Contents

Contents

Contents

1

Window Navigation

Getting Started

Managing RMON

RMON (Remote Networking Monitoring) is an SNMP specification that enables an SNMP agent in the device to proactively monitor traffic statistics over a given period and send traps to an SNMP manager. The local SNMP agent compares actual, real-time counters against predefined thresholds and generates alarms, without the need if Ma2:i cgen2r4-ail( )]TJ1854642 0 TD.0017 Tc-.0424 Tw[S)2-2.4NsMP r

- **Collisions**—Number of collisions received. If Jumbo Frames are enabled, the threshold of Jabber Frames is raised to the maximum size of Jumbo Frames.
- **Frames of 64 Bytes**

To enter RMON alarms:

RAM Memory

This section covers the following topics:

- **Upgrade/Backup Firmware/Language**
-

Select one of the following **Save Actions**:

- **Upgrade**—Specifies that the file type on the device is to be replaced with a new version of that file type located on a TFTP server.
- **Backup**

Administration: File Management

Configuration Files Properties

- The SSH Server is configured in the SSH Trusted Servers list.

If the SSH server authentication process is enabled, and the SSH server is not found in the SSH Trusted Servers list, the Auto Configuration process is halted.

The following table describes the various models, the number and type of ports on them and their PoE information.

Administration: General Information

System Information

- **HTTPS Service**—Displays whether HTTPS is enabled/disabled.

To view the device health parameters, click

Manual Settings—Set the date and time manually. The local time is used when there is no alternate source of time, such as an SNTP server:

- **Date**—Enter the system date.
- **Local Time**—Enter the system time.

Time Zone Settings—The local time is used via the DHCP server or Time Zone offset.

- **Get Time Zone from DHCP**—Select to enable dynamic configuration of the time zone and the DST from the DHCP server. Whether one or both of these parameters can be configured depends on the information found in the DHCP packet. If this option is enabled, you must also enable DHCP client on the device.

  NOTE The DHCP Client supports Option 100 providing dynamic time zone setting.

- **Time Zone from DHCP**—Displays the acronym of the time zone configured from the DHCP server. This acronym appears in the

- **From**—Day and time that DST starts.
- **To**—Day and time that DST ends.

Selecting *Recurring*

7

Administration: Discovery

Administration: Discovery

- **VLAN Tag**—Select whether the traffic is Tagged or Untagged.
- **User Priority**

Administration: Discovery

Configuring LLDP

Administration: Discovery

- **CDP Hold Time**—Amount of time that CDP packets are held before the

- **Syslog Voice VLAN Mismatch**—Select to enable the option of sending a SYSLOG message when a voice VLAN mismatch is detected This means that the voice VLAN information in the incoming frame does not match what the local device is advertising.
- **Syslog Native VLAN Mismatch**

- 1000 Full—1000 Mbps speed and Full Duplex mode.

Configuring LACP

A dynamic LAG is LACP-enabled, and LACP is run on every candidate port

Port Management

Port Management

10

Using CDP/LLDP Information to Identify Smartport Types

The device detects the type of device attached to the port, based on the CDP/LLDP capabilities.

This mapping is shown in the following tablesF010.4/TT2 1 Tm/Cs6 cs .14118 .47843 .56

For more information about LLDP/CDP refer to the

Smartport

Configuring Smartport Using The Web-based Interface

- **guest**
-

Smartport

11

Port Management: PoE

You can decide the following:

-

VLANs address security and scalability issues. Traffic from a VLAN stays within

To create a range of VLANs, select the **Range**

VLAN Management

Frames that are VLAN-tagged can pass through other network devices that are VLAN-aware or VLAN-unaware. If a destination end node is VLAN-unaware, but is to receive traffic from a VLAN, then the last VLAN-aware device (if there is one), must send frames of the destination VLAN to the end node untagged.

Configuring Port to VLAN

Use the Port to VLAN page

VLAN Management

Defining VLAN Membership

The device supports a single voice VLAN. By default, the voice VLAN is VLAN 1.

VLAN Management

- The Voice VLAN cannot be Smartport enabled.
- The Voice VLAN QoS decision has priority over any other QoS decision,

NOTE

- **Switch MAC Address**

13

- **BPDU Guard**—Enables or disables the Bridge Protocol Data Unit (BPDU) Guard feature on the port.

  The BPDU Guard enables you to enforce the STP domain borders and keep

Configuring Static MAC Addresses

15

- **IP Group Address**—Based on the destination IP address of the IP packet

Multicast

Multicast

- **Last Member Query Counter**

Multicast

IGMP or MLD messages are not forwarded to ports defined as Forward All.

NOTE The configuration affects only the ports that are members of the selected VLAN.

To define Forward All Multicast:

STEP 1 Click **Multicast** > **Forward All**.

STEP 2 Define the following:

- **VLAN ID equals to**—The VLAN ID the ports/LAGs are to be displayed.
- **Interface Type equals to**—Define whether to display ports or LAGs.

STEP 3 Click **Go**. The status of all ports/LAGs are displayed.

STEP 4 Select the port/LAG that is to be defined as Forward All by using the following methods:

- **Static**—The port receives all Multicast streams.
- **Forbidden**

Multicast

16

IP Configuration

IP interface addresses can be configured manually by the user, or automatically

IPv6 Global Configuration

To define IPv6 global parameters and DHCPv6 client settings:

IP Configuration

IP Configuration

IP Configuration

To define prefixes to be advertised on the interfaces of the device:

STEP 5

IPv6 Default Router List

IP Configuration

IP Configuration

Domain Name

- **Source**—Source of the server's IP address (static or DHCPv4 or DHCPv6)
- **Interface**—Interface of the server's IP address.

STEP 4 Up to eight DNS servers can be defined. To add a DNS server, click **Add.**

Enter the parameters.

-

17

Security

- **Authentication Port**—Enter the UDP port number of the RADIUS server port for authentication requests.
- **Retries**—Enter the number of requests that are sent to the RADIUS server before a failure is considered to have occurred. If

Security

A caution message displays if you selected any other access profile, warning you that, depending on the selected access profile, you might be disconnected from the web-based configuration utility.

STEP 3 Click **OK** to select the active access profile or click **Cancel** to discontinue the

- **IP Version**—Select the supported IP version of the source address: IPv6 or IPv4.
- **IP Address**—Enter the source IP address.
- **Mask**—Select the format for the subnet mask for the source IP address, and enter a value in one of the field:

Security

Configuring 802.1X

Defining Host and Session Authentication

The Host and Session Authentication page enables defining the mode in which 802.1X operates on the port and the action to perform if a violation has been detected.

The 802.1X modes are:

- **Single**—Only a single authorized host can access the port. (Port Security

Security

18

Security: SSH Client

This section describes the device when it functions as an SSH client.

Ba Ba[(a)Ba[(p)Ba[(p)Tj 8(i)CP) and Tw[(v)Tw[(e)H8.8(t)]TJ/TT4 - scn1.5082 -2.09246.6(A

STEP 1 Click **Security** > **SSH Client** >

SSD grants read permission to sensitive data only to authenticated and authorized users, and according to SSD rules. A device authenticate

- (Higher) **Plaintext Only**—Users are permitted to access sensitive data in

Security: Secure Sensitive Data Management

Security: Secure Sensitive Data Management

SSD Properties

Security: Secure Sensitive Data Management

Security: Secure Sensitive Data Management

If the device creating the configuration file is in Unrestricted passphrase control mode, the device includes the passphrase in the file. As a result, the user can auto configure the target devices, including devices that are out-of-the-box or in factory

STEP 3 Select a trust mode (CoS/802.1p or DSCP) and click **Apply**.

STEP 4

STEP 3 Click **Apply**. The queues are configured, and the Running Configuration file is updated.

DSCP

- **Drop Precedence**—Lowest drop precedence has the lowest probability of being dropped.
-

21

SNMPv1 and v2

SNMP

SNMP

SNMP Engine ID

Each subtree is either included or excluded in the view being defined.

The Views page enables creating and editing SNMP views. The default views (Default, DefaultSuper) cannot be changed.

- **Notification Filter**—Select to enable filtering the type of SNMP notifications sent to the management station. The fi