will occur.

- Link standby is supported on port-channel interfaces.

Configuration

- Configure the various parameters of the Link Standby feature as follows;

Activity	Web Manager	CLI Command(s)	Comments
Select the "active" port	Link Standby (click on a port channel)	(config-if)#int gi 1/3	· All configuration is performed on the active port of the link standby feature.
Define the operating parameters for the ports.	Link Standby	(config-if)#switchport backup interface <int> Mmu Multicast preemption	· Define which interface will be the "backup" port · Specify which vlan will be used for the "MAC move" message. · Enable the "fast convergence" feature. · Set the parameters for preemption.
Optionally enable the MAC move functionality	Link Standby	(config)#mac address-table move update receive Transmit	· · · Only process received MAC Move messages. · · Send out MAC move messages.

Monitoring and Maintaining

- Displaying the Link Standby status

Activity	Web Manager	CLI Command(s)	Comments
Display status of Link Standby	Link Standby Status	#show intertfaces switchport backup {detail}	· If the keyword detail is omitted, it provides a higher level status for the feature.

13 - Operations and Monitoring

The IDS switch line provides the user with the ability to quickly view the overall heath and manage the operation of the switch.

13.1 - General Information

Overview

- The user can obtain the general information about the switch

Pre-requisites

- none

Restrictions / Limitations

- none

Terminology

- none

Feature details / Application notes

General information can be obtain about the switch in a single web manager or CLI view

Configuration

- none

Monitoring and Maintaining

Display general information

Activity	Web Manager	CLI Command(s)	Comments

Display general information on the switch	Monitor/System/General Information	#show sysinfo	· Last alarm: displays whether there is an active alarm or not. If there is an alarm, the last alarm detected will be displayed. · System description: the description of the switch · System name: Host name of the switch · System location: location description · System contact: contact description · System up time: in hours, minutes and seconds · System date: YYYY-MM-DD Time and timezone · Running software version: Firmware version running in memory · Running software build date: Build date of the running firmware · Start-up software version: startup firmware version stored in flash that will load as the running version upon the next reset or reboot · Start-up software build date: Build date of the startup firmware · Backup software version: Version of the firmware that was backed up in flash · Backup software build date: Build date of the backup firmware · Bootloader version: Version of the bootloader · Bootloader build date: Build date of the bootloader · Hardware revision: Revision number of the hardware Model name: Perle model · Part number: orderable Perle part number · Base MAC address: Base MAC

13.2 - RMON Statistics and Counters

Overview

Remote Monitoring RMON is a standard monitoring specification that defines a set of statistics and functions that can be exchanged between RMON-compliant console systems and network probes.

The RMON feature is used with the Simple Network Management Protocol (SNMP) agent in the switch to monitor all the traffic flowing among switches on all connected LAN segments.

Pre-requisites

- none

Restrictions / Limitations

- An SNMP server on the network is required

Feature details / Application notes

The following RMON groups are supported;

Group 1 - Ethernet statistics

- real-time LAN stats: per ethernet interface
  - (received: bytes/packets, packet sizes, collisions, broadcast/multicast packets)

Group 2 - History

- history of network stats for selected interface over time intervals (of a specified length)
  - includes network utilization (%) over given time interval

Group 3- Alarm

- Compares values against a threshold and generates alarms when exceeded.

Group 9 - Event

- Action to be taken when an event is triggered by an alarm.
- define where alarms, defined in group 3, are to be sent.

Configuration

- None required. RMON is settable through the SNMP server

Monitoring and Maintaining

RMON statistics can be viewed by the CLI

Activity	Web Manager	CLI Command(s)	Comments

View RMON data	N/A	#show rmon #show rmon alarms #show rmon events #show rmon history #show rmon statistics	· Display summary of RMON data · Display RMON alarms · Display RMON events · Display RMON history · Display RMON statistics

13.3 - Port Status and Statistics

Overview

- The IDS switch provides the administrator with the ability to monitor port status and statistics.

Pre-requisites

- none

Restrictions / Limitations

- none

Terminology

Feature details / Application notes

Port Status: displays an overview status for each individual port.

- Port enabled/disabled
- Link: Up or down
- Link State: Connected (Forwarding or blocked) or Not-Connected
- VLAN Mode: Access or trunk port
- VLAN ID: VLAN IDs associated with this port
- MAC address:
- Duplex: Full/half/Auto
- Speed: 10/100/1000/Auto
- Media type: 10/100/1000Base-TX, 1000Base-X, 100Base-X, 1000BaseX-SFP
- EEE Status: For IDS 200 and 300 series models which support Energy Efficient Ethernet, this displays whether EEE is enabled or disabled
- MTU: Maximum MTU size allowed
- Unknown unicasts: Unblocked or blocked
- Unknown multicasts: Unblocked or blocked

Port statistics are provided for each individual port

- Received and transmitted count : bytes, packets, unicasts, multicasts and broadcasts
- Undersized and oversized packets
- Collisions and late collisions
- CRC Errors
- Deferred packets
- Frame Errors
- Pause frames (the switch does not originate pause frames)
- Packet Sizes: count for each frame size range

1 - 64
65 - 127
128 - 255
256 - 511
512 - 1023
1024 - Max

Port Flow Control

- Displays how the port is operating in terms of flow control. Admin represents what was configured and operational is what the port was negotiated to

VLAN

- Port mode is an access or trunk
- Access VLAN ID
- Voice VLAN ID if configured

Bandwidth on transmit and receive

- Number of packets dropped
- Rate in bits/sec
- Rate in packets/sec

Configuration

- See Port Setup

Monitoring and Maintaining

Activity	Web Manager	CLI Command(s)	Comments
Display general port status	Monitor/Ports/Port Status	#show interface status	Displays for each port ; Link state VLAN ID Duplex Speed Media Type

	Monitor/Ports/Port Status	#show interface stats or #show interface accounting	Displays port transmit and receive statistics
	Monitor/Ports/Port Status	#show interface description	Displays description of configured for each port
	Monitor/Ports/Port Status	#show interface *<interfaceID>*	Displays full summary of details for a specified port

13.4 - Port Mirroring

Overview

- Port Mirroring is the ability to send packets coming in or going out a port to a second port. This is used mainly when you want to do a packet trace on a port.

Pre-requisites

- None

Restrictions / Limitations

- None

Terminology

Source port (in context of this feature).

- The source port is the port for which we are interested in seeing the traffic from.

Destination port (in context of this feature).

- The destination port is the port to which the copied packets will be sent.

Feature details / Application notes

- The main difference between a hub and a switch is the ability for the switch to localize traffic to a port or ports to which it is intended to go. This helps reduce unneeded traffic on other ports. A side effect of this behaviour is that it makes it impossible to connect up with an Ethernet traces and get a packet trace of the traffic.
- Port Mirroring solves this problem by allowing the user to select the port or ports that they are interested in (source port) and have the packets from these ports sent to a destination port (as well as the original port they were intended for.
- For each source port, the user can select between seeing the received data, transmitted data or both.

Configuration / Operation

- Configure the feature

Web Manager	CLI Command(s)	Comments

Port Mirror	(config)#monitor session <sess #> Source | destination direction	Define a session which includes one or more source ports, a destination port and the type of traffic being monitored (i.e. TX, RX or Both).

- Using the feature
  - Once the traffic is being duplicated to the "destination" port, you simple need to connect a tracing tool to that port and capture the packets coming out of it.

13.5 - Virtual Cable Test

Overview

- Virtual Cable Test is a test which is run on a copper cable in an attempt to identify potential breaks in the cable.

Pre-requisites

- None

Restrictions / Limitations

- None

Terminology

CAT5/6 - Category 5 or Category 6 cable.

- This is the specification for copper Ethernet cables. Different categories are used depending on the speed and distance of the connection.

Feature details / Application notes

- Virtual Cable Test (VCT) technology enables the diagnosis of a conductor (wire or cable) by sending a pulsed signal into the conductor, then examining the reflection of that pulse. This method of cable analysis is referred to as Time Domain Reflectometry (TDR). By examining the reflection, the IDS switch can detect and report on potential cable issues.
- CAT5/6 cable contains 4 sets of two wires which are twisted together. The VCT tests each of the pairs and reports on whether they are physically intact.
- The test will report the status of each of the cables individually.

Initiating the test

Web Manager	CLI Command(s)	Comments
Virtual cable test	#test cable-diagnostic interface gi 1/1	· Select the interface you wish to test.

14 - Diagnostics

- The IDS switch provides a number of utilities which can be used to diagnose various issues regarding the operation of the switch or the network.
- The following diagnostic tools are available in the IDS switch;
  - Port Mirroring
    - See "Port Mirroring" section for details.
  - Virtual Cable Test
    - See “Virtual Cable Test” section for details.
  - RMON Statistics and Counters.
    - See "RMON Statistics and Counters" section for details.
  - SFP DOM/DMI display
    - See "SFP" section for details.
  - Enable debug messages
    - The user can enable debug on specific code modules in order to collect more information on what that specific module is doing.
    - This is available via the CLI command "debug <function>" where function can be any of the following;
      - 802.1x authenticator
      - 802.1x supplicant
      - Alarm Manager
      - Alert Manager
      - Enable all debugging
      - Bandwidth-control
      - Command Line Parser
      - Console Manager
      - DHCP client
      - DHCP relay agent
      - DHCP server
      - Device Manager
      - DSA driver
      - GARP
      - GMRP
      - GVRP
      - IGMP
      - Interface Manager
      - Init - Initialization
      - IP address conflict detection
      - Kernel
      - Link aggregation

- LLDP
- Logging Manager
- MLD
- Modbus TCP server
- Profinet
- Profinet DCP
- PSLVM switch driver
- PTP - Precise Time Protocol
- Ring
- SNMP
- spanning-tree
- Trap Manager
- VTY - Telnet and SSH sessions

§ Debug command does not survive a re-boot.

- Ping
  - Provides the ability to test IP connectivity to a device.
  - Able to ping by IP address or host name.
    - If host name is used, the switch will attempt to resolve the name using the switch host table or DNS.
  - User can also specify the following optional parameters;
    - Data
      - Actual payload to be sent within the ping message
    - Repeat
      - Number of times to send the ping
    - Size
      - Size of the datagram
  - The command is;
    - #ping {IP or name} {data , repeat, size}

- Traceroute
  - This utility displays each hop on the path to the final destination including the time it took to reach that hope and return.
  - It is used in cases where the destination can't be reached. This utility will help identify at what point the routing to the destination fails.
  - The command is;
    - Traceroute <IP or name>

- Technical info display
  - This collects information on various aspects of the switch.

- It can be used to provide Perle Technical support personal with technical information on your switch.
- The command is;
  - Show tech-support
- You should capture the output of this command and send it in to the technical support person.

15 - DHCP Relay, ARP, LLDP and Trace

15.1 - DHCP Server

Overview

- The IDS switch can act as a DHCP server to the devices connected on its ports or other devices which can access it on the network.

Pre-requisites

- None

Restrictions / Limitations

- None

Terminology

DHCP Pool

- A pre-defined grouping of IP addresses from which the DHCP server can assign IP addresses to clients.

DHCP lease

- A DHCP lease defines the duration for which an IP address assigned to a DHCP client, is valid for. When the lease expires, the DHCP client must not continue to use the IP addresses assigned to it.

DHCP Relay Agent

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

Feature details / Application notes

- When assigning an IP address to a client, the DHCP server can optionally attempt to ping the address being assigned to ensure that it is not currently in use. If the request was received via a DHCP relay agent, the pings are not issued since the client is typically in a different subnet.
- When the DHCP server receives a DHCP request from a DHCP relay agent with a “giaddr” missing or zero but the option 82 information is included, the normal action would be to discard this packet.
  - This behaviour can be modified via the command;
    - (config)#ip dhcp relay information trust-all

- When the DHCP server receives a DHCP request from a DHCP relay agent with a “giaddr” missing or zero but the option 82 information is included, the normal action would be to discard this packet.
  - This behaviour can be modified via the command;
    - (config)#ip dhcp relay information trust-all

- The server can be set up to provide DHCP clients with an IP address from a generic pool or it can be set up to provide specific IP addresses to specific DHCP clients. The following criteria can be used to select which IP pool or address is assigned to the DHCP client;
  - Port request came from
  - VLAN request came from
  - Client ID
  - MAC address
  - Giaddr
  - Option 82 info
- The following attributes can be associated with a pool and returned to the DHCP client;
  - Bootfile
  - Default router
  - Domain name
  - DNS server
  - Netbios name server
- You can set up one or more DHCP pools on the server. The pools fall into two main categories;
  - Network pool
    - This is a pool to be used for multiple clients.
    - Within this pool, you can assign specific IP addresses to specific clients using the “client-id” or “client hardware” information.
  - Client specific poll
    - Used for a specific client.
    - Can enter a variety of information to be used for this one client.
- User can define a “class”. A class has relay agent information and a class-id in it. This class can then be assigned to a dhcp pool.

Configuration

- Setting up the switch to be a DHCP server.

Activity	Web Manager	CLI Command(s)	Comments

Enable DHCP server on switch	DHCP Server	(config)#service dhcp server	The no version of the command will disable the service. Command can also be entered on a switchport or VLAN interface.
Enable IP address conflict detection	DHCP Server	(config)#ip dchp ping Packets <nnn> Timeout <tttt>	Before assigning an address to a client, attempt to ping it to see if it is already in use. Number of times to send the ping Time to wait for response in milliseconds.

- Setting up a DHCP address pool.

Activity	Web Manager	CLI Command(s)	Comments
Create a DHCP pool	DHCP Pools	(config)#ip dhcp pool <pool name>	Create the pool
Assign various attributes to the pool	DHCP Pools (Edit DHCP pool)	(dhcp-config)#	At this level you can set up a number of parameters for this pool. Some parameters are not available if the “network” parameter is used. This is because these parameters are used to define attributes about one single client.

- Setting up a port based DHCP allocation.

Activity	Web Manager	CLI Command(s)	Comments
Set subscriber ID to use client ID	DHCP Server	(config)#ip use subscriber-id client-id	If no subscriber-id is configured on the interface, then the client-id is automatically generated as the short name of the interface (i.e. gi 1/2). For port based allocation, user should not configure the subscriber-id on the interface. The client-id already present in the incoming message is ignored.

Define the pool to use the client-d	DHCP Pools (Edit DHCP pool)	(dhcp-config)#address <ip addr> client-id asci gi1/2	This associates the specified ip address with the client id "gi1/2" which will be assigned to requests coming in on port gi ½

Monitoring and Maintaining

- Display existing lease information

Activity	Web Manager	CLI Command(s)	Comments
Display the currently assigned leases	DHCP Server Status	#show ip dhcp binding	
Display pool info	DHCP Pool Status	#show ip dhcp pool <poolname>	If poolname is omitted, display info on all pools.

- Release an IP address which exists in the lease file
  - This should only be done if you know that the client is not still be using this IP address.

Activity	Web Manager	CLI Command(s)	Comments
Remove an assigned IP address from the lease file	DHCP Server status	#clear ip dhcp binding <ip address> <*>	Remove a specific IP address from the lease file. Remove all IP addresses from the lease file

15.2 - DHCP Relay

Overview

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

Pre-requisites

- None

Restrictions / Limitations

- None

Terminology

DHCP Relay Agent

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

GIADDR

- If a DHCP request has been forwarded by a DHCP relay agent, the address of this relay agent is included in the request in the "giaddr" field.

Feature details / Application notes

- The DHCP Relay agent does not transparently forward DHCP requests to the DHCP server. It receives the DHCP request from the client and generates a new request which is forwarded to the DHCP server. The relay agent will include additional information in the DHCP request which provides the remote DHCP server with information on where the request is coming from so that the correct IP address can be assigned to the DHCP client. This information includes;
    - “giaddr” field
        - The IP address of the VLAN interface which received the original DHCP request.
    - Optionally, can include a “DHCP option 82” field.
        - The command to enable/disable the insertion of the option 82 field is;
            - (config)#ip dhcp relay information option-insert
                - Default is disabled (don’t insert).
            - Command can also be issued under the vlan interface.
    - The option 82 information can include the following;
        - “Remote-ID” (sub option 2)
            - MAC address of the VLAN (default)
            - This can be changed to any of the following using the “(config)#ip dhcp relay information option remote-id ….” Command;
                - Vlan <#>
                    - IP
                        - IP address of one of the management VLANs.
                    - MAC
                        - MAC address of one of the management VLANs or switch port interfaces.
                - Hostname
                    - Hostname of the switch

      - Hex string
        - A hex string of up to 63 bytes
  - “Circuit-ID” (sub option 01)
    - Consists of the following;
      - VID – VLAN id of the interface the original DHCP request was received on. (two bytes)
      - Slot number – The slot number associated with the port the original DHCP request was received on. (one byte)
      - Port number – The port number of the port the original DHCP request was received on. (one byte)
- o If the switch receives a packet which already contains an option 82 field, it can take one of the following actions;
  - Drop - The frame is discarded. (default action)
  - Keep – The frame is forwarded with the received option 82 information.
  - Replace – Replace the option 82 information and forward the frame.
  - The above action can be set using the command;
    - #ip dhcp relay information policy
    - This command can be issued globally or on a per interface basis.

- The DHCP relay functionality is enabled on an interface by defining the “ip helper-address” parameter on the interface.
  - o (config-if)#ip helper-address <ipaddr>
  - o This tells the IDS switch where to forward DHCP requests which are received on this interface.

Configuration

- Set up the global DHCP relay agent parameters.

Activity	Web Manager	CLI Command(s)	Comments
Enable/disable DHCP relay function.	DHCP Relay Agent	(config)# service dhcp relay-agent	Default is enabled.
Enable/disable the sending of the option 82 field.	DHCP Relay Agent	(config)# ip dhcp relay information option-insert	Default is not to send the option 82 field.

Define behaviour when receiving a DHCP request which already includes an option 82 field	DHCP Relay Agent	(config)# ip dhcp relay information policy {drop | keep | replace}	Define the action to take.
Define contents of the “remote-ID” field in the option 82 field.	DHCP Relay Agent	(config)# ip dhcp relay information option remote-id {vlan<#> [IP | MAC] | hostname | hex string}	Select the value to be sent for the “remote-id” field of the option 82.

- Setting up the management interface specific DHCP relay agent parameters.

Activity	Web Manager	CLI Command(s)	Comments
Enable/disable DHCP relay function.	DHCP Relay Agent Interface	(config)#int vlan <#> (config)# service dhcp relay-agent	Select the vlan interface you wish to configure. Default is the global setting.
Enable/disable the sending of the option 82 field.	DHCP Relay Agent Interface	(config)#int vlan <#> (config-if)# ip dhcp relay information option-insert	Select the vlan interface you wish to configure. Default is not to send the global setting.
Define behaviour when receiving a DHCP request which already includes an option 82 field	DHCP Relay Agent Interface (Reforwarding policy)	(config)#int vlan <#> (config)# ip dhcp relay information policy {drop | keep | replace}	Select the vlan interface you wish to configure. Define the action to take.

- Setting up the address(es) of the remote DHCP server(s).

Activity	Web Manager	CLI Command(s)	Comments
Add address of remote DHCP server for this vlan.	IP Helper Addresses	(config)#int vlan <#> (config-if)#ip helper-address <ipaddr>	Select the vlan interface you wish to configure. Define the address of the remote DHCP server(s) for this management VLAN.

15.3 - ARP Table Management

Overview

- The ARP table holds information on the association between IP addresses and MAC addresses. This table is maintained by the management software and is used strictly for management functions .

Pre-requisites

- None

Restrictions / Limitations

- None

Terminology

ARP - Address Resolution Protocol

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

Age-out

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

Feature details / Application notes

- The ARP table can consist of "static" and "dynamic" entries.
    - Static entries are ones configured by the user.
    - Dynamic entries are learned by the software
- Dynamic entries will age out if we have not seen a message from that device in the time specified by the ARP age-out parameter.
- Static entries do not age-out.
- Configuring an ARP entry in the switch will prevent the software from "arping" for a host name or IP address.
- This is sometimes used as a security measure to ensure that the switch does not use a MAC address which may have been provided by an imposter who responds to he ARP request with his MAC address thereby causing the messages to come to them.

Configuration

- Adding an ARP entry to the table.

Activity	Web Manager	CLI Command(s)	Comments
Add an ARP entry	Static ARP Table	(config)#arp IP MAC vlan	Add an ARP entry to the ARP table IP address associated with this entry The MAC address of the specified IP address The vlan that this IP address is associated with.

- Setting the ARP table age-out for dynamic entries

Activity	Web Manager	CLI Command(s)	Comments
Set the ARP age-out	ARP Time-out	(config)#arp time-out <time>	Set how long dynamic address will be maintained in the table. The time can be from 1 - 34560 minutes.

Monitoring and Maintaining

- Displaying the "arp" information in the switch.

Activity	Web Manager	CLI Command(s)	Comments
Display the ARP table	ARP Status	#show arp <CR> IP address vlan	Can display ARP entries for; All ARP entries Specific IP address All entries for a specific VLAN.

15.4 - LLDP

Overview

- LLDP is a layer 2 protocol which is used to advertise information about the switch/interface to its immediately connected peer.

Pre-requisites

- None

Restrictions / Limitations

- None

Terminology

- **LLDP** - Link Layer Discovery Protocol
  - LLDP is a vendor-neutral, link layer protocol used by network devices for advertising their identity, capabilities, and neighbors on an local area network.
- **LLDP-MED** - Link Layer Discovery Protocol - Media End-point Discovery
  - Used to exchange information about network devices such as phones (used within a VoIP architecture).
- TLV - Type Length and Value
  - This is the format used by LLDP and LLDP-MED to convey the various attributes (information) about the switch and port.

Feature details / Application notes

- Device discovery protocols such as LLDP and LLDP-MED enable directly connected devices to discover information about each other thereby allowing any device in the network to "know" everything it is connected to. Some examples of applications that use this type of info include:
  - Network management systems (NMS) can use this information to accurately represent a map of the network topology.
  - In a VoIP scenario, voice configuration information can be sent to the phone using LLDP-MED.
  - Since location information can be included in the information sent out, emergency services an use this information to identify the physical location of devices.
  - In PoE environments, the PSE and PD can negotiate the power that the PD will consume.
- The user can configure which specific attributes they want sent out to the peer. The available attributes include;
  - Port Description
  - System Name
  - System Capabilities

  - System Description
  - Management Address (IP address)
  - Port VLAN
  - MAC PHY configuration and status
  - Power management (PoE models only)
  - Link aggregation
  - Maximum frame size
  - These parameters can be enabled on a port by port basis.

- If Profinet is enabled, the following additional TLV are supported.
  - Profinet Port Status
    - TLV 0x000ECF, subtype 0x02
  - Profinet alias
    - TLV 0x000ECF, subtype 0x03
  - Profinet MRP
    - TLV 0x000ECF, subtype 0x04
  - Profinet chassis
    - TLV 0x000ECF, subtype 0x05

- LLDP-MED adds the ability to define location information in the form of a "civic address" as well as emergency location information in the form of a phone number.
  - The user can configure a number of attributes of the Civic address such as;
    - Street number
    - Street name
    - City
    - Country
  - Just to name a few. This can be defined globally for the switch but can also be defined individually for each port on the switch. Doing this allow the switch to provide individual information about each device connected on a port.

Configuration

- **Configure and Enable LLDP**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Configure the LLDP protocol parameters.	LLDP Settings	(config)#lldp Hold-mult Notification-interval Transmit delay Reinit Timer Tx-delay	Set the various LLDP protocol parameters.
2	Select global switch attributes to advertise.	LLDP Settings	(config)#lldp tlv-select	Pick the attributes to advertise to peer.
3	Select global switch attributes to advertise.	LLDP Settings	(config)#lldp run	Globally enable LLDP

- **Override global LLDP parameters on a port basis.**

Step	Activity	Web Manager	CLI Command(s)	Comments
1	Select the port you wish to configure.	LLDP Interface Settings	(config)#int gi 1/3	Pick the port
2	Select mode of operation for this port.	LLDP Interface Settings	(config-if)#lldp receive (config-if)#lldp transmit (config-if)#lldp max-neighbors	Enable receive and/or transmit. Define maximum numbers of peers to collect info on.

3	Select the attributes you wish to advertise and/or accept on this port	LLDP Interface Settings	(config-if)#lldp tlv-select	Pick the attributes to advertise to peer.
4	Optionally define specific location information for port.	LLDP Interface Settings (LLDP-MED tab)	(config-if)#location civic-location-id (config-if)#location elin-location	Can specify a "global" civic location as the base and then override or add specific elements for this interface.
5	End the configuration for port.	Apply button	(config-if)#exit	

Monitoring and Maintaining

- **Reviewing peer information.**

Activity	Web Manager	CLI Command(s)	Comments
Display information collected on each peer on each port.	LLDP Status	#show lldp #show lldp int gi 1/3 #show lldp neighbors #show lldp traffic	Global protocol info. Port specific protocol info. Peer information Protocol message counters.

- **Enable logging**

Activity	Web Manager	CLI Command(s)	Comments
Enable LLDP logging	LLDP Settings	(config)#lldp logging	Provide LLDP specific logging.

15.5 - LLDP Med

Overview

- This protocol is used to collect and distribute Media Endpoints such as IP Phones and PoE devices.

Pre-requisites

- None.

Restrictions / Limitations

- LLDP-MED frames are only sent out if we receive an LLDP-MED frame. This ensures that LLDP-MED frames are only exchanged with media end points.

Terminology

LLDP-MED - Link Layer Discovery Protocol - Media Endpoint Discovery

- The standards based protocol used to discover information about and distribute information to devices directly connected to the switch.

Feature details / Application notes

- Automatically deploys network policies such as Layer 2 and 3 QOS policies and voice VLANs.
- Collects endpoint inventory information.
- LLDP-MED supports the following classes of endpoints
  - Class 1
    - Generic
    - Basic participant endpoints such as IP communications controllers
  - Class 2
    - Media
    - Endpoint that support media streams such as media gateways and conference bridges
  - Class 3
    - Communication Device
    - Endpoints that support IP communications end users such as IP phones.
- The switch is a "Network Connectivity" device type. This is LLDP-MED Device type of 4.
- Can communicate the following type of information
  - Determine the capabilities of the connected device
  - LAN
    - Speed
    - duplex
  - Network connectivity
    - VLAN
    - COS
    - DSCP
  - Power info (on Models supporting PoE)
    - How is the device powered
    - Power priority
    - How much power does device need
  - Inventory management
    - Hardware revision

- Firmware revision
- Software version
- Serial number
- Manufacturer name
- Model name
- Asset ID

o Location

- Civic address, postal code
- ELIN location - caller location. (phone number that emergency services can call back on)

Configuration

- **Defining a voice Network Policy (see --> "Voice VLANs")**
- **Defining Location information**

Activity	Web Manager	CLI Command(s)	Comments
Define Emergency location info	LLDP Settings (LLDP-MED tab)	(config)#location elin-location	Can define multiple ELIN location info record.
Define Civic location info	LLDP Settings (LLDP-MED tab)	(config)#location civic-location <loc name> (config-civic)#	Define the location to be configured. Define location parameters for this location. You can enter multiple parameters for a single location.

- **Defining Port Specific LLDP-MED information**

Activity	Web Manager	CLI Command(s)	Comments

Assign the LLDP-MED parameters to a port	LLDP Interface Settings (LLDP-MED tab)	(config)#int gi 1/1 (config-if)#lldp med-tlv-select Location Network-policy	Select the infterface to apply settings to. Apply desired LLDP-MED parameters to the interface.

Monitoring and Maintaining

- **Viewing LLDP-MED information (See--> "LLDP")**

15.6 - Ping and Traceroute

Overview

- Ping and Traceroute are tools which can aid in diagnosing connectivity issues.

Pre-requisites

- None

Restrictions / Limitations

- None

Terminology

- **Ping**
  - Ping is a protocol based on ICMP which is used to test the reachability of a host on an (IP) network. It measures the time it takes for messages sent from the originating host to a destination computer including the response from the destination.
- **Traceroute**
  - Traceroute is a tools which attempts to display the path which is taken by a packet traveling from the host on which the command is executed to a destination normally reachable via IP routing. It uses ICMP messages to do this. If destination is not reachable, the utility will display how far the message was able to travel.
- **ICMP - Internet Control Message Protocol**
  - ICMP is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be

reached. It is also utilized by ping and traceroute.

Feature details / Application notes

- The Perle IDS switch provides both Ping and Traceroute.
- Ping
  - The ping utility will accept the following parameters
    - Destination
      - This can be specified via;
        - Name (resolvable via DNS or host table)
        - IPv4 address
        - IPv6 address
    - Payload
      - The data to be sent in the Ping message
    - Size of payload
      - Valid range is 36 - 18024 bytes
      - Default is 64 bytes
    - Number of repetitions
      - Valid range is 1 - 2147483647
      - Default is 10
  - If a name was specified, the utility will first attempt to resolve the name to an IP address. If this can't be done, an error message is provided.
  - Next, the utility will attempt to send the ICMP message to the destination host. If this is received by the host, he will respond to the sender. The send / response sequence is one repetition of the ping command.
  - Each repetition is timed. This information is displayed for each successful request.
  - After the requested number of repetitions has been completed, the utility provides a summary of how many requests were sent, how many responses were received and the min/avg/max round-trip times.
- Traceroute
  - The traceroute utility accepts single parameter which is the destination we are attempting to reach. This parameter can be specified as;
    - Name

  - § IPv4
  - § IPv6

- o If a name was specified, the utility will first attempt to resolve the name to an IP address. If this can't be done, an error message is provided.
- o It will then attempt to communicate with the next hop in the path (i.e. default router/ gateway). If this is successful, it will attempt to communicate with the next hop in the path. This is repeated until it either reaches the destination or fails to reach one of the hops on the way.
- o As the attempts are being made, the utility displays the results of each attempt including timing information.
- o The utility will display an "*" to indicate a hop can't be reached.

16 - Industrial Protocols

16.1 - Modbus

Overview

- The Modbus feature allows the user to read a number of parameters from the switch using the Modbus protocol. The list of registers is provided at the end of this chapter.

Pre-requisites

- This feature was introduced in version 1.4 of the Perle-IDS.

Restrictions / Limitations

- None

Terminology

- **RTU -**Remote Terminal Unit
  - The device which is typically monitored by the supervisor of the Modbus network.

- **SCADA -** Supervisory Control And Data Acquisition systems
  - This is what the system which comprises of a supervisor and one or more RTUs which are monitored by the supervisor.

- **MSB -** Most Significant Byte
  - The MSB of 0xABCD is 0xAB

- **LSB -**Least Significant Byte
  - The LSB of 0xABCD is 0xCD

- **Big-endian**
  - Defines the order in which bytes are ordered.
  - In big-endian byte ordering, the most significant byte is transmitted first and the least significant byte is transmitted last.

- **Data types**
  Modbus uses 16 bit registers to transfer data. Each register holds 2 bytes, arranged in big-endian order. In order to transfer larger types of data (e.g. 64-bit integers), multiple registers are used.
  - Uint16
    - Unsigned 16 bit integer
  - Uint64
    - Unsigned 64 bit integer
  - Text
    - One or more ASCII bytes representing a character or string.

Feature details / Application notes

- For a complete list of parameters which can be read via Modbus, see “Modbus Registers” at the end of this section.

Configuration

- Configuring the SNMP parameters.

Activity	Web Manager	CLI Command(s)	Comments
Enable Modbus	Configure Modbus Modbus Server	(config)#scada modbus tcp server	Enable/Disable Modbus. Use the “no” version of the CLI command to disable Modbus. Modbus is disabled by default.
Set up the Modbus TCP port.	Modbus Modbus Server	(config)#scada modbus tcp server port <nnnnn>	This is the TCP port number that the Modbus Server will listen on for Modbus connection requests. Default is 502.
Define the number of connections	Modbus Modbus Server	(config)#scada modbus tcp server connections <n>	Define how many simultaneous Modbus connections will be allowed to be established. Range is 1 - 5 Default is 1

Monitoring and Maintaining

- Displaying the status of Modbus.

Activity	Web Manager	CLI Command(s)	Comments
Show Modbus status	Monitor Modbus Modbus Server status	#show scada modbus tcp server	Will display information on the Modbus Server as well as specific connection information if there is an established Modbus connection.
Clear statistics	Modbus Modbus Server status	#clear scada modbus tcp server statistics	Will cleare the statistics for the Modbus server. Can also clear statistics for one or more Modbus connection.

Modbus Registers

- Modbus global registers.

Address	# of registers	Description	Format
0x0000	64	Vendor Name	Text
0x0040	64	Software Image Name	Text
0x0080	64	Software Image Version	Text
0x00C0	64	Product Name	Text
0x0100	64	System Name	Text
0x0140	64	Serial Number	Text
0x0180	64	Uptime (days, hours, minutes)	Text
0x0200	64	Alarm 1 Description	Text
0x0240	64	Alarm 2 Description	Text
0x0300	1	Power Supply 1 Status (1=good, 0=bad)	Uint16
0x0301	1	Power Supply 2 Status (1=good, 0=bad)	Uint16
0x0302	1	Alarm relay status (1 = alarm, 0 = no alarm)	Uint16
0x0303	1	Alarm input 1 (1=alarm, 0=no alarm,2=no digital input.	Uint16
0x0304	1	Alarm input 2 (1=alarm, 0=no alarm,2=no digital input.	Uint16
0x0305	1	System Temperature (in Celsius)	Int16

- Modbus port information registers.

Address	# of registers	Description	Format
0x1000	64	Port 1 Name	Text
0x1040	64	Port 2 Name	Text
0x1080	64	Port 3 Name	Text
.....	....	Additional ports, up to the number of ports supported by your switch.	Text

0x1FC0	64	Port 64 Name	Text
0x2000	1	Port 1 Status 0 = link down, 1 = link up 2 = link disabled, F = no port	Uint16
0x2001	1	Port 2 Status 0 = link down, 1 = link up 2 = link disabled, F = no port	Uint16
.....	....	Additional ports, up to the number of ports supported by your switch.	Uint16
0x203F	1	Port 64 Status 0 = link down, 1 = link up 2 = link disabled, F = no port	Uint16
0x2040	4	Port 1 Statistics, packets received	Uint64
0x2044	4	Port 2 Statistics, packets received	Uint64
.....	....	Additional ports, up to the number of ports supported by your switch. If port does not exist, returns a zero value.	Uint64
0x213C	4	Port 64 Statistics, packets received	Uint64
0x2140	4	Port 1 Statistics, packets sent	Uint64
0x2144	4	Port 2 Statistics, packets sent	Uint64
.....	....	Additional ports, up to the number of ports supported by your switch. If port does not exist, returns a zero value.	Uint64
0x223C	4	Port 64 Statistics, packets sent	Uint64
0x2240	4	Port 1 Statistics, bytes received	Uint64
0x2244	4	Port 2 Statistics, bytes received	Uint64
.....	....	Additional ports, up to the number of ports supported by your switch. If port does not exist, returns a zero value.	Uint64
0x233C	4	Port 64 Statistics, bytes received	Uint64

0x2340	4	Port 1 Statistics, bytes sent	Uint64
0x2344	4	Port 2 Statistics, bytes sent	Uint64
.....	....	Additional ports, up to the number of ports supported by your switch. If port does not exist, returns a zero value.	Uint64
0x243C	4	Port 64 Statistics, bytes sent	Uint64

16.2 - Profinet

Overview

- Profinet is one of the protocols used to monitor and control equipment in an industrial environment. It allows for centralized control of various vendor’s equipment using a common protocol.

- Profinet IO is the protocol used to communicate between PLCs and Profinet enabled devices. This is the version of the Profinet protocol that the IDS supports. This document refers to Profinet IO simply as Profinet.

Pre-requisites

- This feature was introduced in version 1.4 of the Perle-IDS.

Restrictions / Limitations

- When Profinet is used to manage MRP, native MRP configuration on the switch is disabled.

Terminology

- **I/O Device**
  - This is the role the IDS plays in a Profinet network.

- **I/O Controller (Programmable Logic Controller)**
  - The PLC runs automation programs. It can setup and monitor I/O devices such as the switch.

- **I/O Supervisor**
  - A management PC/station used to commission, monitor or diagnose devices.

- **DCP (Discovery and Configuration Protocol)**
  - A protocol which is used to discover Profinet enabled devices and set up a basic set of parameters on that device.

- **GSM file**
  - An XML based file which describes the device and its capabilities. It is used by the Profinet management software.

- **Cyclical data**
  - Information which is sent between the device and the controller. This information is continuously exchanged at a regular interval typically around 128 - 512 ms.

Feature details / Application notes

- The IDS switch is a Class B conformance Profinet device and supports both RT class 1 (real time) as well as non-time critical, TCP/IP version of the protocol.

- The Profinet protocol can be used to discover and configure IDS switches using DCP (Discovery and Configuration Protocol).

- Profinet can also be used to configure and monitor the Media Redundancy Protocol (MRP).

Configuration

Global configuration

Activity	Web Manager	CLI Command(s)	Comments
Enable Profinet	Configure Profinet	(config)#profinet	Enable/Disable Profinet. Use the "no" version of the CLI command to disable Profinet.
Set up the VLAN number for Profinet.	Configure Profinet	(config)#profinet vlan <nnnn>	This is the vlan which will be used for Profinet communications with PLC. Default is 1
Set up the Profinet "Name of Station".	Configure Profinet	(config)#profinet id <text>	This is sometimes referred to as "Chassis ID" or "Profinet ID". Up to 240 characters Only special characters "." and "-" are allowed. Last character can't be zero. Default is blank
Define if Profinet MRP is used.	Configure Profinet	(config)#profinet mrp	If this field is enabled, MRP will be fully configured and operated by the PLC. Any MRP configuration configured on the switch will be lost.
Define the DCP settings	Profinet DCP Boundary Settings	(config)#profinet dcp block egress	For each port, the user can enable or disable the following DCP options. • Block outgoing DCP Identity frames • Block outgoing DCP Hello frames. Blocking these frame types will prevent them from being send out on the associated port.

Monitoring and Maintaining

To see the Profinet status select “Monitor--> Profinet Status” from navigation menu on the Web Manager.
The status is divided into three sections.

Status

- Provides general Profinet information

Alarms

- Provides the following global alarm information;
  - Redundant Power Source detected
  - Primary temperature alarm
  - Secondary temperature alarm
  - Relay engaged
  - SD card inserted
- Provides the following port alarm information;
  - Link Fault
  - Not forwarding
  - Not operating

Sessions

- Provides information on any connected Profinet sessions.

GSD file

The switch has a copy of the Profinet GSD file as well as the various Icon files associated with each DAP. This file can be uploaded to your Profinet management system. Select “Administration--> File Management --> Profinet GSD file” from navigation menu on the Web Manager.

Switch Parameterization

When the PLC first connects to the IDS, it will perform a “Parameterization” operation on the switch. This sets up basic operating parameters. The following parameters can be set during this process.

Global Parameters

- Redundant power supply alarm
  - Option: Monitored / not monitored / no change
- Primary temperature alarm
  - Option: Monitored / not monitored / no change
- Primary temperature alarm, high threshold
  - Range: -150 to 300, default is 95
- Primary temperature alarm, low threshold
  - Range: -200 to 250, default is -20
- Secondary temperature alarm
  - Option: Monitored / not monitored / no change
- Secondary temperature alarm, high threshold
  - Range: -150 to 300, default is 95
- Secondary temperature alarm, low threshold

    - Range: -200 to 250, default is -20
- Relay major alarm
    - Option: Monitored / not monitored / no change
- SD card alarm
    - Option: Monitored / not monitored / no change
- PoE alarm
    - Option: Monitored / not monitored / no change

Port Specific Parameters

- Link fault alarm
    - Option: Monitored / not monitored / no change
- Port not forwarding alarm
    - Option: Monitored / not monitored / no change
- Port is not operating alarm
    - Option: Monitored / not monitored / no change
- Speed / Duplex
    - Various selections of speed and duplex combinations.
- Port enabled
    - Option: Enabled / Disabled / no change
- Port mode
    - Option: Access / Trunk / no change
- Ingress storm control enable
    - Option: Enabled / Disabled / no change
- Ingress storm control frame type
    - Option: BC / BC+ MC / BC+ MC+UUC
- Ingress storm control maximum level
    - Range: 0 to 100 percent, default 25 percent
- Relay major trigger
    - Option: None / Port link fault alarm / Port not forwarding alarm / Port is not operating alarm / no change (default)

17 - Power Over Ethernet

Overview

- Some models of the The IDS switch support the ability to power other devices connected to their copper ports via the Ethernet cable. The IDS switch itself can't be powered via PoE, it is strictly a Power Sourcing Device (PSE).
- The IDS has two flavours of PoE switches;
  - PoE and PoE+ capable switches
    - IDS-509xPP
  - PoE, PoE+ and PoE++ capable switches
    - IDS-710HP

Pre-requisites

- The IDS switch model must be one of the PoE models.

Restrictions / Limitations

- In order to act as a PSE device, the IDS switch much be powered with a minimum of 44Volts. This requirement varies depending on the class of PD being connected. See next section for details.

Terminology

- **PoE**
  - Defined by 802.3af-2003
  - Allows for up to 15.4W per device
  - 12.95W is available at the PD due to power dissipation in the cable
  - Voltage ranges - 44 - 57V (37 - 57 at the PD)
- **PoE+**
  - Defined by IEEE 802.3at-2009
  - Allows for up to 30W per device
  - 25.5W is available at the PD due to power dissipation in the cable
  - Voltage ranges - 50 - 57V (42.5 - 57 at the PD)
- **PoE++**
  - Defined by IEEE 802.3bt-2018
  - Type 3
    - Allows for up to 60W per device
    - 51W is available at the PD due to power dissipation in the cable

        - Voltage ranges - 50- 57V (42.5 - 57 at the PD)
    - Type 4
        - Allows for up to 100W per device
        - 71W is available at the PD due to power dissipation in the cable
        - Voltage ranges - 52- 57V (41.1 - 57 at the PD)
- **PD - Powered Device**
    - A device which is powered (over the Ethernet cable) by a PSE
- **PSE - Power Sourcing Equipment**
    - A device which sources power over the Ethernet cable to a PD

Feature Details / Application Notes

- The PoE feature is enable by default on PoE capable IDS switches. The user can disable this capability at the port level.
- The IDS switch maintains a “Power Budget”. This is the amount of power available at any given time to be allocated to a PD. As power is granted to devices, the amount available is decreased by the amount granted. The user can control the amount of power given to devices as well as the priority of the devices via configuration parameters. (see configuration below).
- The PoE specification defines 8 classes of Powered Devices as follows;
    - Class 0
        - Power from PSE: 15.4 Watts
        - Power at PD: 0.44 - 12.94 Watts
        - 0 - 5 mA
        - 5 - 8 mA may be class 0 or 1
    - Class 1
        - Power from PSE: 4 Watts
        - Power at PD: 0.44 - 3.84 Watts
        - 8 - 13 mA
        - 13 - 16 mA may be class 1 or 2
    - Class 2
        - Power from PSE: 7 Watts
        - Power at PD: 3.84 - 6.49 Watts
        - 16 - 21 mA
        - 21 - 25 mA may be class 2 or 3
    - Class 3

        - Power from PSE: 15.4 Watts
        - Power at PD: 6.49 - 12.95 Watts
        - 25 - 31 mA
        - 31 - 35 mA may be class 3 or 4
    - Class 4
        - Power from PSE: 30 Watts
        - Power at PD: 12.95 - 25.5 Watts
        - 35 - 45 mA
        - 45 - 51 mA may be class 4 or invalid class
    - Class 5
        - Power from PSE: 45 Watts
        - Power at PD: 40 Watts
        - 36 - 44 mA and 1 - 4mA
    - Class 6
        - Power from PSE: 60 Watts
        - Power at PD: 51 Watts
        - 36 - 44 mA and 9 - 12mA
    - Class 7
        - Power from PSE: 75 Watts
        - Power at PD: 62 Watts
        - 36 - 44 mA and 17 - 20mA
    - Class 8
        - Power from PSE: 99 Watts
        - Power at PD: 71.3 Watts
        - 36 - 44 mA and 26 - 30mA
- LLDP (Link Layer Discovery Protocol)
    - This protocol can be used after the initial power up of a PD to fine tune the power requirements of the PD.
    - This allows a PD which does not necessarily require as much power as is defined by its class to request less power.
    - A PD may also request more power than is specified by its class and if that power is available in the power budget, it will be granted to the requesting PD.
    - If we are operating in PoE mode (not PoE+ mode), the maximum that will be granted to a device (regardless of what it requests) is 15.4W.

- Alarms
    - The following alarm conditions are monitored by the PoE feature.
        - Over-temperature
            - If the temperature of the PoE chip exceeds the manufacturer defined limit, this alarm is triggered
            - The PoE chip automatically will shut down under this condition
        - Under-voltage
            - If the supply voltage to the IDS switch drops below the 44V minimum specified by the PoE specification, this alarm is triggered
    - When one of the above conditions occur, the user can specify which of the following action is to be taken.
        - Disable PoE on the port
        - Send an SNMP trap
        - Trigger the relay
        - Send a Syslog message
- 802.3bt (PoE++) specific features
    - Dual signature detection
        - A 802.3bt capable PD can appear as two separate PoE devices each presenting a separate PoE class. The IDS can automatically detect the class of “device” and individually assign it power based on the class detected for each.
    - Autoclass
        - An 802.3bt capable PD, can use “autoclass” to provide the PSE with the maximum amount of power that it requires. This can be done at power up or any time via the LLDP protocol.
        - The PD signals that it wishes to do “autoclass”. At this point, the PD is consuming the highest level of power which it will need. The PSE measures the amount of power being used by the PD and this becomes the maximum amount that will be budgeted for this PD. The fact that this is based on an actual measurement, takes into account the actual voltage drop over the cable. In the case of a short cable, this could reduce the amount of power that the PSE needs to provide to the PD since not much loss will occur over the cable.
    - Power Down
        - A 802.3bt capable PD may request the PSE to power it down. This is done using the LLDP protocol. This can be an indefinite power down or a timed power down. (maximum power down time is 72 hours).

Configuration

- Set the global parameters for PoE.

Activity	Web Manager	CLI Command(s)	Comments
Set the total PoE budget	PoE Settings	(config)#power inline wattage <Watts>	Specify the total amount of power available for PoE devices. Please note that the IDS will consume some of the power being supplied to it for running itself. The amount of power varies depending on the model and usage.
Set the default consumption	PoE Settings	(config)#power inline consumption default <mWatts>	Define how much power to give to an “unknown” PD device class
Set overall consumption threshold	PoE Settings	(config)#power inline usage-threshold <%nn>	When the PoE consumption reaches this percentage of total budget, a trap and syslog will be issued.
Override input power validation	PoE Settings	(config)#power inline no-input-validation	If the power input to the IDS switch falls below 44V (PoE) or 50V (PoE+) no PoE power will be supplied to PD devices. This command overrides this behavior.
Action on overdrawn condition	PoE Settings	(config)#power inline retry	This is the action to take if there is not enough power left in the budget to power the PD. Option are; • Error-disable the port. • Retry immediately. • Retry on next connect.

- The following parameters can be set for individual PoE ports.

Activity	Web Manager	CLI Command(s)	Comments
Select the port to operate on	PoE Port Settings	(config)#int gi 1/1 (config-if)#	Select a port.
Enable/Disable PoE on a port	PoE Port Settings	(config-if)#power inline never	The never option will disable PoE on the port. Use the “no” version of the command to enable PoE on the port.

Set PoE mode of port	PoE Port Settings	(config-if)#power inline {auto | static}	Auto • Enable PoE detection. • If enough power is available, allocate it to the device. Static • Pre-allocate power for the device (even before detection). • In both cases above, the user can optionally specify the maximum amount of power to allocate to the device.
Set maximum power for port	PoE Port Settings	(config-if)#power inline consumption <mWatts>	The amount to give a device regardless of its class or LLDP request.
Set the priority of the port	PoE Port Settings	(config-if)#power inline priority {low | high | critical}	When there is not enough power to allocate to a port, the port with a lower priority will relinquish its power to a port which has a higher priority setting.
Set action to take in overdrawn condition	PoE Port Settings	(config-if)#power inline police action {errdisable | log}	When there is not enough power to allocate to a port, the port will be powered down. User can configure what additional action to take in this condition.

Monitoring and Maintaining

- Display information on PoE operation.

Activity	Web Manager	CLI Command(s)	Comments
Display PoE status	Power over Ethernet Status	#show power inline {consumption | dynamic-priority | police | interface | <CR>}	For each of the PoE parameters, the user can optionally specify an interface to display that interface specific information.

18 - PerleView

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

PerleVIEW Device Management System is an Enterprise-grade, multi-user, Windows server-based centralized management package that simplifies the configuration, software upgrade, administration, monitoring, and troubleshooting of Industrial Switches in medium to large-scale deployments. Network Administrators, using their Internet Browser, can securely access PerleVIEW and manage 10’s, 100’s or thousands of Perle switches from a centralized server. There is no user client software required to be installed on administrator’s PCs. The management of the Perle device network is simplified by using PerleVIEW to:

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

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