Allied Telesis™

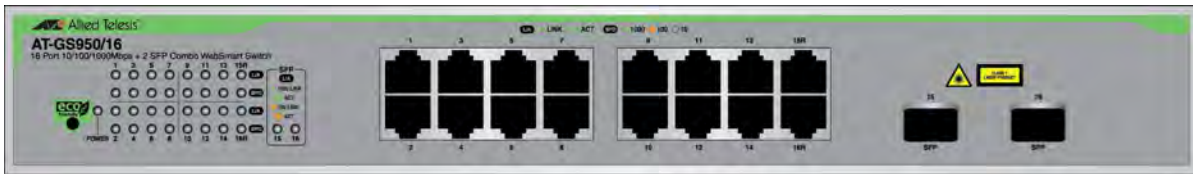# AT-GS950/16

Gigabit Ethernet Switch

3111

AT-GS950/16 Web Interface User Guide
AT-S114 Version 1.1.0 *[1.00.021]*

Allied Telesis™   the solution : the network

Contents

Contents

List of Figures

Figures

List of Tables

List of Tables

Preface

This guide contains instructions on how to use the AT-S114 Management Software to manage and monitor the AT-GS950/16 Gigabit Ethernet Switch.

The AT-S114 Management software has a web browser interface that you can access from any management workstation on your network that has a web browser application.

This preface contains the following sections:

❐ "Document Conventions" on page 18
❐ "Allied Telesis Contact Information" on page 19

Document Conventions

This document uses the following conventions:

Note

Notes provide additional information.

Caution

Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Warning

Warnings inform you that performing or omitting a specific action may result in bodily injury.

Allied Telesis Contact Information

If you need assistance with this product, you may contact Allied Telesis technical support by going to the Support & Services section of the Allied Telesis web site at **www.alliedtelesis.com/support**. You can find links for the following services on this page:

- 24/7 Online Support - Enter our interactive support center to search for answers to your questions in our knowledge database, check support tickets, learn about RMAs, and contact Allied Telesis technical experts.

- USA and EMEA phone support - Select the phone number that best fits your location and customer type.

- Hardware warranty information - Learn about Allied Telesis warranties and register your product online.

- Replacement Services - Submit a Return Merchandise Authorization (RMA) request via our interactive support center.

- Documentation - View the most recent installation guides, user guides, software release notes, white papers and data sheets for your product.

- Software Updates - Download the latest software releases for your product.

For sales or corporate contact information, go to **www.alliedtelesis.com/purchase** and select your region.

Section I
Getting Started

This section contains the following chapters:

Chapter 1
Starting a Web Browser Session

This chapter contains the procedures for starting, using, and quitting a web browser management session on the AT-GS950/16 switch. This chapter includes the following sections:

❒ "Establishing a Remote Connection to the Web Browser Interface" on page 24
❒ "Web Browser Tools" on page 27
❒ "Quitting a Web Browser Management Session" on page 28

Establishing a Remote Connection to the Web Browser Interface

The AT-GS950/16 switch is shipped with a pre-assigned IP address of 192.168.1.1. After your initial login, Allied Telesis suggests that you assign a new IP address to your switch. To manually assign an IP address to the switch, refer to "Configuration of IPv4 Address, Subnet Mask and Gateway Address" on page 32. To configure the switch to obtain its IP configuration from a DHCP server, refer to "DHCP Client Configuration" on page 53.

Whether you use the pre-assigned IP address or assign a new one, you must set your local PC to the same subnet as the switch.

To start a web browser management session, perform the following procedure:

1. Start your web browser.

2. In the URL field of the browser, enter 192.168.1.1.

   This is the default IP address of the switch. See Figure 1.

Switch's IP Address

Figure 1. Entering a Switch's IP Address in the URL Field

The AT-S114 Management Software displays the login dialog box. See Figure 2.

Figure 2. Management Login Dialog Box

3. Enter the AT-S114 management login user name and password.

The default user name is "manager" and the default password is "friend." The login name and password are case-sensitive.
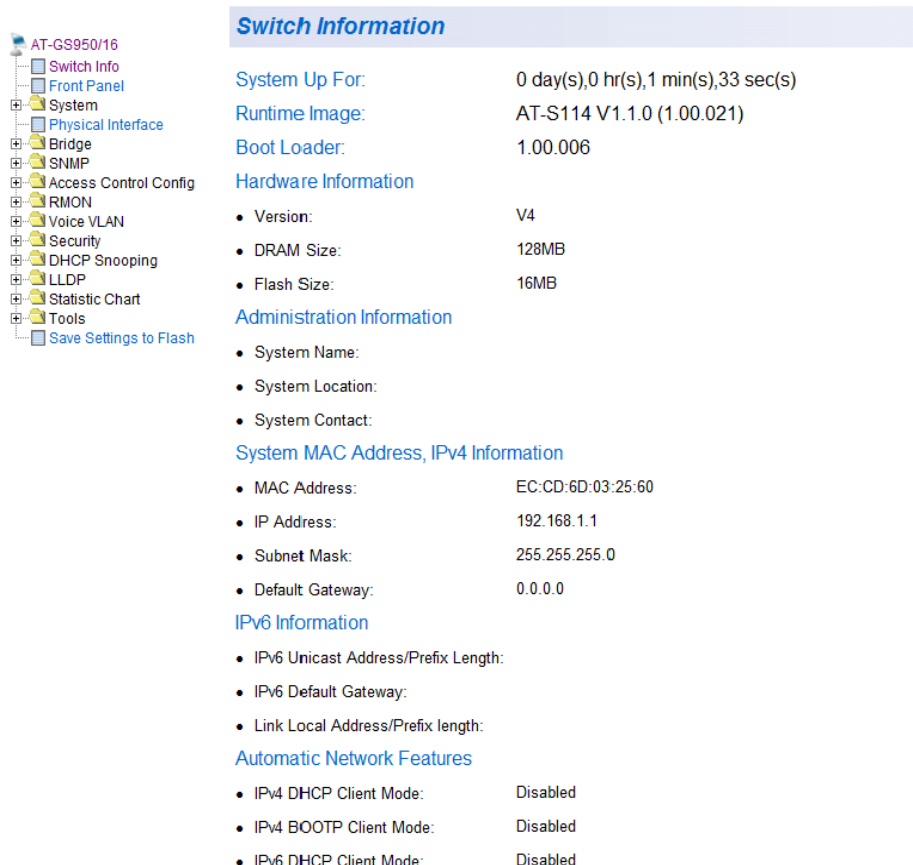
4. Press **OK**.

The AT-GS950/16 Switch Information page is displayed. See Figure 3.

Note

To change the user name and password, refer to "User Name and Password Configuration" on page 42.

Figure 3. AT-GS950/16 Switch Information Page

The main menu appears on the left side and is common for all of the management pages discussed in this guide. It consists of the following folders and web pages:

- Switch Info
- Front Panel

■ System

■ Physical Interface

■ Bridge

■ SNMP

■ Access Control

■ RMON

■ Voice VLAN

■ Security

■ DHCP Snooping

■ LLDP

■ Statistics Chart

■ Tools

■ Save Settings to Flash

5. To see the front panel of the switch, select **Front Panel** from the main menu on the left side of the page.

   The AT-S114 Management software displays the front of the switch. Ports are green that have a link to an end node. Ports without a link are grey. To view the status of the ports for an MSTP instance, select the instance from the MST Instance ID drop-down menu. The AT-GS950/16 switch front panel page is shown in Figure 4.
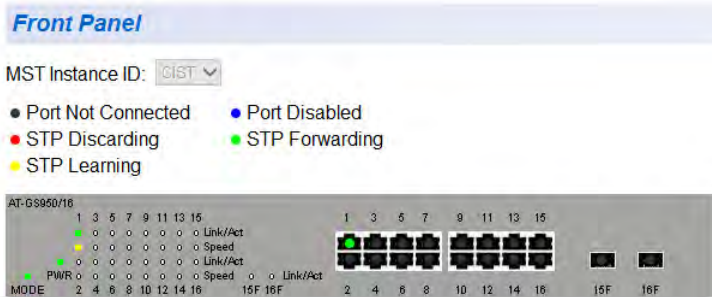
Figure 4. Front Panel Page

A web browser management session remains active even if you link to other sites. You can return to the management web pages anytime as long as you do not quit your browser session or the management session does not time out. The default time-out is 10 minutes.

Web Browser Tools

You can use the web browser tools to move around the management pages. Selecting **Back** on your browser's toolbar returns you to the previous display. You can also use the browser's **Bookmark** feature to save the link to the switch.

Quitting a Web Browser Management Session

To exit a web browser management session, close the web browser.

Chapter 2
System Configuration

This chapter provides procedures to configure basic system parameters for the AT-GS950/16 switch and contains information for the following sections:

Note

To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

System Management Information

This section explains how to assign a name, location, and contact information for the AT-GS950/16 switch. This information helps in identifying each specific AT-GS950/16 switch among other switches in the same local area network. Entering this information is optional.

> **Note**
> Allied Telesis recommends that you assign a name to the switch. Naming each switch can help you identify the specific switch you want to manage among others. It can also help to avoid performing a configuration procedure on the wrong switch.

To set a switch's administration information, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
   The **System** folder expands.

2. From the **System** folder, select **Management**.
   The Management Page is displayed. See Figure 5 for the AT-GS950/16 Management Page.

Figure 5. AT-GS950/16 Management Page

3. Configure the following parameters as necessary:

   System Description - Indicates the Allied Telesis switch model. You cannot change this parameter.

   System Object ID - Indicates the unique SNMP MIB object identifier that identifies the switch model. You cannot change this parameter.

System Name - Specifies a name for the switch, for example, Sales. The name is optional and may contain up to 15 characters.

System Location - Specifies the location of the switch. The location is optional and may contain up to 30 characters.

System Contact - Specifies the name of the network administrator responsible for managing the switch. This contact name is optional and may contain up to 30 characters.

4. Click **Apply**.

5. From the main menu on the left side of the page, click on **Switch Info**. The Switch Information page is displayed. See "AT-GS950/16 Switch Information Page" on page 25 for more information.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Configuration of IPv4 Address, Subnet Mask and Gateway Address

This procedure explains how to change the IP address, subnet mask, and gateway address of the switch. Before performing the procedure, note the following:

- A gateway address is only required if you want to remotely manage the device from a management station that is separated from the switch by a router.

- To configure the switch to automatically obtain its IP configuration from a DHCP server on your network, go to "DHCP Client Configuration" on page 53.

To change the switch's IPv4 configuration, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
   The **System** folder expands.

2. From the **System** folder, select **IPv4 Setup**.
   The IPv4 Setup Page is displayed. See Figure 6.

IPv4 Setup

System MAC Address:	EC:CD:6D:25:10:80
System IP Address:	192 . 168 . 1 . 1
System Subnet Mask:	255 . 255 . 255 . 0
System Default Gateway:	0 . 0 . 0 . 0
System IP Mode:	Static ∨
	Apply

Figure 6. IPv4 Setup Page

3. Change the IPv4 configuration parameters by observing or entering new information in the following fields:

   System MAC Address - This parameter displays the MAC address of the switch. You cannot change this parameter.

   System IP Address - Displays the current IP address of the switch. To change the IP address, enter a new IP address. When DHCP is enabled, you cannot change this parameter.

System Subnet Mask - Displays the current subnet mask of the switch. To change the subnet mask, enter a new subnet mask. When DHCP is enabled, you cannot change this parameter.

System Default Gateway - Displays the default gateway of the switch. To change the default gateway, enter a new gateway. When DHCP is enabled, you cannot change this parameter.

System IP Mode - Displays the current mode of the switch. To change the mode, select **Static**, **DHCP**, or **BootP**. If the **DHCP** or **BootP** mode is selected, you cannot change the **System IP Address**, **System Subnet Mask**, and **System Default Gateway** parameters because these parameters are automatically retrieved by the DHCP or BootP server. For information about setting the DHCP mode, refer to "DHCP Client Configuration" on page 53.

4. Click **Apply**.

Note

Changing the IP address ends your management session. To resume managing the device, enter the new IP address of the switch in the web browser's URL field, as shown in Figure 1 on page 24.

---

5. After you log on to the switch with the new IP address, select **Save Settings to Flash** from the main menu on the left side of the page to save the new IP address to memory.

⚠️ **Caution**

If you do not select **Save Settings to Flash**, the IP address will revert to its original setting when you power cycle or reboot the switch.

IPv6 System Configuration

This procedure explains how to enable IPv6 and configure IPv6 system settings.

To enable IPv6 and configure the switch's IPv6 settings, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
    The **System** folder expands.

2. From the **System** folder, select **IPv6 System Settings**.
    The IPv6 System Settings Page is displayed. See Figure 7.

Figure 7. IPv6 System Settings Page

3. To enable or disable IPv6 on the switch, select **Enabled** or **Disabled** from the **IPv6 State** pull-down menu.

4. To enable or disable the DHCPv6 Client on the switch, select **Enabled** or **Disabled** from the **DHCPv6** pull-down menu.

5. Change the IPv6 system settings by observing or entering new information in the following fields:

    IPv6 Unicast Address/Prefix Length - Displays the current IPv6 unicast address and prefix length of the switch. To change the address and prefix length, enter a new IPv6 unicast address and prefix length. When DHCP is enabled, you cannot change this parameter.

    IPv6 Static Gateway - Displays the current IPv6 static gateway of the switch. To change the gateway, enter a new IPv6 static gateway. When DHCP is enabled, you cannot change this parameter.

    IPv6 Dynamic Gateway - This parameter displays the IPv6 Dynamic Gateway of the switch. You cannot change this parameter.

6. Click **Apply**.

7. To change the Neighbor Solicitation (NS) retransmit time, enter the new time in the field next to **NS Retransmit Time**. The range is from 1 to 3600 seconds.

8. Change the link local address settings as follows:

    Automatic Link Local Address - Select **Enabled** to automatically assign a link local address. Select **Disabled** to manually assign the link local address.

    Link Local Address/Prefix length - To change the link local address and prefix length, enter a new address and prefix length. When Automatic Link Local Address is enabled, you cannot change this parameter.

9. Click **Apply**.

10. Select **Save Settings to Flash** from the main menu on the left side of the page to save the new IPv6 configuration to memory.

> ⚠️ **Caution**
>
> If you do not select **Save Settings to Flash**, the IPv6 setting will revert to its original setting when you power cycle or reboot the switch.

IPv6 Neighbor Configuration

You can configure the switch's IPv6 neighbors manually if a router is unavailable.

The procedures in this section describe how to add IPv6 neighbors or remove them from the list and how to find IPv6 neighbors in the list.

See the following sections:

❐ "Create an IPv6 Neighbor List"

❐ "Delete an IPv6 Neighbor Entry" on page 37

❐ "Find an IPv6 Neighbor" on page 37

Create an IPv6 Neighbor List

To create a list of IPv6 neighbors, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
   The **System** folder expands.

2. From the **System** folder, select **IPv6 Neighbor Settings**.
   The IPv6 Neighbor Settings Page is displayed. See Figure 8.
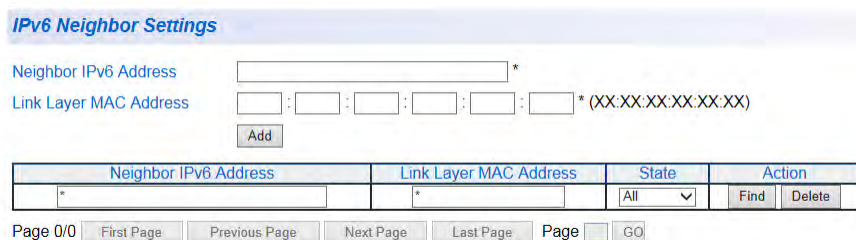
Figure 8. IPv6 Neighbor Settings Page

3. Enter an IPv6 address in the **Neighbor IPv6 Address** field using xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx format, where each x is a hexadecimal digit representing 4 bits.

4. Enter a link layer MAC address in the **Link Layer MAC Address** field.

5. Click **Add**.
   The IPv6 address and link layer MAC address are added to the list. See Figure 9 on page 37.

Figure 9. IPv6 Neighbor Settings Page with Addresses

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Delete an IPv6 Neighbor Entry

To delete an IPv6 neighbor entry or multiple entries, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.

2. From the **System** folder, select **IPv6 Neighbor Settings**.
The IPv6 System Settings Page is displayed. See Figure 9 on page 37.

3. Select **Delete** next to the IPv6 neighbor entry that you want to remove.
The IP address is removed from the list.

You can also delete multiple entries by using the top row of the table:

To delete all entries, select **All** from the drop-down menu under **State**, then click the **Delete** button under **Action**.

To delete all static entries, select **Static** from the drop-down menu under **State**, then click the **Delete** button under **Action**.

To delete all dynamic entries, select **Dynamic** from the drop-down menu under **State**, then click the **Delete** button under **Action**.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Find an IPv6 Neighbor

To find an IPv6 neighbor or multiple neighbors, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.

2. From the **System** folder, select **IPv6 Neighbor Settings**.
    The IPv6 System Settings Page is displayed. See Figure 9 on page 37.

3. Enter the search criteria using the top row of the table:

    ◼ To find a specific IPv6 neighbor, do one of the following:

    Type the IPv6 neighbor address in the **Neighbor IPv6 Address** field and type an asterisk in the **Link Layer MAC Address** field. The asterisk serves as a wildcard character. See Figure 10 for an example.

Figure 10. Example Search with Neighbor IPv6 Address

    Or

    Type an asterisk in the **Neighbor IPv6 Address** field and type the link layer MAC address in the **Link Layer MAC Address** field. See Figure 11 for an example.

Figure 11. Example Search with Link Layer MAC Address

    Or

    Type the IPv6 neighbor address in the **Neighbor IPv6 Address** field and type the link layer MAC address in the **Link Layer MAC Address** field. See Figure 12 on page 39 for an example.

Figure 12. Example Search with Both Addresses

- To find all static IPv6 neighbors, type asterisks in the **Neighbor IPv6 Address** and **Link Layer MAC Address** fields, then select **Static** from the drop-down menu under **State**.

- To find all dynamic IPv6 neighbors, type asterisks in the **Neighbor IPv6 Address** and **Link Layer MAC Address** fields, then select **Dynamic** from the drop-down menu under **State**.

4. Click the **Find** button under **Action**. The entry or entries are displayed in the table.

5. To view all of the IPv6 entries created in the list, refresh the page by selecting **IPv6 Neighbor Settings** from the **System** folder.

IP Access List Configuration

When the IP Access List feature is enabled, remote access to the AT-S114 management software is restricted to the IP addresses entered into the IP Access List.

The procedures in this section describe how to enable or disable the IP Access List feature and how to add or remove IP addresses from the list. See the following sections:

❒ "Create an IP Access List"
❒ "Delete an IP Address List Entry" on page 41

> **Note**
>
> To modify an IP address that has already been created, it must first be deleted and then re-created using the following procedures.

Create an IP Access List

To create a list of accessible IP addresses, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
   The **System** folder expands.

2. From the **System** folder, select **IP Access List**. The IP Access List Page is displayed. See Figure 13.

Figure 13. IP Access List Page

3. Enter an IP address one of the **IP Address** fields:

    For an IPv4 address, click **IPv4**, then enter the address using xxx.xxx.xxx.xxx format.

    For an IPv6 address, click **IPv6**, then enter the address using xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx format, where each x is a hexadecimal digit representing 4 bits.

4. Click **Add**.
    The IP address is added to the IP Access List table in the **Accessible IP** column.

    Note

    You can add up to 10 IP addresses to the IP Access List table.

    ---

5. From the **IP Restriction Status** field, select one of the following choices from the pull-down menu:

    Enabled - This selection restricts the access to the AT-S114 management software to the IP addresses in the table listed under **Accessible IP**.

    Disabled - This selection allows unrestricted access to the AT-S114 management software.

6. Click **Apply**.
    Access to the management software is now restricted to those IP addresses listed in the IP Access List table.

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Delete an IP Address List Entry

To delete an IP address from the IP Access List, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
    The **System** folder expands.

2. From the **System** folder, select **IP Access List**.
    The IP Access List Page is displayed. See Figure 13 on page 40.

3. Select **Delete** next to the IP address that you want to remove.
    The IP address is removed from the IP Access List table. If you remove the last IP address from the table, the **IP Restriction Status** field is set to Disabled.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

User Name and Password Configuration

Password protection is always enabled for access to the AT-S114 Management software. This section explains how to create new user names and passwords and how to modify or delete existing users for the web interface. See the following sections:

❏ "Add New User Name and Password"

❏ "Modify User Name and Password" on page 43

❏ "Delete User Name and Password" on page 44

Add New User Name and Password

The default User Name and Password is "manager" and "friend" - both without the quotes. To configure new User Name and Password information, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
   The **System** folder expands.

2. From the **System** folder, select **Administration**.
   The Administration Page is displayed. See Figure 14.

Figure 14. Administration Page

3. Select an authentication method from the **User Authentication Method** menu: **Local**, **Local & RADIUS**, or **Local & TACACS+**.

4. Click **Apply**.

5. To create a user name, enter a user name in the box next to the **User Name** field.

   You can enter a value of up to 12 alphanumeric characters. The **User Name** field is case sensitive.

6. To add a password that corresponds to the user name entered in Step 5, enter a password of up to 12 alphanumeric characters in the box next to the **Password** field. The **Password** field is case sensitive.

7. To confirm the password entry, retype the password in the box next to the **Confirm Password** field.

8. Click **Add** to activate your changes on the switch.
   An example of the Administration Page is shown in Figure 15.

Figure 15. Administration Page Example

9. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Modify User Name and Password

To modify a user name password, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
   The **System** folder expands.

2. From the **System** folder, select **Administration**.
   The Administration Page is shown in Figure 15 on page 43.

3. Identify the user name that you want to change and click **Modify** in the **Action** column.
   The Modify Administration Page is displayed. See Figure 16 on page 44.

Note

The entry number and default user name cannot be modified or deleted in the Modify Administration page. The entry number is automatically assigned as an index number in the Administration page when the entry is originally created. The default password can be modified.

Figure 16. Modify Administration Page

4. To change a password, enter a password of up to 12 alphanumeric characters in the box next to the **Password** field.

5. To confirm the above password, retype the password in the box next to the **Confirm Password** field.

6. Click **Apply** to activate your changes on the switch.

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Delete User Name and Password

To delete a user name that you have previously added, perform the following procedure.

1. From the main menu on the left side of the page, click the **System** folder.
   The **System** folder expands.

2. From the **System** folder, select **Administration**.
   The Administration Page is shown in Figure 15 on page 43.

3. Identify the user name that you want to delete and click **Delete**.
   The user name is removed from the Administration table.

   Note
   The default user name cannot be modified or deleted. The default password can be modified.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

User Interface Configuration

This procedure explains how to enable and disable the user interfaces on the switch. With this procedure, you can enable or disable the AT-GS950/16 SNMP Agent. For more information about SNMP, go to Chapter 16, "SNMPv1 and v2c" on page 209 and Chapter 17, "SNMPv3" on page 223.

> **Note**
> The **Web Server Status** is displayed as **Enabled** for your information only. The Web Server cannot be disabled.

SNMP Interface
To enable or disable the AT-GS950/16 SNMP interface, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
   The **System** folder expands.

2. From the **System** folder, select **User Interface**.
   The User Interface Page is displayed. See Figure 17.

Figure 17. User Interface Page

3. Choose **Enabled** or **Disabled** from the pull-down list for the **SNMP Agent** parameter.

   Enabled - When you enable this parameter, the SNMP agent is active. You can manage the AT-GS950/16 switch with Network Management Software and the switch's private MIB.

   Disabled - When you enable this parameter, the SNMP agent is inactive.

> **Note**
>
> See Chapter 16, "SNMPv1 and v2c" on page 209 and Chapter 17, "SNMPv3" on page 223 to configure the remaining SNMP parameters.

4. Click **Apply** under the **Web Server Status** field.

5. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

User Interface Timeout

To set the Web Idle Timeout, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
   The **System** folder expands.

2. From the **System** folder, select **User Interface**.
   The User Interface Page is displayed. See Figure 17 on page 45.

3. Refer to the bottom portion of the web page. Enter the **Web Idle Timeout** parameter. The range is from 3 to 60 minutes.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Group Interval

To set the SNMP Group Interval Timeout, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
   The **System** folder expands.

2. From the **System** folder, select **User Interface**.
   The User Interface Page is displayed. See Figure 17 on page 45.

3. Refer to the bottom portion of the web page. Enter the **Group Interval** parameter. The range is from 0 or 120 to 1225 seconds. 0 disables the interval.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

System Time

The procedures in this section describe how to configure the system time by manually entering the time or through SNTP and how to configure the daylight savings time feature. See the following sections:

❏ "Manually Setting System Time"

❏ "Setting SNTP" on page 48

❏ "Setting Daylight Savings Parameters" on page 49

Manually Setting System Time

To set the system time manually, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
   The **System** folder expands.

2. From the **System** folder, select **System Time**.
   The System Time Page is displayed. See Figure 18.

Figure 18. System Time Page

3. Use the pull-down menu to set the **Clock Mode** parameter to **Local** time.

4. In the Local Time Settings section, set the **Date Setting (YYYY:MM:DD)** to the current date in the YYYY:MM:DD format.

5. In the Local Time Settings section, set the **Time Settings (HH:MM:SS)** to the current time in the HH:MM:SS format.

6. Click the **Apply** button at the bottom of the page.
   The time will take effect immediately.

7. Save your new settings or any changes to the configuration file by selecting **Save Settings to Flash** from the main menu on the left side of the page.

Setting SNTP   To configure SNTP, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
   The **System** folder expands.

2. From the **System** folder, select **System Time**.
   The System Time Page is displayed. See Figure 18 on page 47.

3. Use the pull-down menu to set the **Clock Mode** parameter to **SNTP**.

4. Enter the IPv4 or IPv6 address of the **SNTP Primary Server**: The format is xxx.xxx.xxx.xxx for IPv4 and xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxx in hexadecimal digits for IPv6.

5. Click **IPv4** or **IPv6**.

6. Enter the IP address of the **SNTP Secondary Server**. The format is xxx.xxx.xxx.xxx for IPv4 and xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxx in hexadecimal for IPv6.

7. Click **IPv4** or **IPv6**.

8. Enter the **SNTP Poll Interval**. The range is 1 - 60 minutes.

9. Select the local **Time Zone** from the pull-down menu.

10. Click the **Apply** button at the bottom of the page.
    The switch will immediately start polling the SNTP primary server for time information.

11. Save your new settings or any changes to the configuration file by selecting **Save Settings to Flash** from the main menu on the left side of the page.

Setting Daylight Savings Parameters

If you want to configure the switch for daylight savings time, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
   The **System** folder expands.

2. From the **System** folder, select System Time.
   The System Time Page is displayed. See Figure 18 on page 47.

3. In the **Daylight Savings Time Status** field, select **Enabled**.

4. Specify the Month, Day, Hour and Minute when Daylight Savings will take effect in the **From** time fields.

5. Specify the Month, Day, Hour and Minute when Daylight Savings will end in the **To** time fields.

6. Using the pull-down menu, specify the Daylight Savings offset in the **DST Offset** field. You can select either 1 hr or 1/2 hr.

7. Save your new settings or any changes to the configuration file by selecting **Save Settings to Flash** from the main menu on the left side of the page.

SSL Settings

The AT-GS950/16 switch has a web browser server for remote management of the unit with a web browser application from management workstations on your network. By default, the server operates in a non-secure HTTP mode and can be configured to communicate in a secure HTTPS mode with the SSL protocol.

In many situations, the communication with the switch will be in a controlled environment, and it is acceptable to communicate with the management software in the HTTP mode.

However, you may find that your management communications are subject to outside security risks and web sessions conducted in the non-secure HTTP mode are vulnerable to security issues because the packets are sent in clear text. Web browser management sessions that use the secure HTTPS mode with SSL are protected against snooping because the packets exchanged between the switch and your management workstations are encrypted. When operating in this mode, only the AT-GS950/16 switch and the web browser are able to decipher the packets sent and received between them.

Configuring SSL   To enable or disable the SSL protocol feature, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
   The **System** folder expands.

2. From the **System** folder, select **SSL Settings**.
   The SSL Settings Page is displayed. See Figure 19.

Figure 19. SSL Settings Page

3. From the **SSL Settings** field, select one of the following choices from the pull-down menu:

    Enabled - The secure SSL mode is active. You must log into the switch's management using the HTTPS mode on your browser.

    Disabled - The secure SSL mode is inactive. You must log into the switch's management using the HTTP mode on your browser.

4. Click **Apply**.
    The SSL setting that you have selected is now active.

5. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

DHCP and ATI Web Discovery Tool

The AT-GS950/16 Gigabit Ethernet Smart switch is managed through a web browser interface only. The factory default IP address is 192.168.1.1.

The switch does not have a local console connector, which means that you cannot learn what the switch's management IP address is on a web browser without first knowing what the address is. Once the IP address is known, you can enter it in the browser.

When the DHCP feature is enabled, a DHCP server automatically assigns an IP address which is not advertised over the network. As a consequence, you do not know the IP address that has been assigned to the switch.

Note

The new IP address assignment from the DHCP server may take 1 to 2 minutes before the process is completed.

Fortunately, there is an ATI Web Discovery Tool available that resolves this issue. It detects the MAC address, IP address and other information of the AT-GS950 series switches that are present on your local area network.

Note

The ATI Web Discovery Tool is available for download on the AT-GS950/16 product page at alliedtelesis.com.

DHCP Client Configuration

This procedures in this section explain how to activate and deactivate the DHCP client on the AT-GS950/16 switch. See the following sections:

❏ "Activate or Deactivate DCHP for IPv4"

❏ "Activate or Deactivate DCHP for IPv6" on page 54

Activate or Deactivate DCHP for IPv4

When the client is activated, the switch obtains its IP configuration including an IP address and subnet mask from a DHCP server on your network. Before performing the procedure, note the following:

■ By default, the DHCP client is disabled on the switch.

■ The DHCP client supports DHCP Auto Configuration Settings or BOOTP. See "DHCP Auto Configuration" on page 56 for more information.

■ After you enable DHCP, your current management session ends because a different IP address is assigned to the switch by the DHCP server. The new IP address can be discovered using the ATI Discovery Tool. See "DHCP and ATI Web Discovery Tool" on page 52 for more information.

To activate or deactivate the DHCP client on the switch for IPv4, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
   The **System** folder expands.

2. From the **System** folder, select **IPv4 Setup**.
   The IPv4 Setup Page is shown in Figure 6 on page 32.

3. From the pull-down menu next to the **System IP Mode** field, select **DHCP**.

4. Click **Apply**.
   When the DHCP client is selected, the web server connection to the switch is lost because a different IP address is assigned to the switch by the DHCP server.

⚠ **Caution**

Selecting DHCP may end your current management session.

5. Use the ATI Web Discovery Tool to find the new IP address assigned to the switch by the DHCP server. See "DHCP and ATI Web Discovery Tool" on page 52 for more information.

> **Note**
> The ATI Web Discovery Tool is available for download on the AT-GS950/16 product page at **alliedtelesis.com**.

6. Follow the procedure to log on with the new IP address provided by the DHCP Server as described in "Establishing a Remote Connection to the Web Browser Interface" on page 24.

7. Save your new settings or any changes to the configuration file by selecting **Save Settings to Flash** from the main menu on the left side of the page.

   If you do not save the new configuration when DHCP is enabled, the software reverts to the previously saved IP address value when the switch is power cycled or rebooted. If no IP address has been previously saved, the IP address value reverts to 192.168.1.1.

   If you enable DHCP and then save your configuration, you are saving the DHCP setting. The next time the switch boots up, it will use the DHCP process to establish the IP address used to manage the AT-GS950/16 switch.

   If you enter a new IP address after disabling DHCP and save your configuration, the disabled DHCP setting and the new IP address on the switch is saved. The next time the switch boots up, it will respond to the IP address that you entered when you re-establish contact with the AT-S114 Management software.

Activate or Deactivate DCHP for IPv6

When the client is activated, the switch obtains its IPv6 configuration including an IPv6 address and prefix length from a DHCPv6 server on your network. Before performing the procedure, note the following:

- By default, the DHCP client is disabled on the switch.

- The DHCP client supports DHCP Auto Configuration Settings. See "DHCP Auto Configuration" on page 56 for more information.

- After you enable DHCP, a different IP address is assigned to the switch by the DHCP server.

> **Note**
> The ATI Web Discovery Tool does not discover IPv6 addresses. If use of this tool is required, use only IPv4 addresses.

To activate or deactivate the DHCP client on the switch for IPv6, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
   The **System** folder expands.

2. From the **System** folder, select **IPv6 System Settings**.
   The IPv6 System Settings Page is shown in Figure 7.

3. From the pull-down menu next to the **DHCPv6 Client** field, select **Enabled**.

4. Click **Apply**.

5. Follow the procedure to log on with the new IPv6 address provided by the DHCPv6 Server as described in "Establishing a Remote Connection to the Web Browser Interface" on page 24.

6. Save your new settings or any changes to the configuration file by selecting **Save Settings to Flash** from the main menu on the left side of the page to permanently save your changes.

   If you enable DHCPv6 and then save your configuration, you are saving the DHCPv6 setting. The next time the switch boots up, it will use the DHCPv6 process to establish the IPv6 address used to manage the AT-GS950/16 switch.

   If you enter a new IP address after disabling DHCPv6 and save your configuration, the disabled DHCPv6 setting and the new IPv6 address on the switch is saved. The next time the switch boots up, it will respond to the IPv6 address that you entered when you re-establish contact with the AT-S114 Management software.

DHCP Auto Configuration

If you need to automatically update the switch's configuration files via a remote server, the DHCP Auto Configuration feature is available for this purpose via the DHCP server.

To configure this feature on the switch, perform the following procedure:

Note

You must configure your DHCP server to include the configuration file name (option 67) and the server address (option 54). Please note that switch is expecting the TFTP server to reside on the same IP address of the DHCP server.

1. From the main menu on the left side of the page, click the **System** folder.
   The **System** folder expands.

2. From the **System** folder, select **System**.
   The DHCP Auto Configuration Settings Page is shown in Figure 20.

Figure 20. DHCP Auto Configuration Settings Page

3. From the **Auto Configuration State** field, select one of the following choices from the pull-down menu:

   Enabled - The DHCP Auto Configuration feature is active.

   Note

   You must enable the DHCP client so that this feature can operate with the DHCP server. See "DHCP Client Configuration" on page 53 for more information.

   Disabled - The DHCP Auto Configuration feature is inactive.

4. Click **Apply**.
   The DHCP Auto Configuration setting that you have selected is now active.

5. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

System Information Display

The Switch Information page is initially displayed when you first log into the AT-GS950/16 switch. It provides general information about the switch. To view this information, perform the following procedure:

1. From the main menu on the left side of the page, select **Switch Info**. The Switch Information Page is displayed. See Figure 21.

Figure 21. AT-GS950/16 Switch Information Page

The Switch Information Page displays the following information:

System Up For - The number of days, hours, and minutes that the switch has been running since it was last rebooted.

Runtime Image - The version number of the runtime firmware.

Boot Loader - The version number of the bootloader firmware.

Hardware Information Section:

Version - The hardware version number.

DRAM Size - The size of the DRAM, in megabytes.

Flash Size - The size of the flash memory, in megabytes.

Administration Information Section:

Switch Name - This parameter displays the name assigned to the switch. To assign the switch a name, refer to "System Management Information" on page 30.

Switch Location - This parameter displays the location of the switch. To assign the location, refer to "System Management Information" on page 30.

Switch Contact - This parameter displays the contact person responsible for managing the switch. To assign the name of a contact, refer to "System Management Information" on page 30.

System MAC Address, IPv4 Information Section:

MAC Address - This parameter displays the MAC address of the switch.

IP Address - This parameter displays the system IP address. Refer to "Configuration of IPv4 Address, Subnet Mask and Gateway Address" on page 32 to manually assign an IP address or "DHCP Client Configuration" on page 53 to activate the DHCP client.

Subnet Mask - This parameter displays the subnet mask for the switch. Refer to "Configuration of IPv4 Address, Subnet Mask and Gateway Address" on page 32 to manually assign a subnet mask or "DHCP Client Configuration" on page 53 to activate the DHCP client.

Default Gateway - This parameter displays the default gateway IP address. Refer to "Configuration of IPv4 Address, Subnet Mask and Gateway Address" on page 32 to manually assign a gateway address or "DHCP Client Configuration" on page 53 to activate the DHCP client.

IPv6 Information Section:

IPv6 Unicast Address/Prefix Length - This parameter displays the system IPv6 address and prefix length. Refer to "IPv6 System Configuration" on page 34 to manually assign an IPv6 address or "DHCP Client Configuration" on page 53 to activate the DHCP client.

IPv6 Default Gateway - This parameter displays the default gateway IPv6 address. Refer to "IPv6 System Configuration" on page 34 to manually assign a gateway address or "DHCP Client Configuration" on page 53 to activate the DHCP client.

Link Local Address/Prefix Length - This parameter displays the link local address. Refer to "IPv6 System Configuration" on page 34 to manually or automatically assign a link local address.

Automatic Network Features Section:

IPv4 DHCP Client Mode - This parameter displays the status of the DHCP client on the switch. For information about setting this parameter, refer to "DHCP Client Configuration" on page 53.

IPv4 BOOTP Client Mode - This parameter displays the status of the BootP client on the switch. For information about setting this parameter, refer to "Configuration of IPv4 Address, Subnet Mask and Gateway Address" on page 32.

IPv6 DHCP Client Mode - This parameter displays the status of the DHCPv6 client on the switch. For information about setting this parameter, refer to "DHCP Client Configuration" on page 53.

System Log Configuration

The System log is designed to monitor the operation of the AT-GS950/16 switch by recording the event messages it generates during normal operation. These events may provide vital information about system activity that can help in the identification and solutions of system problems.

To configure the System log, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
    The **System** folder expands.

2. From the **System** folder, select **System Log Settings**.
    The System Log Configuration Page is displayed. See Figure 22.

Figure 22. System Log Configuration Page

3. From the **Syslog Status** field, select one of the following choices from the pull-down menu:

> **Enabled** - The System log is active.

> **Disabled** - The System log is inactive.

4. From the Time Stamp field, select one of the following choices from the pull-down menu:

> **Enabled** - Each event message recorded in the log will have a time stamp recorded with it.

> **Disabled** - No time stamp will be recorded with the event messages.

5. Enter the **Messages Buffer Size**.The range is between 1 and 200.

6. Enter the **Syslog Server IP Address**:

> IPv4 addresses: **Click IPv4**, then enter the address.The format is xxx.xxx.xxx.xxx. If the address is left at the default setting of 0.0.0.0, no server is specified.

> IPv6 addresses: **Click IPv6**, then enter the address.The format is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxx in hexadecimal digits.

7. In the **Facility** field, enter the Facility local from the pull-down menu. The choices range from **local0** through **local7**.

8. Select the **Logging Level**. This parameter specifies which level of event messages will be logged into the System log. Your choices are as follows:

> **Alert** - Action must be taken immediately.

> **Critical** - Critical conditions are displayed.

> **Warning** - Warning conditions are displayed.

> **Info** - Informational messages are displayed

9. Click **Apply**.
   The System log is now active.

10. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Section II
Bridge Configuration

This section contains the following chapters:

Chapter 3
Port Configuration

This chapter provides a description of the physical characteristics of the ports and a procedure that explains how to view and change the port settings. This chapter includes the following sections:

❒ "Overview" on page 66
❒ "Displaying and Configuring Ports" on page 67

> **Note**
> To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Overview

This chapter describes how to display and modify the physical characteristics of an AT-GS950/16 switch. You can display and modify the settings of all the ports on one web page. The port characteristics that are displayed are:

- Trunk Group Number
- Port type
- Link Status
- Admin Status
- Duplex Mode
- Jumbo frame
- Flow control
- EAP Pass
- BPDU frame

These characteristics are described in the next section.

Displaying and Configuring Ports

This procedure explains how to configure the ports on the AT-GS950/16 switch using the Port Configuration Page. This page allows you to view and configure the parameter settings of individual or all the switch ports at one time.

To configure the ports, perform the following procedure:

1. From the main menu on the left side of the page, select **Physical Interface**.
   A partial view of the AT-GS950/16 Physical Interface Page is displayed in Figure 23.

Physical Interface

Port	Trunk	Type	Link Status	Admin Status	Mode	Jumbo	Flow Ctrl	EAP	BPDU	Action
All	-	-	-	Ignore ∨	Ignore ∨	Ignore ∨	Ignore ∨	Ignore ∨	Ignore ∨	Apply
1	---	1000TX	Up	Enabled ∨	Auto (100F) ∨	Enabled ∨	Disabled ∨	Disabled ∨	Enabled ∨	Apply
2	---	1000TX	Down	Enabled ∨	Auto ∨	Enabled ∨	Disabled ∨	Disabled ∨	Enabled ∨	Apply
3	---	1000TX	Down	Enabled ∨	Auto ∨	Enabled ∨	Disabled ∨	Disabled ∨	Enabled ∨	Apply
4	---	1000TX	Down	Enabled ∨	Auto ∨	Enabled ∨	Disabled ∨	Disabled ∨	Enabled ∨	Apply
5	---	1000TX	Down	Enabled ∨	Auto ∨	Enabled ∨	Disabled ∨	Disabled ∨	Enabled ∨	Apply
6	---	1000TX	Down	Enabled ∨	Auto ∨	Enabled ∨	Disabled ∨	Disabled ∨	Enabled ∨	Apply
7	---	1000TX	Down	Enabled ∨	Auto ∨	Enabled ∨	Disabled ∨	Disabled ∨	Enabled ∨	Apply
8	---	1000TX	Down	Enabled ∨	Auto ∨	Enabled ∨	Disabled ∨	Disabled ∨	Enabled ∨	Apply

Figure 23. AT-GS950/16 Physical Interface Page

2. Adjust the port settings as needed. Not all parameters are adjustable. The parameters are defined as follows:

   Port - Specifies the port number. The **All** value indicates all ports on the AT-GS950/16 switch. You cannot change this parameter.

   Note

   You can use the **All** row value in the **Port** column to set the **Admin. Status**, **Mode**, **Jumbo**, **Flow Ctrl**, **EAP Pass**, and **BPDU** fields to the same values for all ports at the same time. In the **All** row when you select **Ignore**, **Enable** or **Disable** in one of these columns, it applies to all of the AT-GS950/16 switch ports.

   Trunk - This parameter indicates the trunk group number. A number in this column indicates that the port has been added to a trunk. This parameter can not be configured on this page. However, for information about configuring a trunk, refer to Chapter 6, "Static Port Trunking" on page 99.

   Type - Indicates the port type. On the AT-GS950/16, the port type

is 1000TX for 10/100/1000Base-T twisted-pair ports (1 through 14, 15R and 16R) and 100FX or 1000TX for the SFP ports (15 and 16) for copper or fiber SFP type.

Link Status - This parameter indicates the status of the link between the port and the end node connected to the port. The possible values are:

> **Up** -This parameter indicates a valid link exists between the port and the end node.

> **Down** -This parameter indicates the port and the end node have not established a valid link.

Admin. Status -This parameter indicates the operating status of the port. You can use this parameter to enable or disable a port. You may want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. You can enable the port to resume normal operation after the problem has been fixed. You can also disable an unused port to secure it from unauthorized connections. The possible values are:

> **Ignore** -This parameter applies to the **All** row only and indicates that the **Admin. Status** field must be set individually for each port.

> **Enabled** - This parameter indicates the port is able to send and receive Ethernet frames.

> **Disabled** - This parameter indicates the port is not able to send and receive Ethernet frames.

Jumbo -This parameter indicates whether or not jumbo frames can be accepted by the switch. You may want to activate jumbo frames when your switch will transmit video and audio files. The possible values are:

> **Ignore** -This parameter indicates that the **All** setting does not apply to the **Jumbo** field. In other words, each port is set individually.

> **Enabled** -This parameter indicates the port is permitted to accept jumbo frames.

> **Disabled** -This parameter indicates the port is not permitted to accept jumbo frames.

Note

When **QoS** is enabled on a port, the Jumbo frame parameter can not be enabled. To enable or disable **QoS**, see "Mapping CoS Priorities to Egress Queues" on page 198 and "CoS Page" on page 198.

Mode -This parameter indicates the speed and duplex mode settings for the port. You can use this parameter to set the speed and duplex mode of a port. The possible settings are:

Ignore -This parameter indicates that the **All** setting does not apply to the **Mode** field. In other words, each port is set individually.

Auto -This parameter indicates the port is using Auto-Negotiation to set the operating speed and duplex mode. The actual operating speed and duplex mode of the port are displayed in parentheses (for example, "1000F" for 1000 Mbps full duplex mode) after a port establishes a link with an end node.

Auto (1000F) -This parameter indicates the port is configured for 1000Mbps operation in Auto-Negotiation mode.

1000/Full -This parameter indicates the port is configured for 1000Mbps operation in full-duplex mode.

100/Full -This parameter indicates the port is configured for 100Mbps operation in full-duplex mode.

10/Full -This parameter indicates the port is configured for 10Mbps operation in full-duplex mode.

100/Half -This parameter indicates the port is configured for 100Mbps operation in half-duplex mode.

10/Half -This parameter indicates the port is configured for 10Mbps operation in half-duplex mode.

When selecting a **Mode** setting, the following points apply:

■ When a twisted-pair port is set to Auto-Negotiation, the end node should also be set to Auto-Negotiation to prevent a duplex mode mismatch. A switch port using Auto-Negotiation defaults to half-duplex if it detects that the end node is not using Auto-Negotiation. This can result in a mismatch if the end node is operating at a fixed duplex mode of full-duplex. To avoid this problem when connecting an end node with a fixed duplex mode of full-duplex to a switch port, disable Auto-Negotiation on the port and set the port's speed and duplex mode manually.

■ The only valid setting for the SFP ports is Auto-Negotiation.

Flow Control - This parameter reflects the current flow control setting on the port. The switch uses a special pause packet to notify the end node to stop transmitting for a specified period of time. The possible values are:

Ignore - This parameter indicates that the **All** setting does not apply to the **Flow Control** field. In other words, each port is set individually.

Enabled - This parameter indicates that the port is permitted to use flow control.

Disabled - This parameter indicates that the port is not permitted to use flow control.

EAP Pass - This parameter reflects the current Extensible Authentication Protocol (EAP) setting on the port. The possible values are:

Ignore - This parameter indicates that the **All** setting does not apply to the **EAP Pass** field. In other words, each port is set individually.

Enabled - This parameter indicates that the port is able to send and receive EAP packets.

Disabled - This parameter indicates that the port is disabled and is not able to send or receive EAP packets.

BPDU - This parameter reflects the current BPDU setting on the port.The possible values are:

Ignore - This parameter indicates that the **All** setting does not apply to the **BPDU** field. In other words, each port is set individually.

Enabled - This parameter indicates that the switch will pass BPDU frames through the switch and broadcast them through all other ports.

Disabled - This parameter indicates that the switch will not pass BPDU frames through the switch. With RSTP or STP enabled, the switch will receive BPDU frames and process them according to the spanning tree protocol.

3. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Chapter 4
STP and RSTP

This chapter provides background information about the Spanning Tree Protocol (STP) and the Rapid Spanning Tree Protocol (RSTP). In addition, there are procedures to configure STP and RSTP. The sections in the chapter include:

❐ "Overview" on page 72
❐ "STP and RSTP Global Settings" on page 81
❐ "STP and RSTP Port Settings" on page 84

For detailed information about STP, refer to IEEE Std 802.1D. For detailed information about RSTP, refer to IEEE Std 802.1w.

Note

To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Overview

The performance of an Ethernet network can be negatively impacted by the formation of a data loop in the network topology. A data loop exists when two or more nodes on a network can transmit data to each other over more than one data path. The problem that data loops pose is that data packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and can significantly reduce network performance.

STP and RSTP prevent data loops from forming by ensuring that only one path exists between the end nodes in your network. Where multiple paths exist, these protocols place the extra paths in a standby or blocking mode, leaving only one main active path.

In addition, STP and RSTP can activate a redundant path if the main path goes down. So not only do these protocols guard against multiple links between segments and the risk of broadcast storms, but they can also maintain network connectivity by activating a backup redundant path in case a main link fails.

Where the two protocols differ is in the time each takes to complete the process referred to as *convergence*. With the convergence process, when a change is made to the network topology, such as the addition of a new bridge, a spanning tree protocol must determine whether there are redundant paths that must be blocked to prevent data loops, or activated to maintain communications between the various network segments.

With STP, convergence can take up to a minute or more to complete in a large network. This can result in the loss of communication between various parts of the network during the convergence process and the subsequent lost of data packets.

RSTP is much faster. It can complete a convergence in seconds, and as such, greatly diminish the possible impact the process can have on your network. The STP implementation in the AT-S114 Management software complies with the IEEE 802.1d standard.

Only one spanning tree at a time can be active on the switch. The default protocol is RSTP. The RSTP implementation complies with the IEEE 802.1w standard.

The following subsections provide a basic overview on how STP and RSTP operate and define the different parameters that you can adjust.

Bridge Priority and the Root Bridge

The first task that bridges perform when a spanning tree protocol is activated on a network is the selection of a *root bridge.* A root bridge distributes network topology information to the other network bridges and is used by the other bridges to determine if there are redundant paths in the network.

A root bridge is selected by the *bridge priority* number, also referred to as the bridge identifier, and sometimes the bridge's MAC address. The bridge with the lowest bridge priority number in the network is selected as the root bridge. If two or more bridges have the same lowest bridge priority number, the one with the lowest MAC address is designated as the root bridge.

You can change the bridge priority number in the AT-S114 Management software. You can designate which switch on your network is the root bridge by giving it the lowest bridge priority number. You may also consider which bridge should function as the backup root bridge in the event you need to take the primary root bridge off line and assign that bridge the second lowest bridge identifier number.

The bridge priority has a range of 0 to 61440 in increments of 4096. To make this easier for you, the AT-S114 Management software divides the range into increments. You specify the increment that represents the desired bridge priority value. The range is divided into the following sixteen increments:

❑   0
❑   4096
❑   8192
❑   12288
❑   16384
❑   20480
❑   24576
❑   28672
❑   32768
❑   36864
❑   40960
❑   45056
❑   49152
❑   53248
❑   57344
❑   61440

Path Costs and Port Costs

After the root bridge has been selected, the bridges determine if the network contains redundant paths and, if one is found, select a preferred path while placing the redundant paths in a backup or blocking state.

Where there is only one path between a bridge and the root bridge, the bridge is referred to as the *designated bridge*, and the port through which the bridge is communicating with the root bridge is referred to as the *root port.*

If redundant paths exist, the bridges that are a part of the paths must determine which path is the primary, active path, and which path(s) are placed in the standby, blocking mode. This is accomplished by a determination of *path costs.* The path offering the lowest cost to the root bridge becomes the primary path and all other redundant paths are placed into a blocking state.

Path cost is determined by evaluating *port costs.* Every port on a bridge participating in STP has a cost associated with it. The cost of a port on a bridge is typically based on port speed. The faster the port, the lower the port cost. The exception to this is the ports on the root bridge, where all ports have a port cost of 0.

Path cost is the sum of the port costs between a bridge and the root bridge.

The port cost of a port on the switch is adjustable through the AT-S114 Management software. For STP and RSTP, the range is from 0 to 200,000,000.

Port Priority

If two paths have the same port cost, the bridges must select a preferred path. In some instances this can involve the use of the *port priority* parameter which is used as a tie breaker when two paths have the same cost.

The range for port priority is 0 to 240. As with bridge priority, this range is broken into increments, in this case multiples of 16. To select a port priority for a port, you enter the desired value. Table 1 on page 75 lists the values that are valid.

Table 1. Valid Port Priority Values

Step	Port Priority
1	0
2	16
3	32
4	48
5	64
6	80
7	96
8	112
9	128
10	144
11	160
12	176
13	192
14	208
15	224
16	240

Forwarding Delay and Topology Changes

If there is a change in the network topology due to a failure, removal, or addition of any active components, the active topology also changes. This may trigger a change in the state of some blocked ports. However, a change in a port state is not activated immediately.

It may take time for the root bridge to notify all bridges that a topology change has occurred, especially if it is a large network. A temporary data loop could occur if a topology change is made before all bridges have been notified and that could adversely impact network performance.

To forestall the formation of temporary data loops during topology changes, a port designated to change from blocking to forwarding passes through two additional states - listening and learning - before it begins to forward frames. The amount of time a port spends in these states is set by the forwarding *delay* value. This value states the amount of time that a port spends in the listening and learning states prior to changing to the forwarding state.

The forwarding delay value is adjustable in the AT-S114 Management software. The appropriate value for this parameter depends on a number of variables; the size of your network is a primary factor. For large networks, you should specify a value large enough to allow the root bridge sufficient time to propagate a topology change throughout the entire network. For small networks, you should specify a smaller value so that the time for a topology change is optimized for minimum data loss.

Note

The forwarding delay parameter applies only to ports on the switch that are operating in STP mode.

Hello Time and Bridge Protocol Data Units (BPDU)

The bridges that are part of a spanning tree domain communicate with each other using a bridge broadcast frame that contains a special section devoted to carrying STP or RSTP information. This portion of the frame is referred to as the bridge protocol data unit (BPDU). When a bridge is brought online, it issues a BPDU in order to determine whether a root bridge has already been selected on the network, and if not, whether it has the lowest bridge priority number of all the bridges and should therefore become the root bridge.

The root bridge periodically transmits a BPDU to determine whether there have been any changes to the network topology and to inform other bridges of topology changes. The frequency with which the root bridge sends out a BPDU is called the *hello time*. This is a value that you can set in the AT-S114 Management software. The interval is measured in seconds. Consequently, if the switch is selected as the root bridge of a spanning tree domain, it transmits a BPDU every two seconds.

Point-to-Point and Edge Ports

This section applies only to RSTP. Part of the task of configuring RSTP is defining the port types on the bridge, which is directly related to the device(s) connected to the port. With the port types defined, RSTP can reconfigure a network much quicker than STP when a change in network topology is detected.

There are two possible selections:

❏   Point-to-point port

❏   Edge port

If a bridge port is connected to another bridge or router port, it normally operates in full-duplex mode and is functioning as a point-to-point port. Figure 24 on page 77 illustrates two switches that are connected with one data link. This link is operating between two point-to-point ports.
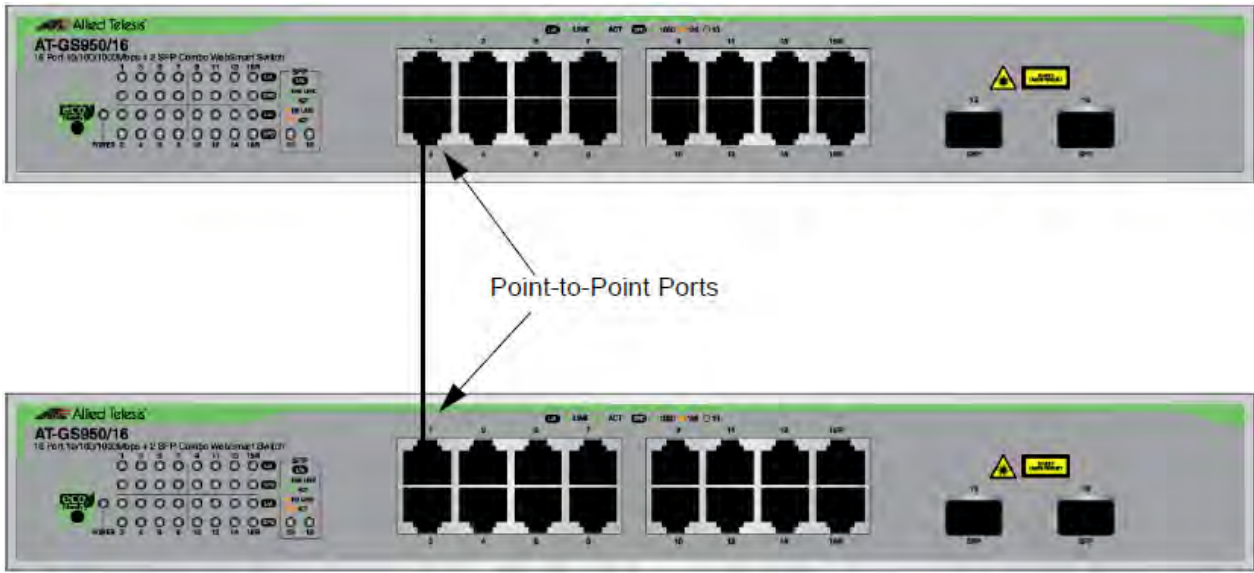
Figure 24. Point-to-Point Ports

A port operates as an edge port when it is connected to a network terminal device such as a workstation or a server. An edge port on a bridge should not have any STP or RSTP devices connected to it either directly or through another device connected to that port. In this configuration, since the port has no STP or RSTP devices connected to it, it will always forward network traffic. Figure 25 illustrates a port functioning as an edge port.
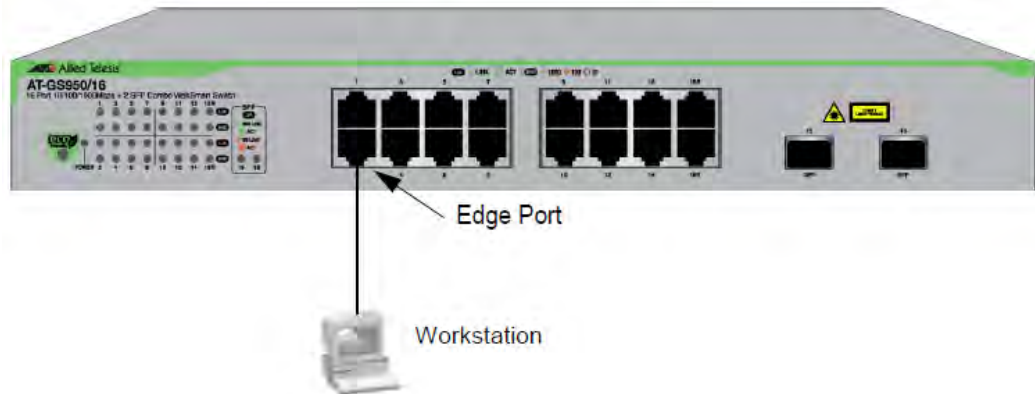
Figure 25. Edge Port

Mixed STP and RSTP Networks

RSTP IEEE 802.1w is fully compliant with STP IEEE 802.1d. Your network can consist of bridges running both protocols. STP and RSTP in the same network can operate together to create a single spanning tree domain.

If you decide to activate spanning tree on the switch, Allied Telesis recommends RSTP instead of STP, even when all of other switches in the network are running STP. The AT-GS950/16 switch can combine RSTP with the STP of the other switches. The switches monitors the traffic on each port for BPDU packets. Ports that receive RSTP BPDU packets operate in RSTP mode, while ports receiving STP BPDU packets operate in STP mode.

Spanning Tree and VLANs

The spanning tree implementation in the AT-S114 Management software can be a single-instance spanning tree as described in this chapter. If you choose to define multiple spanning trees on this switch, go to Chapter 5, "Multiple Spanning Tree Protocol" on page 87.

The single spanning tree encompasses all ports on the switch. If the ports are divided into different VLANs, the spanning tree crosses the VLAN boundaries. This can pose a problem in networks containing multiple VLANs that span two bridges and are connected with untagged ports. In this situation, spanning tree blocks a data link because it detects a suspected data loop. This can cause fragmentation of your VLANs.

This issue is illustrated in Figure 26 on page 79. VLANs 1 – 3 span two switches. One link consisting of untagged ports connect each VLAN. If STP or RSTP is activated on the switches, two of the links are disabled. As a direct result, two VLANs are disconnected between the bridges. In this example, the ports (on the non-root switch) that link the two parts of the VLANs 2 - 3 are changed to the blocking state, which disrupts these VLAN connections.
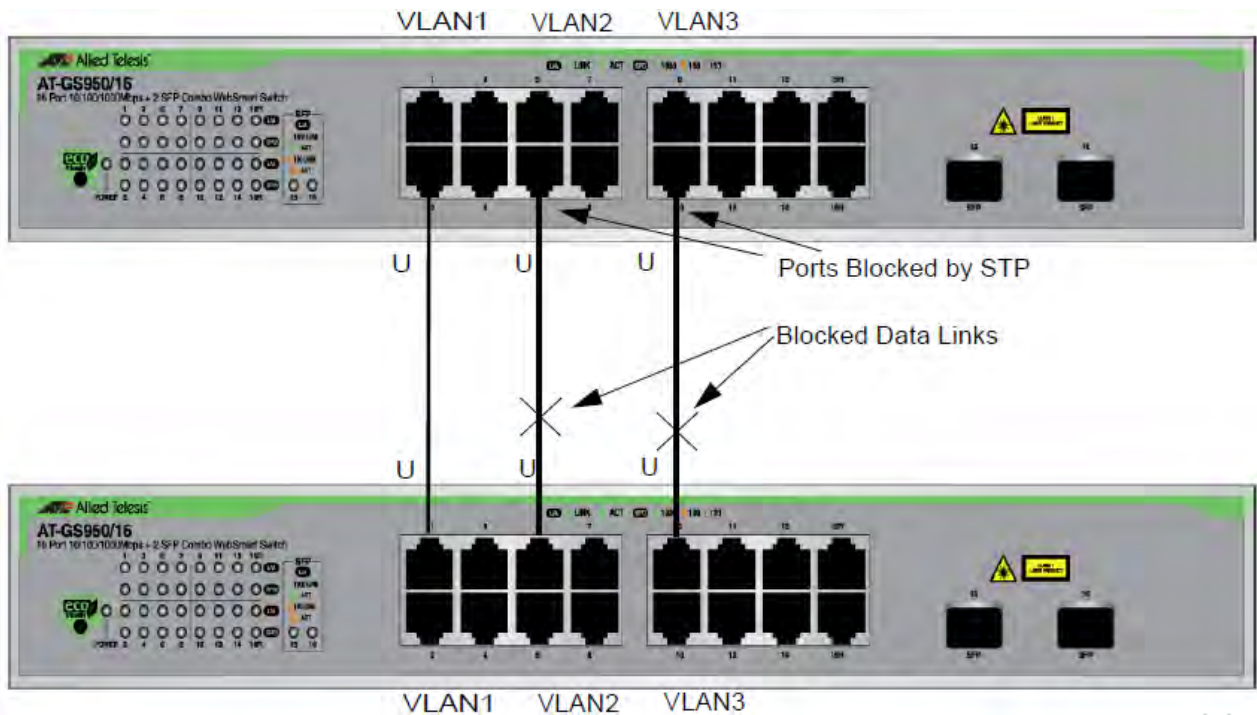
Figure 26. STP and VLAN Fragmentation with Untagged Ports

You can avoid this problem by connecting the switches using tagged instead of untagged ports when you plan to have STP or RSTP enabled on your network. If each port connecting the two bridges is a tagged member of all three VLANs, then traffic for each of the VLANs can still flow through one of the data links if the other two are blocked by Spanning Tree. The second and third data links act as redundant links in case the primary, unblocked data link becomes disabled. See Figure 27 on page 80 for an example of this solution.
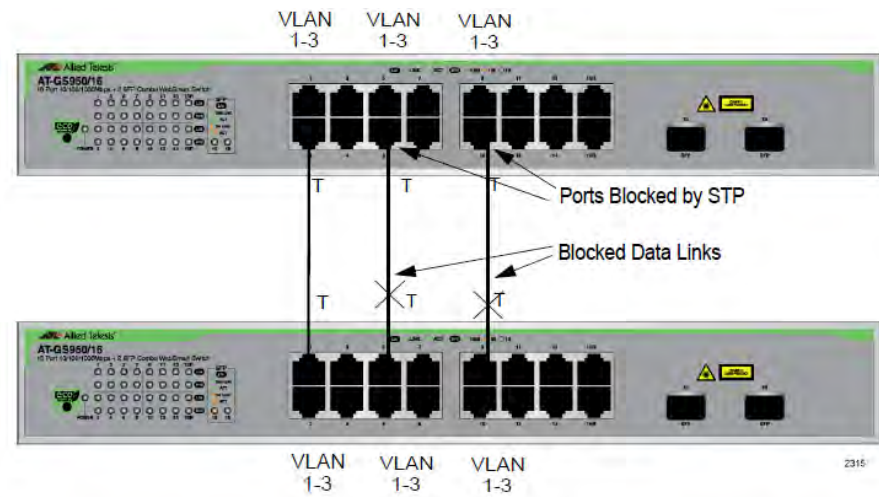
Figure 27. STP and VLAN Compatibility with Tagged Ports

Note

For information about tagged and untagged ports, refer to Chapter 13, "VLAN Overview" on page 158.

STP and RSTP Global Settings

To configure the global (non port-specific) STP and RSTP settings, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select the **Spanning Tree** folder. The **Spanning Tree** folder expands.

3. From the **Spanning Tree** folder, select **Protocol Settings**. The Spanning Tree Protocol Page is displayed. See Figure 28.

Figure 28. Spanning Tree Protocol Settings Page

The Spanning Tree Protocol Settings page allows you to configure global STP or RSTP protocols, as well as to view current settings of the feature.

4. In the upper portion of the page, you can set the following parameters:

Global STP Status - Use this menu to activate or de-activate the STP or RSTP feature on the switch. From the **Global STP Status** pull-down menu at the top of the page, select one of the following choices:

Enable - The STP or RSTP feature is active. The other parameters on the web page become active and are eligible for data to be entered.

Disable - The STP or RSTP feature is inactive. The other parameters on the web page become inactive and are greyed out so that data cannot be entered.

Protocol Version - Select **STP** or **RSTP** to set STP or RSTP on the switch. You can also select **MSTP**. For information on MSTP, refer to Chapter 5, "Multiple Spanning Tree Protocol" on page 87.

Bridge Priority - The priority number for the bridge. This number is used to determine the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, that is, the lowest value of all the other bridges, then the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes offline, the bridge with the lowest priority number automatically takes over as the root bridge. The bridge priority has a range of 0 to 61440 in increments of 4096, with 61440 being the highest priority.

Maximum Age - The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge.

Hello Time - This is the time interval between generating and sending configuration messages by the bridge. This parameter is active only when the switch is the root bridge.

Forward Delay - This is the time interval between generating and sending configuration messages by the bridge.

Transmit Hold Count - Applies only to MSTP. For information on MSTP, refer to Chapter 5, "Multiple Spanning Tree Protocol" on page 87.

Max Hop Count - Applies only to MSTP. For information on MSTP, refer to Chapter 5, "Multiple Spanning Tree Protocol" on page 87.

5. Once you have configured the parameters, click **Apply**. Clicking this button activates STP or RSTP and the above parameters on the switch.

   At the bottom section of the page, the following fields are listed:

Note
You cannot change these fields.

   Root Bridge - The Root Bridge is the MAC address of the bridge. The root bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority. You cannot change this parameter.

   Root Cost - The sum of all root port costs of all bridges between the switch's root port and the root bridge including the switch's root port cost.

   Root Maximum Age - The parameter displays the maximum amount of time that BPDUs are stored before being deleted on the root bridge.

   Root Forward Delay - The parameter displays the time interval between generating and sending configuration messages by the root bridge.

   Root Port - The active port on the switch that is communicating with the root bridge. If the switch is the root bridge for the LAN, then there is no root port, and the root port parameter is set to 0.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

STP and RSTP Port Settings

To configure the STP or RSTP port-specific settings, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select the **Spanning Tree** folder. The **Spanning Tree** folder expands.

3. From the **Spanning Tree** folder, select **Port Settings**. The Port Settings Page is displayed. See Figure 29 for a partial view of this page.

Port Settings

Port	STP Status	Priority	Admin Cost (0 = Auto)	External Cost	State	Edge	P2P	Restricted Role	Restricted TCN	Migrate	Apply
All	Ignore	Ignore		-	-	Ignore	Ignore	Ignore	Ignore	Restart	Apply
1	Enabled	128	0	20000	Disabled	Auto	Auto	False	False	Restart	Apply
2	Enabled	128	0	20000	Disabled	Auto	Auto	False	False	Restart	Apply
3	Enabled	128	0	20000	Disabled	Auto	Auto	False	False	Restart	Apply
4	Enabled	128	0	20000	Disabled	Auto	Auto	False	False	Restart	Apply
5	Enabled	128	0	20000	Disabled	Auto	Auto	False	False	Restart	Apply
6	Enabled	128	0	20000	Disabled	Auto	Auto	False	False	Restart	Apply
7	Enabled	128	0	20000	Disabled	Auto	Auto	False	False	Restart	Apply
8	Enabled	128	0	20000	Disabled	Auto	Auto	False	False	Restart	Apply

Figure 29. Port Settings Page

This page displays the following information about the ports:

Port - Indicates the port numbers on the AT-GS950/16 switch. You can select the **All** row to apply the same setting to all ports of your switch.

STP Status - Indicates if spanning tree protocol (either RSTP or STP) is active or not on the port. Select one of the following choices from the pull-down menu:

Enabled - The spanning tree protocol (RSTP or STP) is enabled on the port.

Disabled - The spanning tree protocol (RSTP or STP) is disabled on the port.

Priority - Indicates the port priority. See "Port Priority" on page 74 for more information.

Admin Cost - Indicates the path cost assigned to each port. For STP, the range is from 0 to 65,535. For RSTP, the range is from

0 to 200,000,000. A setting of 0 indicates Auto (path cost is based on link negotiation). The path cost is described in "Path Costs and Port Costs" on page 74.

External Cost - Applies only to MSTP. For information on MSTP, refer to Chapter 5, "Multiple Spanning Tree Protocol" on page 87.

State - Indicates one of the following port states:

Blocking - A blocking state does not allow network traffic to be sent or received on a the port, except for BPDU data. A port with a higher path cost to the root bridge than another on the switch will cause a switching loop and is placed in the blocking state by the Spanning Tree algorithm. The port's state may change to the forwarding state if the other links in use fail, and the Spanning Tree algorithm determines the port may transition to the forwarding state.

Listening - This state occurs on a port during the convergence process. The port in the listening state processes BPDUs and awaits new information that would cause the port to return to the blocking state.

Learning - While the port does not yet forward frames (packets) in this state, the port does learn source addresses from frames received and adds them to the filtering (switching) database.

Forwarding - A port that both receives and sends data. This indicates normal operation. STP continues to monitor the port for incoming BPDUs that indicate the port should return to the blocking state to prevent a loop.

Disabled - This state is not strictly part of STP. However, a network administrator can manually disable a port.

Edge - This parameter applies to RSTP only. Indicates whether or not a port is connected to an edge device in the network topology.

Auto - Automatic identification of edge ports. By default, Auto is enabled. With the Auto setting, the port looks for BPDUs for 3 seconds: If there are no BPDUs, the port is connected to an edge device and is in a forwarding state. If BPDUs are detected, the port is not connected to an edge device.

ForceTrue - The port is connected to an edge device, and the port will always be in a forwarding state.

ForceFalse - The port is not connected to an edge device.

P2P - This parameter applies to RSTP only. Indicates if the port is connected to another network device (point-to-point) in the network topology.

Auto - Automatically determines whether or not the port is connected to a network device in the network topology. By default, Auto is enabled.

ForceTrue - The port is connected to a network device in the network topology.

ForceFalse - The port is not connected to a network device in the network topology.

Restricted Role - Applies only to MSTP. For information on MSTP, refer to Chapter 5, "Multiple Spanning Tree Protocol" on page 87.

Restricted TCN - Applies only to MSTP. For information on MSTP, refer to Chapter 5, "Multiple Spanning Tree Protocol" on page 87.

Migrate - Clicking the **Restart** button under the **Migrate** field in the **All** row restarts the protocol migration process for all ports on the switch. Clicking the **Restart** button under the **Migrate** field for a specific port restarts the protocol migration process for that port only.

4. Click **Apply** for the port you are configuring.

5. To configure all of the ports to the same settings, in the **All** row, configure any or all settings.

6. Click **Apply**.

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Chapter 5

Multiple Spanning Tree Protocol

This chapter provides the procedures for configuring Multiple Spanning Tree Protocol (MSTP). You can find an overview and configuration guidelines for this feature in "MSTP Overview" on page 367.

When you configure MSTP, the information should be entered in order on the following web pages:

❐ "MSTP Global Settings" on page 88
❐ "Generic MSTP Port Settings" on page 91
❐ "MST Settings" on page 94
❐ "MST Port Settings" on page 96
❐ "Instance Information" on page 98 to view the settings

MSTP Global Settings

To configure the MSTP global settings, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select the **Spanning Tree** folder. The **Spanning Tree** folder expands.

3. From the **Spanning Tree** folder, select **Protocol Settings**. The Spanning Tree Protocol Settings Page is displayed. See Figure 30.
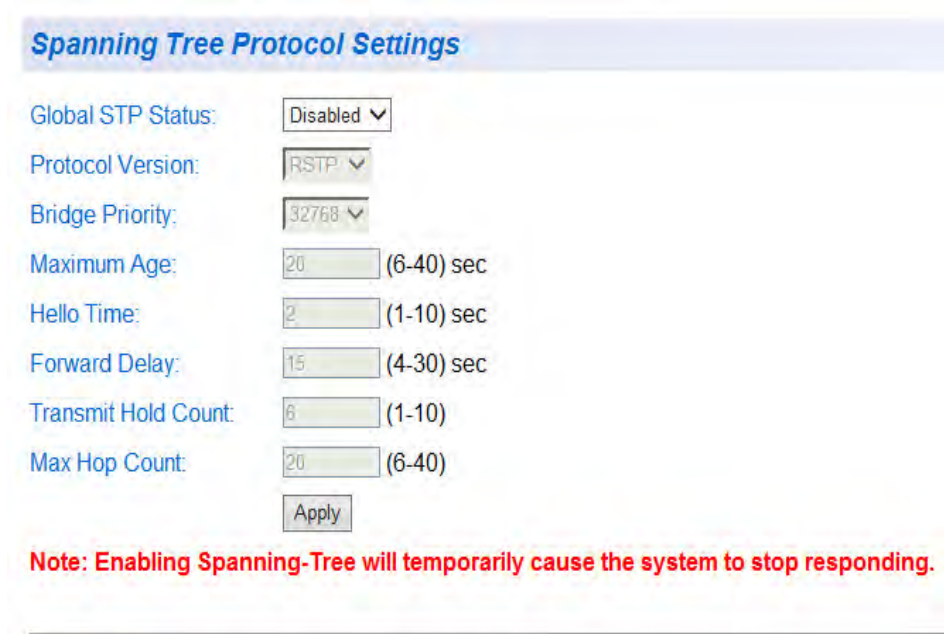
Figure 30. Spanning Tree Protocol Settings Page

The Spanning Tree Protocol Settings page allows you to configure global MSTP parameters, as well as to view current settings of the feature.

4. In the upper portion of the page, you can set the following parameters:

Global STP Status - Use this menu to activate or de-activate the MSTP feature on the switch. From the **Global STP Status** pull-down menu at the top of the page, select one of the following choices:

Enabled - The MSTP feature is active. The other parameters on the web page become active and are eligible for data to be entered.

Disabled - The MSTP feature is inactive. The other parameters on the web page become inactive and are greyed out so that data cannot be entered.

⚠️ **Caution**

Enabling or disabling MSTP causes the switch to temporarily stop switching Ethernet network traffic.

Note

BPDU Passthrough must be disabled before you enable MSTP. Refer to "Displaying and Configuring Ports" on page 67.

Protocol Version - Select **MSTP**.

Bridge Priority - This parameter specifies the priority used in determining the regional root for a particular MSTI. For more information about **Bridge Priority**, see Table 8 on page 378.

Maximum Age - The Maximum Age defines the amount of time a port will wait for STP/RSTP information. MSTP uses this parameter when interacting with STP/RSTP domains on the boundary ports. Its range is 6 - 40 seconds.

Hello Time - This is the time interval between generating and sending configuration messages by the bridge. This parameter is active only when the switch is the root bridge.

Forward Delay - The Forward Delay defines the time that the bridge spends in the listening and learning states. Its range is 4 - 30 seconds.

Transmit Hold Count - The Transmit Hold Count specifies the maximum number of BPDUs that the bridge can send per second. Its range is 1 - 10.

Max Hop Count - The Maximum Hop Count is a parameter set in a BPDU packet when it originates. It is decremented by 1 each time it is retransmitted by the next bridge. When the Hop Count value reaches zero, the bridge drops the BPDU packet. Its range is 6 - 40 hops.

5. Once you have configured the parameters, click **Apply**. Clicking this button activates MSTP and the above parameters on the switch.

   At the bottom section of the page, the following fields are listed:

   Note

   You cannot change these fields.

   Root Bridge - The Root Bridge is the MAC address of the bridge. The root bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority.

   Root Cost - The sum of all root port costs of all bridges between the switch's root port and the root bridge including the switch's root port cost.

   Root Maximum Age - Displays the maximum amount of time that BPDUs are stored before being deleted on the root bridge.

   Root Forward Delay - Displays the time interval between generating and sending configuration messages by the root bridge.

   Root Port - The active port on the switch that is communicating with the root bridge. If the switch is the root bridge for the LAN, then there is no root port, and the root port parameter is set to 0.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Generic MSTP Port Settings

To configure the generic MSTP parameters for each of the ports, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select the **Spanning Tree** folder. The **Spanning Tree** folder expands.

3. From the **Spanning Tree** folder, select **Port Settings**. The Port Settings Page is displayed. See Figure 31 for a partial view of this page.

Port Settings

Port	STP Status	Priority	Admin Cost (0 = Auto)	External Cost	State	Edge	P2P	Restricted Role	Restricted TCN	Migrate	Apply
All	Ignore ∨	Ignore ∨		-	-	Ignore ∨	Ignore ∨	Ignore ∨	Ignore ∨	Restart	Apply
1	Enabled ∨	128 ∨	0	20000	Disabled	Auto ∨	Auto ∨	False ∨	False ∨	Restart	Apply
2	Enabled ∨	128 ∨	0	20000	Disabled	Auto ∨	Auto ∨	False ∨	False ∨	Restart	Apply
3	Enabled ∨	128 ∨	0	20000	Disabled	Auto ∨	Auto ∨	False ∨	False ∨	Restart	Apply
4	Enabled ∨	128 ∨	0	20000	Disabled	Auto ∨	Auto ∨	False ∨	False ∨	Restart	Apply
5	Enabled ∨	128 ∨	0	20000	Disabled	Auto ∨	Auto ∨	False ∨	False ∨	Restart	Apply
6	Enabled ∨	128 ∨	0	20000	Disabled	Auto ∨	Auto ∨	False ∨	False ∨	Restart	Apply
7	Enabled ∨	128 ∨	0	20000	Disabled	Auto ∨	Auto ∨	False ∨	False ∨	Restart	Apply
8	Enabled ∨	128 ∨	0	20000	Disabled	Auto ∨	Auto ∨	False ∨	False ∨	Restart	Apply

Figure 31. Port Settings Page

You may choose a port and configure its MSTP parameters on this page. The following information is displayed:

Port - Indicates the port numbers on the AT-GS950/16 switch. You can select the **All** row to apply the same setting to all ports of your switch.

STP Status - Specifies if MSTP is Enabled or Disabled.

Enabled - MSTP is active on the port.

Disabled - MSTP is inactive on the port.

Priority - Specifies the spanning tree port priority.

Admin Cost - Specifies the cost of a port to the root.

External Cost - Indicates the operating cost of a port connected to a device outside its region.

State - Indicates one of the following port states:

Blocking - A blocking state does not allow network traffic to be sent or received on a the port, except for BPDU data. A port with a higher path cost to the root bridge than another on the switch will cause a switching loop and is placed in the blocking state by the Spanning Tree algorithm. The port's state may change to the forwarding state if the other links in use fail, and the Spanning Tree algorithm determines the port may transition to the forwarding state.

Listening - This state occurs on a port during the convergence process. The port in the listening state processes BPDUs and awaits new information that would cause the port to return to the blocking state.

Learning - While the port does not yet forward frames (packets) in this state, the port does learn source addresses from frames received and adds them to the filtering (switching) database.

Forwarding - A port that both receives and sends data. This indicates normal operation. STP continues to monitor the port for incoming BPDUs that indicate the port should return to the blocking state to prevent a loop.

Disabled - This state is not strictly part of STP. However, a network administrator can manually disable a port.

Edge - Specifies whether or not a port is connected to an edge device in the network topology. See "Point-to-Point and Edge Ports" on page 76 for more information.

Auto - The switch will automatically determine the port type.

ForceTrue - The port is connected to an edge device, and the port will always be in a forwarding state.

ForceFalse - The port is not connected to an edge device.

P2P - Specifies if the port is connected to another network device (point-to-point) in the network topology. See "Point-to-Point and Edge Ports" on page 76 for more information.

Auto - The switch will automatically determine the port type.

ForceTrue - The port is connected to a network device in the network topology.

ForceFalse - The port is not connected to a network device in the network topology.

Restricted Role - This parameter prevents the port from becoming a root port.

True - The port is prevented from being a root port or a port that is used to communicate with the root bridge.

False - This switch can only operate with RSTP and MSTP packets.

The net effect of setting all ports on the switch to True is that it forces the switch into the role of the root bridge regardless of other path costs in the network.

Restricted TCN - The Restricted TCN parameter does not allow Topology Change Notification (TCN) BPDUs to be processed on the port.

True - The port cannot process receive/transmit TCN BPDUs.

False - The port can process receive/transmit TCN BPDU packets.

Migrate - A switch running MSTP supports a built-in protocol migration mechanism that enables it to inter-operate with legacy 802.1D switches. Clicking the **Restart** button under the **Migrate** field in the **All** row restarts the protocol migration process for all ports on the switch. Clicking the **Restart** button under the **Migrate** field for a specific port restarts the protocol migration process for that port only.

4. Once you have configured the parameters, click **Apply** in the **Action** column.

5. If you choose to change the MSTP port configuration for other ports, repeat Step 3 and Step 4.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

MST Settings

You can create, modify and delete MST instance settings with the procedures in the following sections:

❑ ”Open MST Settings Page”

❑ "Specify Region and Revision Level" on page 94

❑ "Create VLAN Mapping to MST Instance" on page 95

❑ "Modify MST Instance" on page 95

❑ "Delete MST Instance" on page 95

Open MST Settings Page

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select the **Spanning Tree** folder. The **Spanning Tree** folder expands.

3. From the **Spanning Tree** folder, select **MST Settings**. The MST Settings Page is displayed. See Figure 32.

Figure 32. MST Settings Page

Specify Region and Revision Level

1. Define the region and revision:

   Configuration Name - This parameter specifies the region's name where the bridge is a member. This name must be identical to the regional names specified on other switches in the same MSTP region.

See "Multiple Spanning Tree Regions" on page 376 for more information.

Revision Level - The parameter indicates the region's revision and must be identical to the regional names specified on other switches in the same MSTP region. See "Multiple Spanning Tree Regions" on page 376 for more information.

2. Click **Apply**.

3. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Create VLAN Mapping to MST Instance

1. Enter the instance ID in the **MSTI ID** field (1-31).

2. Enter an existing VLAN ID or a range of existing VLAN IDs in the **VID List** field that you want to associate with the MSTI ID entered in Step 1.

3. Select the instance priority that determines the regional root using the **Priority** drop-down menu.

4. Click **Add**.
The Instance ID and the Mapped VLAN or VLANs will be displayed in the table on the page.

5. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Modify MST Instance

1. In the **VID List** field, enter the VLAN ID(s) for the MST Instance that you want to modify.

2. Use the **Priority** drop-down menu to select the MST instance priority.

3. In the **Action** column of the table, click **Apply**.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Delete MST Instance

1. In the **Action** column of the table, click **Delete** for the MST Instance that you want to delete.
The instance is deleted along with the mapped associations to the VLANs that are listed.

2. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

MST Port Settings

To configure the MST port settings, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**.
    The **Bridge** folder expands.

2. From the **Bridge** folder, select the **Spanning Tree** folder.
    The **Spanning Tree** folder expands.

3. From the **Spanning Tree** folder, select **MST Port Settings**.
    The MST Port Settings Page is displayed. See Figure 33.
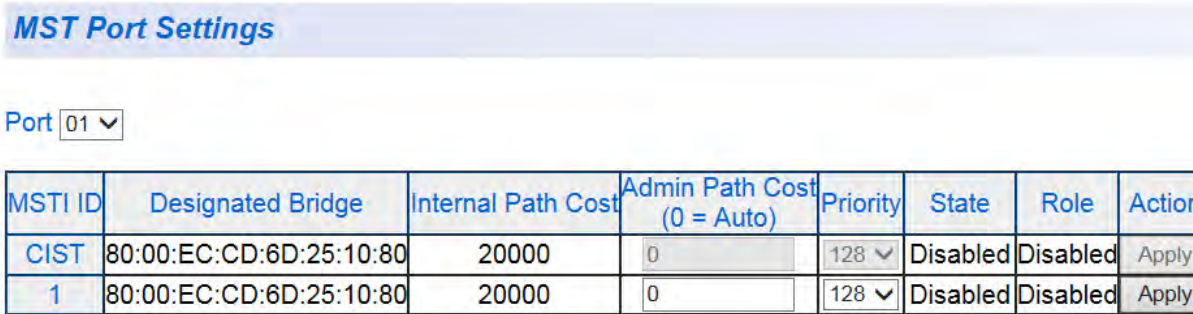
MST Port Settings

Port `01 ▾`

MSTI ID	Designated Bridge	Internal Path Cost	Admin Path Cost (0 = Auto)	Priority	State	Role	Action
CIST	80:00:EC:CD:6D:25:10:80	20000	0	128 ▾	Disabled	Disabled	Apply
1	80:00:EC:CD:6D:25:10:80	20000	0	128 ▾	Disabled	Disabled	Apply

Figure 33. MST Port Settings Page

You may choose a port and configure its MSTP parameters on this page. The following information is displayed:

Port - You can select one of the ports on the AT-GS950/16 switch using the **Port** drop-down menu.

MSTI ID - Indicates the MSTP Instance associated with this port.

Designated Bridge - Indicates the bridge providing the least-cost path to the root bridge from a network segment.

Internal Path Cost - Indicates the operating cost of a port when it is connected to a bridge in the same MSTP region.

Admin Path Cost - Specifies the cost of a port to the root.

Priority - Select the spanning tree port priority using the **Priority** drop-down menu.

State - Indicates the port state:

Enabled - Allows the port to forward packets.

Disabled - Does not allows the port to forward packets.

Role - Indicates whether or not the port is prevented from being a root port.

Enabled - The port is prevented from being a root port or a port that is used to communicate with the root bridge.

Disabled - This switch can only operate with RSTP and MSTP packets.

4. Once you have configured the parameters, click **Apply** in the **Action** column.

5. If you choose to change the MSTP port settings for other ports, repeat Step 3 and Step 4.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Instance Information

To view MST instance information, perform the following:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select the **Spanning Tree** folder. The **Spanning Tree** folder expands.

3. From the **Spanning Tree** folder, select **Instance Information**. The Instance Information Page is displayed. See Figure 34.

Instance Information

MSTI ID	Internal Root Cost	Root Port	Regional Root Bridge	Designated Bridge	Instance Priority
CIST	0	0	80:00:EC:CD:6D:25:10:80	80:00:EC:CD:6D:25:10:80	32768
1	0	0	10:00:EC:CD:6D:25:10:80	10:00:EC:CD:6D:25:10:80	4096

Figure 34. Instance Information Page

The following information displayed on this page shows the current status of each MST instance:

MSTI ID - MST instance ID.

Internal Root Cost - Operating cost of a port when it is connected to a bridge in the same MSTP region.

Root Port - Active port on the switch that is communicating with the root bridge.

Regional Root Bridge - The root bridge of the MST instance.

Designated Bridge - The bridge providing the least-cost path to the root bridge from a network segment.

Instance Priority - Regional root for a particular MST instance.

Chapter 6
Static Port Trunking

This chapter contains a description of port trunking and the procedures for creating, modifying, and deleting a static port trunk. The following topics are discussed:

❑ "Overview" on page 100
❑ "Create a Port Trunk" on page 103
❑ "Modify a Port Trunk" on page 105
❑ "Disable a Port Trunk" on page 107

> **Note**
> For information about Link Aggregation Control Protocol (LACP) port trunking, see Chapter 7, "LACP Port Trunks" on page 109.

> **Note**
> To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Overview

A port trunk is an economical way for you to increase the bandwidth between the Ethernet switch and another networking device, such as a network server, router, workstation, or another Ethernet switch. A port trunk is a group of ports that have been grouped together to function as one logical path. A port trunk increases the bandwidth between the switch and another network device and is useful in situations where a single physical link between the devices is insufficient to handle the traffic load.

A static port trunk consists of 2 or more ports on the switch that function as a single virtual link between the switch and another device. A static port trunk improves performance by distributing the traffic across multiple ports between the devices and enhances reliability by reducing the reliance on a single physical link.

A static trunk is easy to configure. You designate the ports on the switch that are in the trunk, and the AT-S114 Management software on the switch automatically groups them together.

The example in Figure 35 illustrates a static port trunk of four links between two AT-GS950/16 switches.
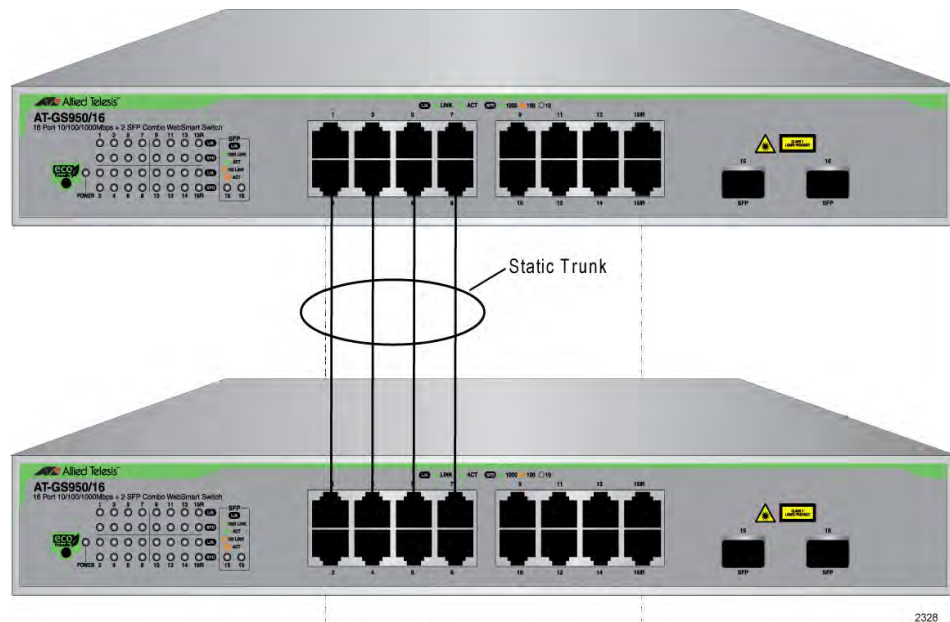
Figure 35. Static Port Trunk Example

Network equipment vendors tend to employ different techniques to implement static trunks. Consequently, a static trunk on one device may be incompatible with the same feature on a device from a different manufacturer. For this reason, static trunks are typically employed only between devices from the same vendor. That is not to say that an Allied Telesis Layer 2 managed switch cannot form a static trunk with a device from another manufacturer; however, the implementations of static trunking on the two devices may be incompatible.

Also, note that a static trunk does not provide for redundancy or link backup. If a port in a static trunk loses its link, the trunk's total bandwidth is diminished. Although the traffic carried by the lost link is shifted to one of the remaining ports in the trunk, the bandwidth remains reduced until the lost link is re-established or you reconfigure the trunk by adding another port to it.

General Guidelines

Following are the guidelines for creating a static trunk:

- Allied Telesis recommends setting static port trunks between Allied Telesis networking devices to ensure compatibility.

- A static trunk can contain up to 10 ports.

- The ports of a static trunk must be of the same medium type. They can be all twisted-pair ports or all fiber optic ports, but not a combination of the two.

- The ports of a trunk can be either consecutive (for example, Ports 2 through 4) or nonconsecutive (for example, ports 3, 5, and 7).

- Before creating a port trunk, verify that the settings are the same for all ports in the trunk including speed (1000/Full), duplex mode, flow control, back pressure settings and VLAN membership. If these settings are not the same, then the switch does not allow you to create the trunk.

Note

When a trunk group is formed with only combo ports as members, all port members are configured to the forced port mode at 1000/Full. The trunk ports on the connecting network switch should also be configured for 1000/Full to insure speed and duplex compatibility between the switches.

- After you have created a port trunk, a change to the speed, duplex mode, flow control, or back pressure of any port in the trunk automatically implements the same change on all the other member ports.

- A port can belong to only one static trunk at a time.
- The ports of a static trunk can be configured to be members of more than one VLAN.
- The ports of a static trunk can be either untagged or untagged members of the same VLAN.

The switch selects a port in the trunk to handle broadcast packets and packets of unknown destination. The switch makes this choice based on a hash algorithm, depending upon the source and destination MAC addresses.

Create a Port Trunk

This procedure explains how to create a static port trunk.

⚠️ **Caution**

Do not connect the cables of a port trunk to the ports on the switch until you have configured the ports on both the switch and the end nodes. Connecting the cables prior to configuring the ports can create loops in your network topology. Loops can result in broadcast storms which can severely limit the effective bandwidth of your network.

To create a port trunk, perform the following procedure:

1. Select the **Bridge** folder.
   The **Bridge** folder expands.

2. From the **Bridge** folder, select the **Trunk Config** folder.
   The **Trunk Config** folder expands.

3. From the **Trunk Config** folder, select **Trunking**.
   A partial view of the Trunking Page is displayed in Figure 36.

Figure 36. Trunking Page

If the switch does not contain a port trunk, all of the ports on the switch are unchecked. If there is a port trunk, the ports in the trunk are checked.

4. Click the check boxes of the ports that will make up the port trunk.

   A check in a box indicates the port is a member of the trunk. No check means the port is not a member. A port trunk can contain up to 10 ports.

5. Change the trunk mode from **Disable** to another setting using the pull-down menu. The choices are the following:

   Active - The specific aggregator will broadcast and respond to LACP Data Unit (LACPDU) packets. This setting enables the LACP feature for the trunk.

   Passive - The specific aggregator will not broadcast LACPDU packets, but it will respond to them. This setting disables the LACP feature for the trunk.

   Manual - Enables static port trunking and disables the LACP feature for the trunk.

   Disable - Disables the static port trunk and disables the LACP feature for the trunk.

6. Click **Apply**.

7. If you did not select the trunk mode, **Disable**, the trunk is now operational on the switch.

8. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

9. Configure the port trunk on the other switch.

10. Connect the Ethernet cables between trunk ports on the AT-GS950/16 switch and the trunk ports on the other switch.

Modify a Port Trunk

This procedure explains how to change the status of a port trunk and add or remove ports from a port trunk.

> ⚠️ **Caution**
>
> Before you disable or modify a port trunk, disconnect all of the cables from the ports of the trunk. Leaving the cables connected during the reconfiguration of a trunk can create loops in your network topology. Loops can result in broadcast storms which can severely limited the effective bandwidth of your network.

To add or remove ports from a trunk, perform the following procedure:

1. Disconnect all of the Ethernet cables from the ports of the trunk.

2. Select the **Bridge** folder.
   The **Bridge** folder expands.

3. From the **Bridge** folder, select the **Trunk Config** folder.
   The **Trunk Config** folder expands.

4. From the **Trunk Config** folder, select **Trunking**.
   The Trunking Page is shown in Figure 36 on page 103.

5. Click the pull-down menu of the port trunk you want to modify and change the status to one of the following options:

   Disable - Disables the port trunk.

   Active - The aggregator will broadcast and respond to LACPDU packets. This setting enables the LACP feature.

   Passive - The aggregator will not broadcast LACPDU packets, but it will respond to them. This setting enables the LACP feature.

   Manual - Enables static port trunking and disables the LACP feature.

6. To add or remove a port from a trunk, click the check box for the port in the corresponding trunk row.
   A check in a box indicates the port is a member of the trunk. No check means the port is not a member. A port trunk can contain up to 10 ports.

7. Click **Apply**.

8. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

9. Configure the port trunk on the other switch with the same parameters.

10. Connect the Ethernet cables between trunk ports on the AT-GS950/16 switch and the trunk ports on the other switch.

Disable a Port Trunk

This procedure explains how to disable a port trunk.

⚠️ **Caution**

Before you disable or modify a port trunk, disconnect all of the cables from the ports of the trunk. Leaving the cables connected during the reconfiguration of a trunk can create loops in your network topology. Loops can result in broadcast storms which can severely limit the effective bandwidth of your network.

To disable a port trunk, perform the following procedure:

1. Disconnect all of the Ethernet cables from the ports of the trunk.

2. Select the **Bridge** folder.
   The **Bridge** folder expands.

3. From the **Bridge** folder**,** select the **Trunk Config** folder.
   The **Trunk Config** folder expands.

4. From the **Trunk Config** folder, select **Trunking**.
   The Trunking Page is shown in Figure 36 on page 103.

5. To disable a port trunk, select **Disable** from the pull-down menu next to the trunk that you want to disable.

6. Click **Apply**.

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

8. Modify the port trunk configuration in the same way on the other switch.

Chapter 7

LACP Port Trunks

This chapter contains overview information about LACP port trunks and the procedures for setting this feature. This chapter contains the following sections:

❑ "Overview" on page 110

❑ "System Priority" on page 111

❑ "Port Priority Value" on page 112

❑ "General Guidelines" on page 113

❑ "Group Status" on page 115

❑ "Port Priority Configuration" on page 118

> **Note**
>
> For information about port trunking, see Chapter 6, "Static Port Trunking" on page 99.

> **Note**
>
> To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Overview

LACP (Link Aggregation Control Protocol) port trunks perform the same function as static trunks. They increase the bandwidth between network devices by distributing the traffic load over multiple physical links. The advantage of an LACP trunk over a static port trunk is its flexibility. While implementations of static trunking tend to be vendor-specific, the AT-S114 Management software implementation of LACP is compliant with the IEEE 802.3ad standard, making it interoperable with equipment from other vendors that also comply with the standard. Therefore, you can create an LACP trunk between an Allied Telesis device and network devices from other manufacturers.

Another advantage is that ports in an LACP trunk can function in a standby mode. This adds redundancy and resiliency to the trunk. If a link in a static trunk goes down, the overall bandwidth of the trunk is reduced until the link is re-established or another port is added to the trunk. In contrast, an LACP trunk can automatically activate ports in a standby mode when an active link fails so that the maximum possible bandwidth of the trunk is maintained.

For example, assume you create an LACP trunk of ports 1 to 9 on a switch and the switch is using ports 1 to 4 as the active ports and 9 as reserve. If an active port loses its link, the switch automatically activates one of the reserve ports to maintain maximum bandwidth of the trunk.

The main component of an LACP trunk is an *aggregator* which manages a group of ports on the switch. On the AT-GS950/16 switch, the ports assigned to a trunk group are automatically assigned to an aggregator. Only one aggregator can be assigned to each trunk group. With LACP activated, each active trunk group is referred to as an *aggregate trunk*.

An aggregate trunk can consist of any number of ports on a switch, but only a maximum of eight ports can be active at a time. If an aggregate trunk contains more ports than can be active at once, the extra ports are placed in a standby mode. Ports in the standby mode do not pass network traffic, but they do transmit and accept LACP Data Unit (LACPDU) packets, which the switch uses to search for LACP compliant devices.

Only ports that are part of an aggregator transmit LACPDU packets. A port that is part of an aggregator assumes that the other port is not part of an LACP trunk if it does not receive LACPDU packets from its corresponding port on the other device. Instead, it functions as port in standby mode and does not forward network traffic. However, it does continue to send LACPDU packets. If it begins to receive LACPDU packets, it automatically transitions to an active or standby mode as part of an aggregate trunk.

System Priority

It is possible for two devices interconnected by an aggregate trunk to encounter a conflict when they form the trunk. For example, the two devices might not support the same number of active ports in an aggregate trunk or might not agree on which ports are active and which are in standby mode.

If a conflict does occur, the two devices need a mechanism for resolving the problem and deciding whose LACP settings take precedence. This is the function of the system LACP priority value. This value is used whenever the devices encounter a conflict creating a trunk - the lower the number, the higher the priority. As a result, the settings on the device with the higher priority take precedence over the settings on the other device. If both devices have the same system LACP priority value, the settings on the switch with the lowest MAC address take precedence. In the AT-S114 Management software, the MAC address is called the System ID.

The LACP System Priority is pre-assigned, and you cannot alter this parameter.

Port Priority Value

The switch uses a port's LACP priority to determine which ports are active and which are in the standby mode in situations where the number of ports in the aggregate trunk exceeds the highest allowed number of active ports. This parameter is a value in a range of 1 to 65535, based on the port number. The lower the number, the higher the priority. Ports with the highest priorities are designated as the active ports in an aggregate trunk.

For example, if both 802.3ad-compliant devices support up to eight active ports and there are a total of nine or more ports in the trunk, the eight ports with the highest priorities (lowest priority values) are designated as the active ports, and the others are placed in the standby mode. If an active link goes down on a active port, the standby port with the next-highest priority is automatically activated to take its place.

The selection of the active links in an aggregate trunk is dynamic and changes as links are added, removed, lost, or re-established. For example, if an active port loses its link and is replaced by another port in the standby mode, the re-establishment of the link on the originally active port causes the port to return to the active state by virtue of having a higher priority value than the replacement port, which returns to the standby mode.

Two conditions must be met for a port in an aggregate trunk to function in the standby mode. First, the number of ports in the trunk must exceed the highest allowed number of active ports, and second, the port must be receiving LACPDU packets from the other device. A port functioning in the standby mode does not forward network traffic. However, it continues to send LACPDU packets. If a port that is part of an aggregator does not receive LACPDU packets, it functions as a normal Ethernet port and forwards network packets along with LACPDU packets.

Note
You can adjust the value of a port's priority.

General Guidelines

The following guidelines apply when creating aggregators:

- LACP must be activated on both the AT-GS950/16 switch and its partner device.

- The other device must be 802.3ad-compliant.

- The AT-S114 Management software supports up to eight active ports in an aggregate trunk at a time.

- The AT-GS950/16 Gigabit Ethernet Switch can support up to eight static and LACP aggregate trunk groups at a time (for example, four static trunks and four LACP trunks). An LACP trunk is counted against the maximum number of trunks only when it is active.

- The ports of an aggregate trunk must be the same medium type: all twisted pair ports or all fiber optic ports.

- The ports of a trunk can be consecutive (for example ports 1-5) or nonconsecutive (for example, ports 2, 4, 6, 8).

- A port can belong to only one aggregator at a time.

- A port cannot be a member of an aggregator and a static trunk at the same time.

- The ports of an aggregate trunk must be untagged members of the same VLAN.

- Twisted pair ports must be set to Auto-Negotiation or 1000 Mbps, full-duplex mode. LACP trunking is not supported in half-duplex mode.

- 1000Base-X fiber optic ports must be set to full-duplex mode.

- You can create an aggregate trunk of transceivers with 1000Base-X fiber optic ports.

- Only those ports that are members of an aggregator transmit LACPDU packets.

- A member port of an aggregator functions as part of an aggregate trunk only if it receives LACPDU packets from the remote device. If it does not receive LACPDU packets, it functions as a regular Ethernet port, forwarding network traffic, while also continuing to transmit LACPDU packets.

- The port with the highest priority in an aggregate trunk carries broadcast packets and packets with an unknown destination.

- Prior to creating an aggregate trunk between an Allied Telesis device and another vendor's device, refer to the vendor's documentation to determine the maximum number of active ports the device can support in a trunk. If the number is less than eight, the maximum number for the AT-GS950/16 switch, you should assign the other vendor's device a higher system LACP priority than your AT-GS950/16 switch. This can help avoid a conflict between the devices if some ports are placed in the standby mode when the devices create the trunk. For background information, refer to "System Priority" on page 111.

- LACPDU packets are transmitted as untagged packets.

Group Status

To display the LACP Group Status, perform the following procedure:

1. Select the **Bridge** folder.
   The **Bridge** folder expands.

2. From the **Bridge** folder, select the **Trunk Config** folder.
   The **Trunk Config** folder expands.

3. From the **Trunk Config** folder, select **LACP Group Status**.
   The LACP Group Status Page is displayed. See Figure 37 for a partial
   view of this page.
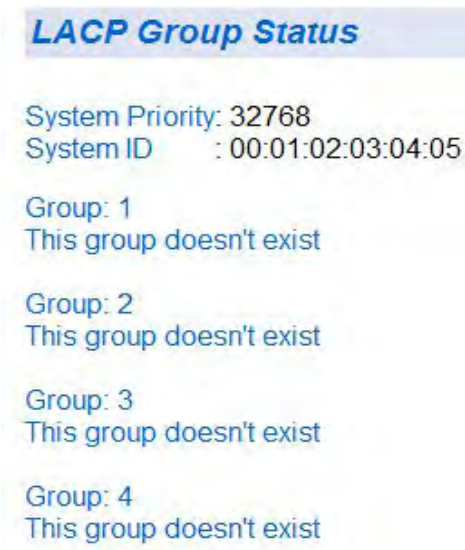
Figure 37. LACP Group Status Page

Note
Go to "Create a Port Trunk" on page 103 to directly change the
parameters on this page:

The **System Priority** is a pre-assigned value that you cannot alter.
This value applies to the switch. See "System Priority" on page 111.

The **System ID** is a MAC address value assigned to the individual
switch. You cannot change this value.

Group 1 to 8 indicates the ID number of the trunk (aggregation group).

Configuration Example

The following procedure provides an example for an LACP group configuration:

1. Use the procedure given in "Create a Port Trunk" on page 103: Configure Trunk ID 1 as Active with ports 1 - 9.

    The LACP Group Status Page is updated. This configuration is shown in Figure 38 before the Ethernet cables are connected.

LACP Group Status

System Priority : 32768

System ID   : EC:CD:6D:25:10:80

Group: 1

Aggregator	Active Port List	Standby Port List
1		

Group: 2
This group doesn't exist

Group: 3
This group doesn't exist

Group: 4
This group doesn't exist

Group: 5
This group doesn't exist

Group: 6
This group doesn't exist

Group: 7
This group doesn't exist

Group: 8
This group doesn't exist

Figure 38. LACP Group Status Page with No Cables Connected

2. Physically connect the network cables between the switch and a second LACP device.
    The second device should be pre-configured with an LACP activated trunk of nine or more ports.

    The LACP Group Status Page is updated. An example of these updates is shown in Figure 39 on page 117 after nine trunking cables are installed and the ports have Link-Up status.

Figure 39. LACP Group Status Page with Three Cables Connected

You can now see that each port has been grouped under a single aggregator since the ports are now in a Link-Up status.

Port Priority Configuration

To select a priority for an LACP port, perform the following procedure:

1. Select the **Bridge** folder.
   The **Bridge** folder expands.

2. From the **Bridge** folder, select the **Trunk Config** folder.
   The **Trunk Config** folder expands.

3. From the **Trunk Config** folder, select **Port Priority**.
   The AT-GS950/16 Port Priority Page is displayed. See Figure 40 for a partial view of this page.

Port Priority

System Priority : 32768

System ID : EC:CD:6D:25:10:80

Port	Priority (0-65535)
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0

Figure 40. AT-GS950/16 Port Priority Page

The **System Priority** is a preassigned value that you cannot alter. This value applies to the switch. See "System Priority" on page 111.

The **System ID** is a MAC address value assigned to the switch. You cannot change this value.

4. To set the port priority, select a value from 0 to 65535 in the Priority column for the port you want to alter. For more information, see "Port Priority Value" on page 112

5. Select **Apply**.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Chapter 8

Port Mirroring

This chapter describes the Port Mirroring feature and the procedure for setting up port mirroring. Port mirroring allows you to unobtrusively monitor the ingress and egress traffic on a port by having the traffic copied to another port. This chapter contains the following sections:

❑ "Overview" on page 120
❑ "Port Mirroring Configuration" on page 121
❑ "Disable Port Mirroring" on page 123

Note
To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Overview

The port mirroring feature allows you to unobtrusively monitor the traffic received and transmitted on one or more ports by copying the traffic to another switch port. You can connect a data analyzer to the port where the traffic is copied and monitor the traffic on the other ports without impacting network performance or speed.

A port mirror has two component ports. The port or ports whose traffic you want to mirror is called the *source port(s)*. The port where the traffic will be copied to is called the *mirroring port*.

Observe the following guidelines when you create a port mirror:

- You can select more than one source port at a time. However, the more ports you mirror, the less likely the mirroring port is able to handle all the traffic. For example, if you mirror the traffic of six heavily active ports, the destination port is likely to drop packets, meaning that it does not provide an accurate mirror of the traffic of the six source ports.
- The source and mirror ports must be located on the same switch.
- You can mirror the ingress or egress traffic of the source ports or both.
- While the Mirroring feature is enabled, the mirroring port is dedicated to monitoring the traffic from the source ports and cannot be used for regular network operations.

Port Mirroring Configuration

To configure Port Mirroring, perform the following procedure:

1. Select the **Bridge** folder.
    The Bridge folder expands.

2. From the **Bridge** folder, select **Mirroring**.
    The Mirroring Page is displayed. See Figure 41.

Figure 41. AT-GS950/16 Mirroring Page

3. Click the pull-down menu next to the **Status** field and select one of the following choices:

    Enabled - This parameter activates the Port Mirroring feature, and the rest of the configuration parameters become active on the page.

    Disabled - This parameter de-activates the Port Mirroring feature, and the rest of the configuration parameters become inactive on the page.

4. Click **Mirroring Port** and from the pull-down menu, select the port.

5. For the source port, select the port(s) whose ingress, egress, or both ingress and egress traffic you want to monitor.
    To select all ports for an ingress or egress, click the **All** button. (The **All** button changes to **Clear**.)
    To de-select all ports for an ingress or egress, click the **Clear** button.
    A check in a box indicates the Ingress or Egress traffic for a port has been selected.

6. Click **Apply** on the right-hand side of the page.
   The Port Mirroring configuration is implemented immediately on the
   AT-GS950/16 switch.
   You can connect a data analyzer to the mirroring port to monitor the
   Ethernet traffic on the source port(s).

7. From the main menu on the left side of the page, select **Save Settings
   to Flash** to permanently save your changes.

Disable Port Mirroring

To disable Port Mirroring, perform the following procedure:

1. Select the **Bridge** folder.
    The Bridge folder expands.

2. From the **Bridge** folder, select **Mirroring**.
    The Mirroring page is shown in Figure 41 on page 121.

3. Next to the **Status** field, select **Disabled** and click **Apply**.
    Port mirroring is immediately disabled on the switch, and the parameters on the web page become inactive. You can now use the mirroring port for regular network operations.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Chapter 9
Loopback Protection

This chapter explains how to configure the Loopback Protection feature for specific ports on the AT-GS950/16 switch. If the Tx and Rx pairs on the same port are connected, then this feature detects this condition and disables the port for a pre-configured amount of time.

This chapter contains the following topics:

> **Note**
>
> To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Configuration

To configure the Loopback Detection feature, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**.

   The **Bridge** folder expands.

2. From the **Bridge** folder, select **Loopback Detection**.
   The AT-GS950/16 Loopback Detection Page is displayed. See Figure 42 for a partial view of this page.

Loopback Detection

State	○ Enabled ⦿ Disabled

Loopback Detection Global Settings

Interval (1-32767)	2	sec	
Recover Time (0 or 60-1000000, 0 is Disabled)	60	sec	Apply

Note: Disabling will turn off the function and return all values to default.

Port	Loopback Detection State	Loop Status	Action
All	Ignore	-	Apply
1	Disabled	Normal	Apply
2	Disabled	Normal	Apply
3	Disabled	Normal	Apply
4	Disabled	Normal	Apply
5	Disabled	Normal	Apply
6	Disabled	Normal	Apply
7	Disabled	Normal	Apply
8	Disabled	Normal	Apply

Figure 42. AT-GS950/16 Loopback Detection Page

3. For the **Loopback Detection State** field at the top of the page, select one of the following radio buttons:

   Enabled: This selection enables the Loopback Detection feature across the switch. This state must be enabled for the individual port **Loopback Detection State** to be effective.

   Disabled: This selection disables the Loopback Detection feature on the switch.

4. Under the **Loopback Detection Global Settings**, configure the following parameters:

    Interval: This parameter sets the interval of time that the ports are tested. The range is 1 to 32767 seconds.

    Recover Time: This parameter sets the amount of time that the port will take to recover once the loopback condition has been removed. The range is 60 to 1000000 seconds.

    If the **Recover Time** is set to 0, the port recovery is disabled until it is manually reset. It can be reset by re-configuring the **Recover Time** to its normal operating range or by disabling the Loopback Detection feature on the switch.

5. Click the **Apply** button just above the **Action** column in the table at the bottom of the page.

    The **Loopback Detection Global Settings** parameters become active.

6. In the table at the bottom of the page, select one of the **Loopback Detection State** choices from the pull-down menu:

    Ignore: This parameter indicates that the setting in the **All** row does not apply to the **Loopback Detection State** field. In other words, each port is set individually.

    Enabled: This selection enables the Loopback Detection feature for each port. This state must be enabled along with the **State** field at the top of the page before this feature can be active on the selected port.

    Disabled: This selection disables the Loopback Detection feature on the selected port.

    Note

    In the **All** row when you select **Enable** or **Disable** instead of **Ignore**, the selection applies to all of the AT-GS950/16 switch ports.

    ---

7. Click the **Apply** button in the Action column of the table.

8. Repeat Step 6 and Step 7 for other individual port settings.

9. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Status

The status of the Loopback Detection is given in the Loop Status column of the table at the bottom of the Loopback Detection page. See Figure 42 on page 126. The status is one of the following states:

Normal: This status indicates that the port does not have the Tx to Rx pairs connected.

Disabled: This status indicates that the port does not have the Tx to Rx pairs connected. The **Disabled** state will be reset to **Normal** after two conditions are both met:

- The loopback condition does not exist anymore.
- The specified **Recovery Time** has elapsed.

Note

If the **Recover Time** is set to 0, the port recovery is disabled until it is manually reset. It can be reset by re-configuring the **Recover Time** to its normal operating range or by disabling the Loopback Detection feature on the switch.

Chapter 10

MAC Address Table

This chapter provides a description of the static unicast and multicast MAC address features and the procedures for configuring them. This chapter includes the following sections:

Note

To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Overview

The AT-GS950/16 switch has a MAC address table with a storage capacity of up to 8,000 entries. The table stores the MAC addresses of the network nodes connected to its ports and the port number where each address is learned. There are two types of MAC addresses, dynamic and static.

Dynamic MAC addresses are addresses that the switch learns automatically by examining the source MAC addresses of the frames received by the ports. This type of MAC address is not stored indefinitely in the MAC address table. The switch deletes a dynamic MAC address from the table if it does not receive any frames from the node after a specified period of time. The switch assumes that the node is no longer active and that its MAC address can be purged from the table. This prevents the MAC address table from becoming filled with addresses of nodes that are no longer active.

The MAC address table can also store a *static MAC address* which is a MAC address of an end node that you assign to a switch port manually. A static MAC address remains in the table indefinitely and is never deleted by the switch, even when the end node is inactive. You can only delete a static MAC address by manually configuring the switch with the AT-S114 Management Software.

There are two reasons to enter static MAC addresses. You may want to enter end nodes the switch does not learn in its normal dynamic learning process. Or, you want a MAC address to remain permanently in the table, even when the end node is inactive.

Static multicast addresses are a subset of the static MAC addresses. With the Static Multicast Address feature, you can add static multicast addresses to the MAC address table. You can then assign the static MAC address to a port or ports which are called Group Members in the AT-S114 interface. Each port has a maximum limit of 256 static multicast addresses.

In some network environments that are confined to one LAN (such as an industrial application with a server, a switch and many controllers), there may be various multicast streams that need to be distributed to some network nodes, but not others. If the data sent in these streams are time-sensitive and cannot be delayed because of the configuration time associated with the IGMP Snooping feature, then static multicast addresses may be the solution.

If a multicast address and its associated ports of the switch are predefined within the network design and they will not change over time, then they can be manually entered as static entries into the MAC address table. This allows the multicast stream to be forwarded immediately to those predefined ports entered in the MAC table without any configuration delays or loss of data.

Static Unicast MAC Address Configuration

This procedure explains how to set the static unicast feature for each port on the AT-GS950/16 switch. Before beginning this procedure, you must create either an 802.1Q VLAN ID or a Port-Based VLAN Index. For information about defining these parameters, see:

❒ "Tagged VLAN Configuration" on page 166 regarding the **802.1Q VLAN** parameter.

❒ "Port-Based VLAN Configuration" on page 173 regarding the **Port-Based VLAN** parameter.

To add a static MAC address to the switch, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.
   The **Bridge** folder expands.

2. From the **Bridge** folder, select **Static Unicast.**
   The Static Unicast Address Table Page is displayed. See Figure 43.

Figure 43. AT-GS950/16 Static Unicast Address Table Page

3. Select either the **802.1Q VLAN** or **Port-Based VLAN** radio button and enter the respective VLAN ID (1-4093) or VLAN Index (1 - 52).

Note

An error message is generated when you enter a VLAN ID or VLAN Index which has not been defined, or when you enter a VLAN ID or VLAN Index without also clicking on the respective radio button.

---

4. In the **MAC Address** field, enter a unicast MAC address.

5. Assign the MAC address a **Port Member** by selecting the radio button beside the port number.

Note

You can assign a maximum limit of 256 static unicast addresses on the switch.

---

6. Click **Apply**.
    The Static Unicast Address Table is updated and displayed with the new MAC Address.
    See Figure 44 for an example of a Port-based VLAN.

Figure 44. Static Unicast Address Table with Port-Based VLAN Example

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Modify Static Unicast Address

To modify the port assignment of a unicast MAC address in the MAC address table, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.

2. From the **Bridge** folder, select **Static Unicast**.
   The Static Unicast Address Table Page is displayed. See Figure 43 on page 132.

3. Select **Modify** next to the static unicast MAC address that you want to change.
   The Modify Static Unicast Address Page is displayed. See Figure 45.

Figure 45. Modify Static Unicast Address Page

4. In the **Port Member** row, click the radio button for the port that you want to include or remove in the **Port Member** area. The selected port is indicated with an active radio button.

   Note

   To restore the original group member ports, click **Restore**.

5. Click **Apply**.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Delete Static Unicast Address

To delete a unicast MAC address from the MAC address table, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.

2. From the **Bridge** folder, select **Static Unicast**.
    The Static Unicast Address Table Page is displayed. See Figure 43 on page 132.

3. Select **Delete** next to the static unicast address that you want to remove.
    The static unicast address is removed from the Static Unicast Address Table Page.
    To delete all 802.1q address entries, click the **Delete All** button above the 802.1Q VLAN table.
    To delete all port-based VLAN address entries, click the **Delete All** button above Port-Based VLAN table.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Static Multicast Address Configuration

This procedure explains how to set the static multicast feature for each port on the AT-GS950/16 switch. Before beginning this procedure, you must create an 802.1Q VLAN ID or a Port-Based VLAN Index. For information about defining these parameters, see:

❑ "Tagged VLAN Configuration" on page 166 regarding the **802.1Q VLAN** parameter.

❑ "Port-Based VLAN Configuration" on page 173 regarding the **Port-Based VLAN** parameter.

To add a static multicast MAC address to the switch, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.
    The **Bridge** folder expands.

2. From the **Bridge** folder, select **Static Multicast**.
    The Static Multicast Address Table Page is displayed.
    See Figure 46.

Figure 46. Static Multicast Address Table Page

3. Select either the **802.1Q VLAN** or **Port-Based VLAN** radio button and enter the respective VLAN ID (1-4093) or VLAN Index (1 - 52).

Note

An error message is generated when you enter a VLAN ID or VLAN Index which has not been defined, or when you enter a VLAN ID or VLAN Index without also clicking on the respective radio button.

4. In the **Group MAC Address** field, enter a multicast MAC address. The range is from 01:00:5E:00:01:00 to 01:00:5E:7F:FF:FF.

5. Assign the MAC address a **Group Member** (or members) by selecting the check box beside each port number.

   To select all ports, click the **All** button under **Group Member**.

Note

You can assign a maximum limit of 256 static multicast addresses on the switch.

6. Click **Add**.
   The Static Multicast Address Table is updated with the new MAC Address See Figure 47 for a partial view of this page.

Figure 47. Static Multicast Address Table Example

Note

The **Group MAC Address** values that you enter on the Static Multicast Address Table Page are also displayed on the IGMP Snooping Page. For more information, see "IGMP Snooping Configuration" on page 144.

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Modify Static Multicast Address

To modify the port assignment of a multicast MAC address in the MAC address table, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.

2. From the **Bridge** folder, select **Static Multicast**.
   The Static Multicast Address Table Page is displayed. See Figure 46 on page 136.

3. Select **Modify** next to the static MAC address that you want to change.
   The Modify Static Multicast Address Page is displayed. See Figure 48.

Figure 48. Modify Static Multicast Address Page

4. In the **Group Member** row, select the check boxes for the ports that you want to include or remove in the Group Member area. Selected ports are indicated with a check mark.

   To select all ports, click the **All** button under **Group Member**.

   > **Note**
   > To restore the original group member ports, click **Restore**.

5. Click **Apply**.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Delete Static Multicast Address

To delete a multicast MAC address from the MAC address table, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.

2. From the **Bridge** folder, select **Static Multicast**.
    The Static Multicast Address Table Page is displayed. See Figure 47 on page 137.

3. Select **Delete** next to the static multicast address that you want to remove.
    The static multicast address is removed from the Static Multicast Address Table Page.
    To delete all 802.1q address entries, click the **Delete All** button above the 802.1Q VLAN table.
    To delete all port-based VLAN address entries, click the **Delete All** button above Port-Based VLAN table.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Chapter 11
IGMP Snooping

This chapter contains a description of the IGMP Snooping feature, as well as procedures for working with IGMP Snooping in the web interface. The following topics are discussed:

❐ "Overview" on page 142
❐ "IGMP Snooping Configuration" on page 144
❐ "IGMP Snooping Router Port Modification" on page 147

Note

To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Overview

IGMP enables IPv4 routers to create lists of nodes that are members of multicast groups. (A group of end nodes that receive multicast packets from a multicast application is defined as a multicast group.) The router creates a multicast membership list by periodically sending out queries to the local area networks connected to its ports.

A node that wants to become a member of a multicast group responds to a query by sending a *report* which indicates an end node's desire to become a member of a multicast group. Nodes that join a multicast group are referred to as *host nodes*. After becoming a member of a multicast group, a host node must continually issue reports on a continuous basis to remain a member.

After the router has received a report from a host node, it notes the multicast group that the host node wants to join and the port on the router where the node is located. Any multicast packets belonging to that multicast group are then forwarded by the router out the port. If a particular port on the router has no nodes that want to be members of multicast groups, the router does not send multicast packets from the port. This improves network performance by restricting multicast packets only to router ports where host nodes are located.

There are three versions of IGMP— versions 1, 2, and 3. One of the differences between the versions is how a host node signals that it no longer wants to be a member of a multicast group. In version 1, it stops sending reports. If a router does not receive a report from a host node after a predefined length of time, referred to as a *time-out value*, it assumes that the host node no longer wants to receive multicast frames and removes it from the membership list of the multicast group.

In version 2, a host node exits from a multicast group by sending a *leave request*. After receiving a leave request from a host node, the router removes the node from appropriate membership list. The router also stops sending multicast packets from the port if it determines there are no further host nodes on the port.

Version 3 adds the ability of host nodes to join or leave specific sources in a multicast group.

The IGMP snooping feature on the AT-GS950/16 switch supports IGMP versions 1 and 2. The switch monitors the flow of queries from a router and checks report and leave messages from host nodes to build its own multicast membership lists. It uses the lists to forward multicast packets only to its own ports where there are host nodes that are members of multicast groups. This improves switch performance and network security by restricting the flow of multicast packets only to those ports connected to host nodes.

Without IGMP snooping, a switch floods multicast packets from all of its ports, except the port on which it received the packet. Such flooding of packets can negatively impact network performance.

The AT-GS950/16 switch maintains a list of multicast groups through an adjustable time-out value, which controls how frequently it expects to see reports from end nodes that want to remain members of multicast groups, and by processing leave requests.

Note

By default, IGMP snooping is disabled on the switch.

IGMP Snooping Configuration

This procedure explains how to set IGMP snooping and IGMP Snooping Querier on the switch, and set the IGMP Snooping (V1) age-out timer.

To configure IGMP snooping, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.
    The **Bridge** folder expands.

2. From the **Bridge** folder, select the **IGMP Snooping** folder.

3. From the **IGMP Snooping** folder**,** select **IGMP Snooping Settings**.
    The IGMP Snooping Settings Page is displayed. See Figure 49.

Figure 49. IGMP Snooping Settings Page

4. To enable or disable IGMP Snooping on the switch, select **Enabled** or **Disabled** from the pull-down menu next to **Status**.

5. To set the **Age-Out Timer**, type the number of seconds you want the switch to wait before it purges an inactive dynamic MAC address.

   The range of this parameter is from 280 to 420 seconds.

6. To enable the IGMP Snooping Querier, select **Enabled** from the pull-down menu next to **Querier Status**.
   If you want to disable the IGMP Snooping Querier, select **Disabled**.

7. To set the IGMP Snooping **Query Interval**, set the timer from 60 to 600 seconds.

8. To set the **Max. Response Time** for query messages, set the timer from 10 to 25 seconds.

9. To set the robustness value for the VLANs, set the **Robustness Variable** from 2 to 255. The robustness variable is an integer used during IGMP snooping calculations for IGMP messages to allow for expected packet loss.

10. To set the **Last Member Query Interval**, type the number of seconds you want the switch to wait before it removes the group from the associated VLAN port if no hosts respond to an IGMP query message.

    The range of this parameter is from 1 to 25 seconds.

11. To set the aging time of the router port, set the **Router Timeout** parameter from 120 to 12000 seconds.

12. Click **Apply**.

13. The IGMP Snooping Page is updated with active Multicast Group addresses. See Figure 50 on page 146.

    Note

    The **Multicast Group Address** table contains MAC addresses of nodes that are active members of multicast groups. To set a static Multicast Group Address, see "Static Multicast Address Configuration" on page 136.

Figure 50. IGMP Snooping Page with MAC Address

14. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

IGMP Snooping Router Port Modification

This procedure explains how to modify the IGMP snooping router port.

To modify the IGMP snooping router port, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.
   The **Bridge** folder expands.

2. From the **Bridge** folder, select the **IGMP Snooping** folder.

3. From the **IGMP Snooping** folder, select **IGMP Snooping Router Port**.
   The IGMP Snooping Router Port Page is displayed. See Figure 51.

Figure 51. IGMP Snooping Router Port Page

4. Select **Modify** under the Action column for the entry you want to modify.
   The **Modify IGS Static Router Port** page is displayed. See Figure 52.

Figure 52. Modify IGS Static Router Port Page

5. In the **Static Router Port** row, select the check boxes for the ports that you want to include or remove in the Static Router Port area. Selected ports are indicated with a check mark.

   To select all ports, click the **All** button under **Static Router Port**.

   Note
   To restore the original group member ports, click **Restore**.

   ---

6. Click **Apply**.

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Chapter 12
Storm Control

This chapter contains a description and configuration procedures for the Storm Control (bandwidth) feature. The following topics are discussed:

> **Note**
> To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Overview

The features available in the AT-S114 Management Software allow you to limit Ethernet traffic within your switch based on specific criteria. You can use Storm Control to limit the bandwidth of various types of Ethernet packets. With Ingress and Egress Rate Limiting, you can limit the traffic volume at the input or output ports respectively.

The Storm Control feature allows you regulate the reception rate of broadcast, multicast, and destination lookup failure (DLF) packets. The AT-S114 Management Software allows you to set separate limits for each port beyond which each of the different packet types are discarded. Each setting can be configured on individual ports or on all of the ports of the AT-GS950/16 switch. Traffic is measured in packets per second. See the following definitions for more information about these settings.

Destination Lookup Failure - The Destination Lookup Failure (DLF) setting is concerned with comparing the destination MAC address of a packet received by the switch to the forwarding database. When the AT-GS950/16 switch receives a packet, it scans the forwarding database and looks for a match to the destination MAC address in the received packet. If the MAC address is not present, then the packet is flooded according to the VLAN rules. By default, this setting is disabled on the switch which means that all DLF packets are automatically forwarded according to the VLAN rules.

Broadcast Setting - The broadcast setting applies to allowing or denying broadcast packets on each port.

Multicast Setting - The multicast setting applies to allowing or denying multicast packets on each port.

Threshold Level - In regards to Bandwidth control, the threshold level is the number of DLF, broadcast, and multicast packets that are sent by or received from a port. This value is measured in packets per second. You can set the threshold level from 1 to 22194 packets per second.

Note

The packet sizes affected by this threshold level can vary in size from 64 Bytes to 1024 Bytes.

Ingress Rate Limiting   The Ingress Rate Limiting feature restricts the traffic to a pre-configured data rate that can flow into a port. This data rate limit can be configured in 64 Kbps increments within a range from 64 Kbps to 1000 Mbps. The formula for calculating the bandwidth limit is as follows:

Bandwidth = 64Kbps x rate limit

The rate limit parameter is an integer ranging from 1 to 15625.

Egress Rate Limiting   The Egress Rate Limiting feature restricts the traffic to a pre-configured data rate that can flow out of a port. This data rate limit can be configured in 64 Kbps increments within a range from 64 Kbps to 1000 Mbps. The formula for calculating the bandwidth limit for the 10/100/1000Base-T ports is as follows:

Bandwidth = 64Kbps x rate limit

The rate limit parameter is an integer ranging from 1 to 15625.

Configuration

This procedure explains how to set DLF, broadcast, multicast, and threshold levels for each port on the AT-GS950/16 switch.

To change the settings of the storm control feature, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.

2. From the **Bridge** folder, select **Bandwidth Control**.
   The **Bandwidth Control** folder expands.

3. From the **Bandwidth Control** folder, select **Storm Control**.
   The AT-GS950/16 Storm Control page is displayed. See Figure 53 for a partial view of this page.

Figure 53. AT-GS950/16 Storm Control Page

4. To enable or disable the **DLF** field, select **Enable** or **Disable** from the **DLF** pull-down menu next to the port that you want to change.
   You can select the **All** row to set all of the ports to the same setting.
   The **Ignore** parameter indicates that the setting in the **All** row does not apply to the **DLF** menu for individual ports. In other words, each port is set individually.

   Note

   For more information about the Destination Lookup Failure (**DLF**) setting, see "Overview" on page 150.

5. Click **Apply**.

6. To enable or disable ingress and egress **Broadcast** packets, select **Enable** or **Disable** from the **Broadcast** pull-down menu next to the port that you want to change.
   You can select the **All** row to set all of the ports to the same setting. The **Ignore** parameter indicates that the setting in the **All** row does not apply to the **Broadcast** menu for individual ports.

   Note

   For more information, refer to the **Broadcast** setting definition in "Overview" on page 150.

7. Click **Apply**.

8. To enable or disable ingress and egress **Multicast** packets, select **Enable** or **Disable** from the **Multicast** pull-down menu next to the port that you want to change.
   You can select the **All** row to set all of the ports to the same setting. The **Ignore** parameter indicates that the setting in the **All** row does not apply to the **Multicast** menu for individual ports.

   Note

   For more information, see the **Multicast** setting definition in "Overview" on page 150.

9. Click **Apply**.

10. To set the **Threshold** field, type in the threshold next to the port that you want to change. The range is from 1 to 22194 packets per second.
    You can select the **All** row to set all of the ports to the same setting. The **Ignore** parameter indicates that the setting in the **All** row does not apply to the **Threshold** menu for individual ports.

    Note

    For more information, see the **Threshold** setting definition in "Overview" on page 150.

11. Click **Apply**.

12. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Ingress Rate Limiting

This procedure explains how to set **Bandwidth** levels and **Status** for Ingress Rate Limiting on each port of the AT-GS950/16 switch.

To change the settings of the ingress rate limiting feature, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.

2. From the **Bridge** folder, select **Bandwidth Control**.
   The **Bandwidth Control** folder expands.

3. From the **Bandwidth Control** folder, select **Ingress Rate Limiting**.
   The AT-GS950/16 Ingress Rate Limiting page is displayed. See Figure 54 for a partial view of this page.

Ingress Rate Limiting

Bandwidth = 64kbps x rate limit

Port	Bandwidth		Status	Action
All	64kbps x [ ]	(1-15625)	Ignore	Apply
1	64kbps x 15625	(1-15625)	Disabled	Apply
2	64kbps x 15625	(1-15625)	Disabled	Apply
3	64kbps x 15625	(1-15625)	Disabled	Apply
4	64kbps x 15625	(1-15625)	Disabled	Apply
5	64kbps x 15625	(1-15625)	Disabled	Apply
6	64kbps x 15625	(1-15625)	Disabled	Apply
7	64kbps x 15625	(1-15625)	Disabled	Apply
8	64kbps x 15625	(1-15625)	Disabled	Apply

Figure 54. AT-GS950/16 Ingress Rate Limiting Page

4. To set the **Bandwidth** field on the AT-GS950/16 switch, enter a number in the range from 1 to 15625.

Note
Refer to "Ingress Rate Limiting" on page 151 for calculating the bandwidth limit set by the **Bandwidth** field.

You can select the **All** row to set all of the ports to the same setting.

5. To enable or disable the ingress rate filter, select **Enable** or **Disable** from the **Status** pull-down menu next to the port that you want to change. You can select the **All** row to set all of the ports to the same setting.
The **Ignore** parameter indicates that the setting in the **All** row does not apply to the **Status** menu for individual ports.

6. Click **Apply**.

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Egress Rate Limiting

This procedure explains how to set **Bandwidth** levels and **Status** for Egress Rate Limiting on each port of the AT-GS950/16 switch.

To change the settings of the egress rate limiting feature, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.

2. From the **Bridge** folder, select **Bandwidth Control**.
   The **Bandwidth Control** folder expands.

3. From the **Bandwidth Control** folder, select **Egress Rate Limiting**.
   The AT-GS950/16 Egress Rate Limiting page is displayed. See Figure 55 for a partial view of this page.

Egress Rate Limiting

Bandwidth = 64kbps x rate limit

Port	Bandwidth		Status	Action
All	64kbps x	(1-15625)	Ignore ▼	Apply
1	64kbps x 0	(1-15625)	Disable ▼	Apply
2	64kbps x 0	(1-15625)	Disable ▼	Apply
3	64kbps x 0	(1-15625)	Disable ▼	Apply
4	64kbps x 0	(1-15625)	Disable ▼	Apply
5	64kbps x 0	(1-15625)	Disable ▼	Apply
6	64kbps x 0	(1-15625)	Disable ▼	Apply
7	64kbps x 0	(1-15625)	Disable ▼	Apply
8	64kbps x 0	(1-15625)	Disable ▼	Apply

Notes: Disable will reset the setting to default value then turn off the function.

Figure 55. AT-GS950/16 Egress Rate Limiting Page

To set the **Bandwidth** field, enter a number in the range of 1 to 15625. You can select the **All** row to set all of the ports to the same setting.

> **Note**
> See "Egress Rate Limiting" on page 151 for calculating the bandwidth limit set by the **Bandwidth** field.

4. To enable or disable the egress rate filter, select **Enable** or **Disable** from the **Status** pull-down menu next to the port that you want to change. You can select the **All** row to set all of the ports to the same setting.
   The **Ignore** parameter indicates that the setting in the **All** row does not apply to the **Status** menu for individual ports.

5. Click **Apply**.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Chapter 13
Virtual LANs

This chapter contains a description of Virtual Local Area Networks (VLANs) and the procedures for creating, modifying, and deleting both port-based and tagged VLANs. It also describes setting the mode of the MAC address forwarding table, viewing the dynamic forwarding table, configuring private VLANs, and viewing the current VLAN database.

This chapter contains the following sections:

Note

The Voice VLAN feature is not covered in this section. For more information, see "Voice VLAN" on page 269.

Note

To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

VLAN Overview

A virtual LAN (VLAN) is a group of ports on an Ethernet switch that form a logical Ethernet segment via the AT-S114 Management software. The ports of a VLAN form an independent traffic domain where the traffic generated by the nodes of a VLAN remains within the VLAN.

With VLANs, you can segment your local area network using the AT-S114's Management software and group nodes with related functions into their own separate, logical, VLAN segments. These VLAN groupings can be based on similar data needs or security requirements. For example, you can create separate VLANs for each department in your company, such as Sales, Accounting and Engineering.

VLANs offer several important benefits:

■ Improved network performance

Network performance often suffers as networks grow in size and as data traffic increases. The more nodes on each LAN segment vying for bandwidth, the greater the likelihood overall network performance decreases.

VLANs improve network performance because traffic stays within the separate, logical LAN segment of the VLAN. The nodes of a VLAN receive traffic only from nodes of the same VLAN. This reduces the need for nodes to handle traffic that is not destined for them. It also frees up bandwidth within all the logical workgroups.

In addition, because each VLAN constitutes a separate broadcast domain, broadcast traffic remains within the VLAN and is not shared with other ports of the switch that are not members of that VLAN. Because the broadcast traffic is not shared with ports outside of the VLAN, those non-member ports experience an overall network performance improvement.

■ Increased security

Because data traffic generated by a node in a VLAN is restricted only to the other nodes of the same VLAN, you can use VLANs to control the flow of packets in your network and prevent packets from being shared with unauthorized end nodes.

■ Simplified network management

VLANs can simplify network management. Before VLANs became a layer 2 feature, physical changes to the network often had to been made at the switches in the wiring closets. For example, if an employee changed departments, changing the employee's LAN segment assignment might require a change to the cabling of the switches.

With VLANS, you can reconfigure the LAN segment assignment of an end node connected to the AT-GS950/16 switch's management software. Also, you can change the VLAN memberships without moving the workstations physically or change group memberships without moving cables from one port to another.

In addition, a virtual LAN can span more than one switch. This means that the end nodes of a VLAN do not need to be connected to the same switch, so they are not restricted to being in the same physical location.

The AT-GS950/16 Gigabit Ethernet Smart Switch supports the following types of VLANs:

■   Port-based VLANs

■   Tagged VLANs

■   Private VLANs

These types of VLANs are described in the following sections.

Port-based VLAN Overview

As explained in the "VLAN Overview" on page 158, a VLAN consists of a group of ports on an Ethernet switch that form an independent traffic domain. This type of VLAN is independent of the header information including VLAN tags in a frame. Traffic generated by the end nodes of a VLAN remains within the VLAN and does not cross over to the end nodes of other VLANs unless there is an interconnection device, such as a router or Layer 3 switch.

A port-based VLAN is a group of ports on the switch that form a logical Ethernet segment. A port-based VLAN can have as many or as few ports as needed. The VLAN can consist of all ports on an Ethernet switch, or just a few ports.

There are two components of a port-based VLAN in the AT-S114 Management software:

■   VLAN Name

■   VLAN Index

VLAN Name

To create a port-based VLAN, you must give it a unique name. This name can reflect the function of the network devices that are VLAN members, such as Sales, Production, and Engineering.

VLAN Index

You must assign a unique number to each VLAN in a network. This number is called the Port-Based VLAN Index. This number uniquely identifies a VLAN in the AT-GS950/16 switch and across the network.

Each port of a port-based VLAN can belong to as many VLANs as needed. Therefore, traffic can be forwarded to the members of the groups to which the port is assigned. For example, port 1 and port 2 are members of group 1, and ports 1 and 3 are members of group 2. In this case, traffic from port 1 is forwarded to ports 2 and 3, traffic from port 2 is forwarded only to port 1, and traffic from port 3 is forwarded only to port 1.

General Rules for Creating a Port-based VLAN

Here is a summary of general rules to observe when creating a port-based VLAN:

- Assign a unique name to each port-based VLAN.
- Assign a unique VLAN Index to each port-based VLAN. If a particular port-based VLAN spans multiple switches, each part of the VLAN on the different switches must be assigned the same VLAN index.
- Create up to 52 port-based VLANs.

Tagged VLAN Overview

The second type of VLAN supported by the AT-S114 Management software is the *tagged VLAN*. In this type of VLAN, membership is determined by tag information within the frames that are received on a port and the VLAN configuration of each port.

The VLAN information within an Ethernet frame is referred to as a *tag* and is contained in a *tagged header* for the frame. A tag, which follows the source and destination addresses in a frame, contains the VLAN ID of the VLAN to which the frame belongs (IEEE 802.3ac standard). This number uniquely identifies each VLAN in a network.

When a switch receives a frame with a VLAN tag, referred to as a *tagged frame*, the switch forwards the frame only to those ports whose VLAN ID equals the VLAN tag.

A port that receives or transmits tagged frames is referred to as a *tagged port*. Any network device connected to a tagged port must be IEEE 802.1Q compliant. This is the standard that outlines the requirements and standards for VLAN tagging. The device must be able to process the tagged information on received frames and add tagged information to transmitted frames.

A tagged VLAN consists of the following:

❑ "VLAN Index"

❑ "VLAN Name"

❑ "Tagged and Untagged Ports"

❑ "Port VLAN Identifier (PVID)" on page 162

❑ "General Rules for Creating a Tagged VLAN" on page 162

VLAN Index

You must assign a unique number to each tagged VLAN in a network. This number is called the tagged VLAN ID. This number uniquely identifies a tagged VLAN in the AT-GS950/16 switch and across the network.

VLAN Name

To create a tagged VLAN, you must give it a unique name. This name can reflect the function of the network devices that are VLAN members, such as Sales, Production, and Engineering.

Tagged and Untagged Ports

When you specify that a port is a member of a tagged VLAN, you need to specify that it is tagged or untagged. By definition, the port is a static member of a tagged VLAN when it is configured as either a tagged or untagged port. You can have a combination of tagged and untagged ports in the same VLAN.

Note

A port can also be dynamically assigned to a tagged VLAN within a voice VLAN configuration which is a special configuration of a tagged VLAN. For more information concerning static and dynamic membership in a tagged VLAN, see "Overview" on page 270 in the "Voice VLAN" chapter.

Packet transmission from a tagged port differs from packet transmission from an untagged port. When a packet is transmitted from a tagged port, the tagged information within the packet is maintained when it is transmitted to the next network device. If the packet is transmitted from an untagged port, the VLAN tag information is removed from the packet before it is transmitted to the next network device.

The IEEE 802.1Q standard describes how tagging information within a packet is used to forward or discard traffic throughout the switch. If the incoming packet has a VLAN tag that matches one of the Group IDs of which the port is a member, the packet is accepted and forwarded to the appropriate port(s) within that VLAN. If the incoming packet's VLAN tag

does not match one of the Group IDs assigned to the port, the packet is discarded.

Port VLAN Identifier (PVID)

When an untagged packet is received on a port in a tagged VLAN, it is assigned to one of the VLANs of which that port is a member. The deciding factor in this process is the Port VLAN Identifier (PVID). Both tagged and untagged ports in a tagged VLAN must have a PVID assigned to them. The default value of the PVID for each port is 1. The switch associates a received untagged packet to the VLAN ID that matches the PVID assigned to the port, and the packet is only forwarded to those ports that are members.

General Rules for Creating a Tagged VLAN

Here is a summary of the rules to observe when you create a tagged VLAN:

- Assign a unique name to each tagged VLAN.
- Each tagged VLAN must be assigned a unique VLAN ID. If a particular VLAN spans multiple switches, each part of the VLAN on the different switches must be assigned the same VLAN ID.
- A tagged port can be a member of multiple VLANs.
- The AT-GS950/16 Gigabit Ethernet Switch can support up to 255 tagged VLANs per switch.

Private VLAN Overview

Private VLANs create special broadcast domains in which the traffic of the member ports is restricted to source ports. Ports in a private port VLAN are only allowed to forward traffic to, and receive traffic from, a designated source port, and are prohibited from forwarding traffic to each other.

An example application of a private port VLAN would be a library in which user booths each have a computer with Internet access. In this situation, it would usually be undesirable to allow communication between these individual PCs. Connecting the computers to ports within a private isolated VLAN would enable each computer to access the Internet or a library server via a single connection, while preventing access between the computers in the booths.

Another application for private port VLANs is to simplify IP address assignments. Ports can be isolated from each other while still belonging to the same subnet.

A private port VLAN consists of one or more forwarding ports and a source port.

Forwarding Ports

Forwarding ports of a private port VLAN can only forward traffic to, and receive traffic from, a source port, and are prohibited from forwarding traffic to each other. A private port VLAN can have any number of forwarding ports on the switch, up to all the ports, minus the source port. Forwarding ports cannot be members of static port trunks or LACP trunks. A port can be a forwarding port of only one private port VLAN at a time.

Forwarding ports are untagged. VLAN membership is defined by their PVIDs, which are equivalent to the ID of the VLANs. The devices to which they are connected should not send tagged packets.

Source Port

The source port can communicate with all of the forwarding ports in its VLAN. A private port VLAN can have only one source port, but it can be any port on the switch. A port can be a source port of just one private port VLAN at a time. The source port cannot be a static port trunk or an LACP trunk.

The source port is untagged. It does not include tagged VLAN information in the packets that it forwards to forwarding ports or the device to which it is connected. Thus, its network counterpart should not send tagged packets.

General Rules for Creating a Private VLAN

Here is a summary of general rules to observe when creating private port VLANs:

- A private port VLAN can have any number of forwarding ports, up to all the ports on the switch, minus the source port.
- A private port VLAN can have only one source port.
- The forwarding and source ports of private port VLANs are untagged ports, and as such, transmit only untagged traffic.
- The switch can support private, port-based, tagged, and MAC address-based VLANs simultaneously.
- The forwarding ports and the source port of a private port VLAN cannot belong to static port trunks or LACP trunks.
- Ports can be forwarding or source ports of only one private port VLAN simultaneously.
- Ports cannot be members of both private port VLANs and port-based or tagged VLANs simultaneously.

Assign Ports to a VLAN Mode

The procedure described in this section allows you to assign ports to tagged or a port-based VLAN. In addition, it permits you to display the current VLAN assignment of ports.

However, you can assign ports to a port-based VLAN only after you have created a port-based VLAN with the procedure described in "Port-Based VLAN Configuration" on page 173.

By default, all of the ports on the switch are assigned as untagged members to the default tagged VLAN with a VLAN ID of 1. The default VLAN is permanent and must have at least one untagged port assigned to it at any time.

To assign ports to an 802.1Q Tagged VLAN or port-based VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**.
    The **Bridge** folder expands.

2. From the **Bridge** folder, select **VLAN**.
    The **VLAN** folder expands.

3. From the **VLAN** folder, select **VLAN Mode**.
    The VLAN Mode Page is displayed. See Figure 56.
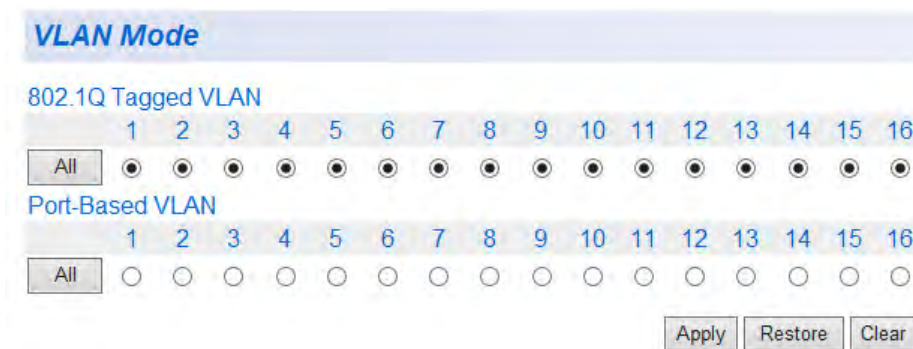
Figure 56. AT-GS950/16 VLAN Mode Page

4. To add ports to an **802.1Q Tagged VLAN** or **Port-Based VLAN**, select the ports accordingly on the VLAN Mode Page.
    To add all ports to an **802.1Q Tagged VLAN** or **Port-Based VLAN**, click the **All** button.

Note

Before you assign a port as a member of a port-based VLAN, you must create the port-based VLAN by following the steps defined in "Port-Based VLAN Configuration" on page 173.

5. Click **Apply**.

6. If you want to restore the port assignment before saving the configuration, click **Restore**.

Note

Once the VLAN assignment has been saved by clicking first on the **Apply** button and then saving the configuration, the **Restore** button will not be active for those port assignments.

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Tagged VLAN Configuration

On a port, the tag information within a frame is examined when it is received to determine if the frame is qualified as a member of a specific tagged VLAN. If it is, it is eligible to be switched to other member ports of the same VLAN. If it is determined that the frame's tag does not conform to the tagged VLAN, the frame is discarded.

You can create and delete tagged VLANs by following the procedures in the following sections:

❐ "Create a Tagged VLAN"

❐ "Modify a Tagged VLAN" on page 168

❐ "Delete a Tagged VLAN" on page 170

Create a Tagged VLAN

To create a tagged VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select **VLAN**. The **VLAN** folder expands.

3. From the **VLAN** folder, select **Tagged VLAN**. The AT-GS950/16 Tagged VLAN Page is displayed. See Figure 57.

Figure 57. AT-GS950/16 Tagged VLAN Page

4. Assign a VLAN ID by entering a VLAN ID in the **VLAN ID** field.
The range for this field is 2 to 4,093. You can create a maximum of 255 tagged VLANs.

5. Assign a name for the VLAN by entering a unique name in the **VLAN Name** field.
You can enter a value of up to 32 characters. For more information about this field, refer to "VLAN Name" on page 159.

6. Set the **Management VLAN** to one of the following choices from the pull-down menu:

> **Enabled** - This parameter enables management access on this VLAN.

> **Note**
>
> - If you enable management on a VLAN other than 1, you can access management only through a tagged port of that VLAN.
> - You can access management through the tagged port of all VLANs on which you have enabled management.
> - You can still access management through a port that is only an untagged member of VLAN 1 and not a tagged member of another VLAN.

> **Disabled** - This parameter disables **Management VLAN** on this VLAN. If you change this parameter from **Enable** to **Disable**, the **Management VLAN** is still enabled on the **DefaultVLAN**.

> **Note**
>
> The Management VLAN is always Enabled on the untagged ports of the DefaultVLAN. It cannot be disabled on the DefaultVLAN.

7. To assign ports to the VLAN, click on the port numbers labeled either **Static Tagged** or **Static Untagged**.
To assign all ports to the VLAN as **Static Tagged**, click **All** under **Static Tagged**.
To assign all ports to the VLAN as **Static Untagged**, click **All** under **Static Untagged**.
By default, all the ports are assigned to the **Not Member** category when a specific VLAN is created. The **Not Member** ports are either part of the DefaultVLAN (VLAN ID=1) or another VLAN.

8. Click **Apply**.

9. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Modify a Tagged VLAN

To modify the name or port assignments of a tagged VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**.
   The **Bridge** folder expands.

2. From the **Bridge** folder, select **VLAN**.
   The **VLAN** folder expands.

3. From the **VLAN** folder, select **Tagged VLAN**.
   An example of a tagged VLAN is shown in the table at the bottom of Figure 58.

Figure 58. Example of AT-GS950/16 Tagged VLAN Page

4. In the **VLAN Action** column, click **Modify** in the row of the VLAN that you want to change.
   The Modify VLAN Page is displayed. See Figure 59 on page 169.

Figure 59. AT-GS950/16 Modify VLAN Page

5. You cannot modify the VLAN ID on this web page. If you want to delete the VLAN ID, go to "Delete a Tagged VLAN" on page 170 for more information.

6. To change the VLAN Name, type a new VLAN Name in the **VLAN Name** field.
    For more information about this field, refer to "VLAN Name" on page 159.

7. To allow management access on this VLAN, select one of the following choices from the pull-down menu:

    Enable: This parameter enables **Management VLAN** on this VLAN.

⚠️ **Caution**

If you Disable the Management VLAN on a newly assigned VLAN, and you are connected to a **Member** port, you may lose your connection to the AT-S114 Management software. To restore the connection, change the connection of your PC to an appropriate port or re-boot the switch.

    Disable - This parameter disables **Management VLAN** on this VLAN. If you change this parameter from **Enable** to **Disable**, the **Management VLAN** will be enabled on the **DefaultVLAN** automatically.

Note

The Management VLAN is always Enabled on the DefaultVLAN and cannot be disabled.

---

8. To change the port selections, click on the port numbers labeled either **Static Tagged** or **Static Untagged**. You can also use the **All** button to select all ports as **Static Tagged** or **Static Untagged**.

9. Click **Apply**.

10. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Delete a Tagged VLAN

To delete a tagged VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**.
    The **Bridge** folder expands.

2. From the **Bridge** folder, select **VLAN**.
    The **VLAN** folder expands.

3. From the **VLAN** folder, select **Tagged VLAN**.
    An example of the Tagged VLAN Page is shown in Figure 58 on page 168.

4. In the VLAN Action column, click **Delete** next to the VLAN that you want to delete.
    A confirmation prompt is displayed.

5. Click **OK** to delete the VLAN or **Cancel** to cancel the deletion.

Note

You cannot delete the Default VLAN which has a VID of 1.

---

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Tagged VLAN Port Settings

To configure a VLAN port that is a member of a Tagged VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select **VLAN**. The **VLAN** folder expands.

3. From the **VLAN** folder, select **Port Settings**. The AT-GS950/16 VLAN Port Settings Page is displayed. See Figure 60 for a partial view of this page.

Port	PVID	Acceptable Frame Types	Ingress Filtering	Action
All		Ignore	Ignore	Apply
1	1	All	Enabled	Apply
2	1	All	Enabled	Apply
3	1	All	Enabled	Apply
4	1	All	Enabled	Apply
5	1	All	Enabled	Apply
6	1	All	Enabled	Apply
7	1	All	Enabled	Apply
8	1	All	Enabled	Apply

Figure 60. AT-GS950/16 VLAN Port Settings Page

4. For a selected port, set the **PVID** field to an existing VLAN ID. For an explanation of the PVID parameter, see "Port VLAN Identifier (PVID)" on page 162**.**

5. Set the **Acceptable Frame Types** to one of the following choices from the pull-down menu:

   All - This selection allows all incoming ingress frames presented to the port to enter the switch.

   Tagged - This selection allows only tagged frames presented to the port to enter the switch. Untagged frames are discarded at ingress.

   Untagged and Priority Tagged - This selection allows only untagged frames and frames with a priority tag that are presented

to the port to enter the switch. Tagged frames are discarded at ingress.

6. For the **Ingress Filtering** parameter, select one of the following choices from the pull-down menu:

> **Enabled** - This enables ingress filtering at the selected port.

> **Disabled** - This disables ingress filtering at the selected port.

7. Click **Apply**.
   The port configuration becomes effective.

8. If you need to configure other ports of the switch for the VLAN Port Settings, repeat Step 4 through Step 7.

9. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Port-Based VLAN Configuration

A port-based VLAN is a group of ports on the switch that form a logical Ethernet segment. This type of VLAN is independent of the header information including VLAN tags in a frame.

You can create and delete port-based VLANs by following the procedures in the following sections:

❑ "Create a Port-Based VLAN"

❑ "Modify a Port-Based VLAN" on page 174

❑ "Delete a Port-Based VLAN" on page 175

Create a Port-Based VLAN

To create a port-based VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select **VLAN**. The **VLAN** folder expands.

3. From the **VLAN** folder, select **Port-Based VLAN**. The Port-Based VLAN Page is displayed. See Figure 61.

Figure 61. Port-Based VLAN Page

4. Assign a VLAN Index by entering a VLAN ID in the **VLAN Index** field. Choose a value between 1 and 52.

5. Assign a name to a VLAN by entering a name in the **VLAN Name** field. You can enter a value of up to 32 characters. For more information about this field, refer to "VLAN Name" on page 159.

6. To assign individual ports to the VLAN, click on the port numbers under **VLAN Member**. To assign all ports to the VLAN, click **All** under **VLAN Member**.

7. Click **Apply**.

8. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Modify a Port-Based VLAN

To modify the name or port assignments of a port-based VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select **VLAN**. The **VLAN** folder expands.

3. From the **VLAN** folder, select **Port-Based VLAN**. An example VLAN is shown in the table at the bottom of the Port-Based VLAN Page. See Figure 62.

Figure 62. Example of AT-GS950/16 Port Based VLAN Page

4. In the VLAN Action column, click **Modify** next to the VLAN that you want to change. The Modify Port-Based VLAN page appears. See Figure 63 on page 175.

Figure 63. Modify Port-Based VLAN Page

5. Modify name or port assignments as needed. You cannot modify the Index number from this page.

6. Click **Apply**.

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Delete a Port-Based VLAN

To delete a port-based VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select **VLAN**. The **VLAN** folder expands.

3. From the **VLAN** folder, select **Port-Based VLAN**. The Port-Based VLAN Page is shown in Figure 62 on page 174.

4. In the VLAN Action column, click **Delete** next to the VLAN that you want to delete.

> **Note**
> You cannot delete the Default VLAN which has a VID of 1.

5. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Select MAC Address Forwarding Table Mode

After you have configured the VLANs on the switch, you can select one of two modes in which the switch learns MAC addresses: Independent VLAN learning (IVL) or Shared VLAN learning (SVL). IVL is the default mode. For more information on IVL and SVL, refer to the IEEE 802.1Q standard.

To select the mode in which the switch learns MAC addresses, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select **VLAN**. The **VLAN** folder expands.

3. From the **VLAN** folder, select **Forwarding Table Mode**. The Forwarding Table Mode Page is shown in Figure 64.

Figure 64. Forwarding Table Mode Page

4. From the **Learning Mode** drop-down menu, select one of the following:

    IVL: Independent MAC address forwarding table for each VLAN is maintained by the switch.

    SVL: One MAC address forwarding table for all VLANs is maintained by the switch.

5. Click **Apply**.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

View Dynamic Forwarding Table

You can view the MAC addresses the switch has stored in the forwarding table. You can view all of the addresses in the table or only the addresses learned on a particular port.

To view the MAC address forwarding table, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select **VLAN**. The **VLAN** folder expands.

3. From the **VLAN** folder, select **Dynamic Forwarding Table**. The Dynamic Forwarding Table Page is shown in Figure 65.

Figure 65. Dynamic Forwarding Table Page

4. To view all MAC addresses, select **All** from the **Port** drop-down menu.

   To view MAC addresses for a particular port, select the port from the **Port** drop-down menu.

   > **Note**
   > Ports without a "p" before the number indicate switch ports. Ports with a "p" before the number indicate port trunks. For example, **02** would indicate switch port 2, and **po2** would indicate port trunk 2.

The Dynamic Forwarding Table Page displays the following:

   ID - ID number of recorded entry in database.

   VID - ID number of the VLAN where the port is a member.

   Port - Port or port trunk where the address was learned by the switch.

MAC Address - MAC address learned by the switch or assigned to the port.

Type - Dynamic or Static:

Dynamic - MAC address the switch learns automatically and is not stored indefinitely in the table.

Static - MAC address assigned manually and remains in the table indefinitely.

VLAN Mode - 802.1Q or Port-Based.

Private VLAN Configuration

You can create, modify, and delete private VLANs by following the procedures in the following sections:

❒ "Enable or Disable Private VLAN"

❒ "Create a Private VLAN" on page 180

❒ "Modify a Private VLAN" on page 181

❒ "Delete a Private VLAN" on page 181

For more information on Private VLANs, refer to "Private VLAN Overview" on page 162.

Enable or Disable Private VLAN

To enable or disable private VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select **VLAN**. The **VLAN** folder expands.

3. From the **VLAN** folder, select **Private VLAN**. The Private VLAN Page is displayed. See Figure 66 for a partial view of this page.

Figure 66. Private VLAN Page

4. Use the **State** radio buttons to select the Private VLAN state:

   Enabled - Will activate Private VLAN. The other parameters on the web page will become active.

   Disabled - Will de-activate Private VLAN. The other parameters on the web page will become inactive and will be greyed out so that data cannot be entered.

5. Click the **Apply** button at the upper right of the page.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Create a Private VLAN

To create a private VLAN, perform the following procedure:

> **Note**
>
> Private VLANs must be Enabled before a specific Private VLAN can be created. See "Enable or Disable Private VLAN" on page 179.

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select **VLAN**. The **VLAN** folder expands.

3. From the **VLAN** folder, select **Private VLAN**. The Private VLAN Page is displayed. See Figure 66 on page 179 for a partial view of this page.

4. Use the **Source Port** drop-down menu to select the source port. All ports under **Forwarding Ports** are automatically selected, and the source port is grayed out.

5. Select the forwarding ports:

   To select individual ports, click the **Clear** button, then click one or multiple check boxes under **Forwarding Ports**.

   > **Note**
   >
   > You will not be able to select the check box for the source port.

   To select all ports except the source port, skip to Step 6.

6. Click the **Apply** button under the forwarding ports. The private VLAN is shown in the **Port List** table. In the **Port Map** column, the source port is indicated first, followed by a comma and the forwarding ports. For example, if you selected **02** as a source port, and **06**, **07**, and **08** as forwarding ports, the port map would indicate **2,6-8**.

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Modify a Private VLAN

To modify a private VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**.
    The **Bridge** folder expands.

2. From the **Bridge** folder, select **VLAN**.
    The **VLAN** folder expands.

3. From the **VLAN** folder, select **Private VLAN**.
    The Private VLAN Page is displayed. See Figure 66 on page 179 for a partial view of this page.

4. Use the **Source Port** drop-down menu to select the source port of the private VLAN to be modified.

5. Select the forwarding ports: Click the check box to add or delete forwarding ports.

6. Click the **Apply** button under the forwarding ports.
    The modified private VLAN is shown in the Port List table.

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Delete a Private VLAN

To delete a private VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**.
    The **Bridge** folder expands.

2. From the **Bridge** folder, select **VLAN**.
    The **VLAN** folder expands.

3. From the **VLAN** folder, select **Private VLAN**.
    The Private VLAN Page is displayed. See Figure 66 on page 179 for a partial view of this page.

4. Use the **Source Port** drop-down menu to select the source port of the private VLAN to be deleted.

5. Click the **Clear** button under **Forwarding Ports**.

6. Click the **Apply** button under the forwarding ports.
    The modified private VLAN is deleted from the Port List table.

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

View Current VLAN Database

You can view the currently configured 802.1Q Tagged and Port-Based VLANs on the switch.

To view these VLAN configurations, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select **VLAN**. The **VLAN** folder expands.

3. From the **VLAN** folder, select **VLAN Current Database**. See Figure 67 for an example of the VLAN Current Database page with VLAN configurations.

VLAN Current Database

802.1Q Tagged VLAN

VLAN ID	VLAN Name	VLAN FDB ID	Member Ports	Untagged Ports	Status
1	DefaultVLAN	1	1-6	1-6	permanent
2	VLAN2	2	3-4	None	permanent

Page 1/1 First Page Previous Page Next Page Last Page Page [ ] GO

Port-Based VLAN

VLAN Index	VLAN Name	VLAN Member
5	Engineering	7-8

Page 1/1 First Page Previous Page Next Page Last Page Page [ ] GO

Figure 67. VLAN Current Database Page

The VLAN Current Database Page displays the following:

802.1Q Tagged VLAN table:

VLAN ID - VLAN ID numbers.

VLAN Name - VLAN names.

VLAN FBD ID - VLAN forwarding database ID numbers.

Member Ports - Tagged member ports.

Untagged Ports - Untagged member ports.

Status - Permanent (static) or dynamic.

Port-Based VLAN table:

VLAN Index - VLAN ID numbers.

VLAN Name - VLAN names.

VLAN Member - VLAN (untagged) member ports.

Chapter 14

GVRP

This chapter contains the following sections:

Overview and Guidelines

The GARP VLAN Registration Protocol (GVRP) allows network devices to share VLAN information and to use the information to modify existing VLANs or create new VLANs, automatically. This makes it easier to manage VLANs that span more than one switch. Without GVRP, you have to manually configure your switches to ensure that the various parts of the VLANs can communicate with each other across the different switches. With GVRP, which is an application of the Generic Attribute Registration Protocol (GARP), this is done for you automatically.

Here are the guidelines for GVRP:

- GVRP is supported with STP or RSTP or without spanning tree.

- Both ports constitute a network link between the switch, and the other device must be running GVRP.

- You cannot modify or delete dynamic GVRP VLANs.

- You cannot remove dynamic GVRP ports from static or dynamic VLANs.

- To be detected by GVRP, a VLAN must have at least one active node or have at least one port with a valid link to an end node. GVRP cannot detect a VLAN that does not have any active nodes or valid port links.

- Resetting the switch erases all dynamic GVRP VLANs and dynamic GVRP port assignments. The dynamic assignments are relearned by the switch as PDUs arrive on the ports from other switches.

- GVRP has three timers: join timer, leave timer, and leave all timer. The values for these timers must be identically configured on all switches running GVRP. Timers with different values on different switches can result in GVRP compatibility problems.

- You can convert dynamic GVRP VLANs and dynamic GVRP port assignments to static VLANs and static port assignments.

- The default port setting on the switch for GVRP is active, meaning that the ports participate in GVRP. Allied Telesis recommends disabling GVRP on those ports that are connected to GVRP-inactive devices, meaning devices that do not feature GVRP.

- PDUs are transmitted from only those switch ports in which GVRP is enabled.

General Configuration

Perform the following procedure to enable or disable GVRP:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select **GVRP**. The **GVRP** folder expands.

3. From the **GVRP** folder, select **GVRP Global Settings**. The GVRP Global Settings Page is displayed. See Figure 68.
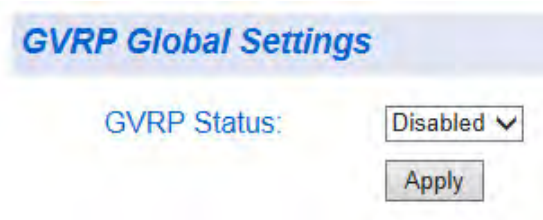
Figure 68. GVRP Global Settings Page

4. From the **GVRP Status** field, select one of the following choices from the pull-down menu:

    Enabled - The GVRP feature is active.

    Disabled - The GVRP feature is inactive.

5. Click **Apply**. The GVRP setting that you have selected is now active.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Port Settings

Perform the following procedure to configure the GVRP port settings:

1. From the main menu on the left side of the page, select **Bridge**.
    The **Bridge** folder expands.

2. From the **Bridge** folder, select **GVRP**.
    The **GVRP** folder expands.

3. From the **GVRP** folder, select **Port Settings**.
    The AT-GS950/16 Port Settings Page is displayed. See Figure 69 for a partial view of this page.

GVRP Port Settings

Port	Dynamic Vlan Status	Restricted VLAN Registration	Action
All	Ignore	Ignore	Apply
1	Enabled	Disabled	Apply
2	Enabled	Disabled	Apply
3	Enabled	Disabled	Apply
4	Enabled	Disabled	Apply
5	Enabled	Disabled	Apply
6	Enabled	Disabled	Apply
7	Enabled	Disabled	Apply
8	Enabled	Disabled	Apply

Figure 69. GVRP Port Settings Page

4. The following fields are listed for each port:

    Port - This parameter displays the ports on the switch.

    Dynamic Vlan Status - This parameter defines the GVRP status of the port. From the **Dynamic Vlan Status** field, select one of the following choices from the pull-down menu:

    Ignore - This parameter indicates that the setting in the **All** row does not apply to the **Dynamic Vlan Status** field. In other words, each port is set individually.

    Enabled - The **Dynamic Vlan** is activated for the port row selected.

    Disabled - The **Dynamic Vlan** is de-activated for the port row selected.

    Restricted VLAN Registration - This parameter controls if the VLAN registration on the port is restricted or not.

Ignore - This parameter indicates that the setting in the **All** row does not apply to the **Restricted VLAN Registration** field. In other words, each port is set individually.

Enabled - The **Restricted VLAN Registration** is activated for the port row selected.

Disabled - The **Restricted VLAN Registration** is de-activated for the port row selected.

5. Once you have configured the parameters, click **Apply** for the affected port.

6. If you want to configure GVRP for other ports, repeat Step 4 and Step 5.

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Time Settings

Perform the following procedure to configure the GVRP port settings:

1. From the main menu on the left side of the page, select **Bridge**.
    The **Bridge** folder expands.

2. From the **Bridge** folder, select **GVRP**.
    The **GVRP** folder expands.

3. From the **GVRP** folder, select **Time Settings**.
    The AT-GS950/16 GVRP Time Settings Page is displayed. See Figure 70 for a partial view of this page.

GVRP Time Settings

Port	JoinTime (10 ~ 2^30-14) msec	LeaveTime (30 ~ 2^31-18) msec	LeaveAllTime (40 ~ 2^31-8) msec	Action
All				Apply
1	200	600	10000	Apply
2	200	600	10000	Apply
3	200	600	10000	Apply
4	200	600	10000	Apply
5	200	600	10000	Apply
6	200	600	10000	Apply
7	200	600	10000	Apply
8	200	600	10000	Apply

Figure 70. AT-GS950/16 GVRP Time Settings Page

Note

The GARPLeaveTimer must be greater than (GARPJoinTimer x2 + 10) and the GARPLeaveAllTimer must be greater than (GARPLeaveTimer + 10). The acceptable input values are multiples of 10. If you try to enter a value that is not a multiple of 10, the value is rounded down.

4. The following fields are listed for each port:

    Port - This parameter displays the ports on the switch.

    JoinTime - This parameter is the GARP Join Timer. Its range is 10 - 1073741810 milli-seconds.

LeaveTime - This parameter is the GARP Leave Timer. Its range is 30 - 2147483630 milli-seconds. This timer must be set in relation to the GVRP Join Timer according to the following equation:

GARPLeaveTimer >= (GARPJoinTimer X 2) + 10

LeaveAllTime - This parameter is the GARP Leave Timer. Its range is 30 - 2147483630 milli-seconds. This timer must be set in relation to the GVRP Leave Timer according to the following equation:

GARPLeaveAllTimer > (GARPLeaveTimer + 10)

Note

To ensure compatibility between network devices, you must configure the same values for the GARP Join Timer, GARP Leave Timer, and GARP Leave All Timer on all participating GVRP devices in your network.

5. Once you have configured the parameters, click **Apply** for the affected port.

6. If you want to configure the GVRP timers for other ports, repeat Step 4 and Step 5.

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Chapter 15

Quality of Service and Class of Service

This chapter provides descriptions of both the Quality of Service (QoS) and Class of Service (CoS) features. The following topics are covered:

❒ "Overview" on page 194
❒ "Mapping CoS Priorities to Egress Queues" on page 198
❒ "Associate Ports to CoS Priorities" on page 200
❒ "Associate DSCP Classes to Egress Queues" on page 201
❒ "Queue Scheduling Algorithm" on page 203
❒ "IPv6 Traffic Class Mapping" on page 204

Note

Before mapping the QoS Priorities and the egress queues, you must disable the Jumbo frame parameter on each port. See the Jumbo parameter definition in "Displaying and Configuring Ports" on page 67.

Note

To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Overview

When a port on an Ethernet switch becomes oversubscribed, its egress queues contain more packets than the port can handle in a timely manner. In this situation, the port may be forced to delay the transmission of some packets, resulting in the delay of packets reaching their destinations. A port may be forced to delay transmission of packets while it handles other traffic, and, in some situations, some packets destined to be forwarded to an oversubscribed port from other switch ports may be discarded.

Minor delays are often of no consequence to a network or its performance. But there are applications, referred to as delay or time-sensitive applications, that can be impacted by packet delays. Voice transmission and video conferences are two examples. If packets carrying data in either of these cases are delayed from reaching their destination, the audio or video quality may suffer.

This is where Class of Service (CoS) is of value. It allows you to manage the flow of traffic through a switch by having the switch ports give higher priority to some packets, such as delay sensitive traffic, over other packets. This is referred to as prioritizing traffic.

The various aspects of CoS are:

❒ "Packet Priority"
❒ "Egress Queue vs Packet Priority Mapping" on page 195
❒ "Prioritizing Untagged Packets" on page 196
❒ "Scheduling" on page 196

Packet Priority   CoS applies primarily to tagged packets. A tagged packet contains information within it that specifies the VLAN to which the packet belongs.

A tagged packet can also contain a priority level. This priority level is used by network switches and other networking devices to know how important (delay sensitive) that packet is compared to other packets. Packets of a high priority are handled before packets of a low priority.

CoS, as defined in the IEEE 802.1p standard, has eight levels of priority. The priorities are 0 to 7, with 0 the lowest priority and 7 the highest.

When a tagged packet is received on a port on the switch, it is examined by the AT-S114 Management software for its priority. The switch software uses the priority to determine which ingress priority queue the packet should be directed to on the ingress port.

Egress Queue vs Packet Priority Mapping

Each port has four egress queues, labeled Low, Medium, High, Highest. Low is the lowest priority queue and Highest is the highest. A packet in a high-priority egress queue is typically transmitted sooner than a packet in a low-priority queue.Table 2 lists the default mappings between the eight CoS priority levels and the four egress queues of a switch port.

Table 2. Default Mappings Priority Levels to Priority Queues

IEEE 802.1p Priority Level	Port Priority Queue
0	Low
1	Low
2	Low
3	Low
4	Low
5	Low
6	Low
7	Low

You can change these mappings. For example, you might decide that packets with a priority of 6 and 7 need to be handled by egress queue Highest and packets with a priority of 2 and 3 should be handled in Medium. The result is shown in Table 3.

Table 3. Customized Mappings Priority Levels to Priority Queues

IEEE 802.1p Priority Level	Port Priority Queue
0	Low
1	Low
2	Medium
3	Medium
4	High
5	High
6	Highest
7	Highest

The procedure for changing the default mappings is found in "Associate Ports to CoS Priorities" on page 200. Note that because all ports must use the same priority-to-egress queue mappings, these mappings are applied at the switch level. They cannot be set on a per-port basis.

You can also map an IPv6 packet header's 8 bit priority field to one of the switch's priority queues. IPv6 traffic class priority settings are used by the switch to differentiate between classes or priorities of IPv6 ports. The procedure for mapping the IPv6 traffic class priorities is found in "IPv6 Traffic Class Mapping" on page 204.

One last thing to note is that the AT-S114 Management Software does not change the priority level in a tagged packet. The packet leaves the switch with the same priority it had when it entered. This is true even if you change the default priority-to-egress queue mappings.

Prioritizing Untagged Packets

CoS relates primarily to tagged packets rather than untagged packets because untagged packets do not contain a priority level. However, the AT-GS950/16 switch has a priority associated with each individual ingress port. By default, each port's priority is Low. You can redefine this parameter as described in "Associate Ports to CoS Priorities" on page 200.

Scheduling

A switch port needs a mechanism for knowing the order in which it should handle the packets in its four egress queues. For example, if all the queues contain packets, should the packets in queue Highest (the highest priority queue) be processed through the switch before moving on to the other queues, or should it instead just process a few packets from each queue in a sequential fashion and, if so, how many?

This control mechanism is referred to as the *scheduling algorithm*. Scheduling determines the order in which a port handles the packets in its egress queues. The AT-S114 software has two types of scheduling:

■ Strict priority
■ Weighted round robin priority

To specify the scheduling, refer to "Associate Ports to CoS Priorities" on page 200.

Note
Scheduling is set at the switch level. You cannot set this parameter on a per-port basis.

Strict Priority Scheduling

With this type of scheduling, a port transmits all packets out of higher priority queues before transmitting any from the lower priority queues. For

instance, as long as there are packets in the Highest queue, it does not handle any packets in the High queue. The value of this type of scheduling is that high-priority packets are always handled before low-priority packets which is required for voice or video data.

The problem with this method is that some low-priority packets might never be transmitted from the switch because the algorithm might never have time to process the packets waiting in the lower-priority queues.

Weighted Round Robin Priority Scheduling

The weighted round robin (WRR) scheduling method functions as its name implies. The port transmits a set number of packets from each queue, in a round robin fashion, so that each has a chance to transmit traffic. Normally, the higher the queue's priority, the more packets are transmitted in as the algorithm cycles through the queues in turn. This method guarantees that every queue receives some attention from the port for transmitting packets.

Table 4 shows the WRR settings for the number of packets transmitted from each queue. These values are permanent, and you cannot change these values.

Table 4. Example of Weighted Round Robin Priority

Port Egress Queue	Maximum Number of Packets
Highest	8
High	4
Medium	2
Low	1

Mapping CoS Priorities to Egress Queues

Before mapping the CoS priorities and the egress queues, you must disable the **Jumbo** frame parameter on each port. See the **Jumbo** parameter definition in "Displaying and Configuring Ports" on page 67.

Note

When **Jumbo** frames are enabled, CoS cannot be enabled.

To configure CoS mapping, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select **QoS**. The **QoS** folder expands.

3. From the **QoS** folder, select **CoS**. The CoS Page is displayed. See Figure 71.
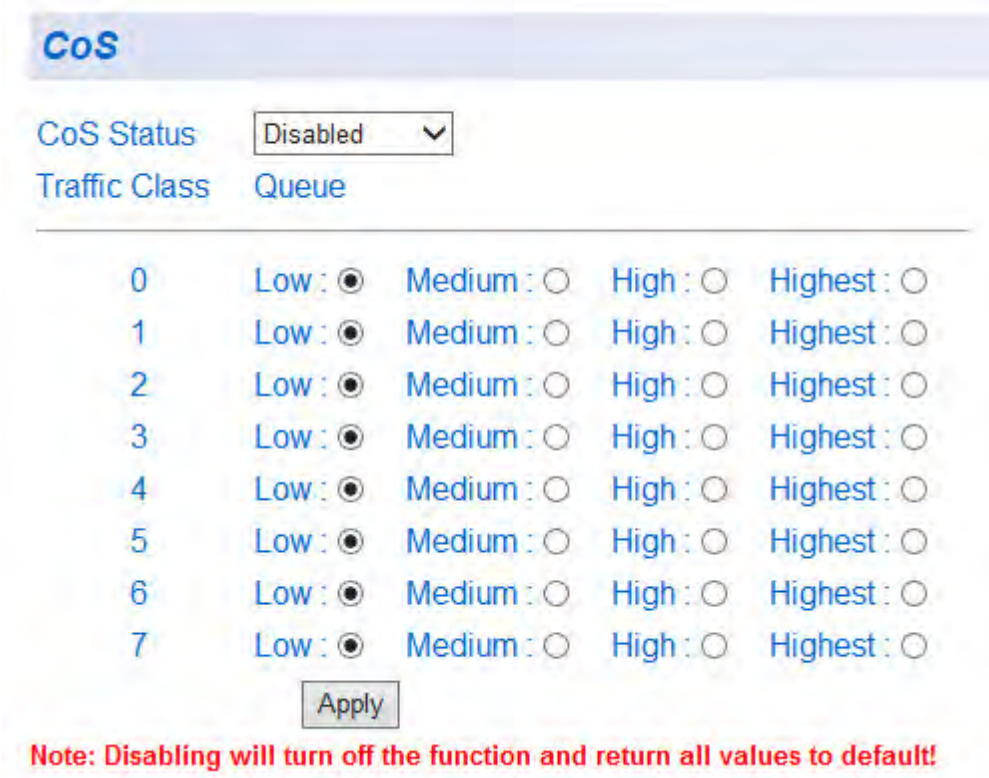
Figure 71. CoS Page

4. For each **Traffic Class** whose queue you want to change, click on the **Queue** (Low, Medium, High, Highest) radio button that applies to your configuration.

5. After you have completed this mapping process, select **Enable** in the **QoS Status** field.

6. Click **Apply**.

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Associate Ports to CoS Priorities

The Port Priority value is assigned to an untagged frame at the ingress for internal processing in the switch. This procedure explains how to change the default mappings of port priorities to the User Priority. This is set at the switch level. You cannot set this at the per-port level.

To change the port priority mappings, perform the following procedure.

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select **QoS**. The **QoS** folder expands.

3. From the **QoS** folder, select **Port Priority**. The AT-GS950/16 Port Priority Page page is displayed. See Figure 72 for a partial view of this page.

Port Priority

Port	User Priority	Action
All	Ignore ▼	Apply
1	0 ▼	Apply
2	0 ▼	Apply
3	0 ▼	Apply
4	0 ▼	Apply
5	0 ▼	Apply
6	0 ▼	Apply
7	0 ▼	Apply
8	0 ▼	Apply

Figure 72. AT-GS950/16 Port Priority Page

4. For each port whose priority you want to change, select a priority (0-7) in the **User Priority** column.

5. Click **Apply** for each port.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Associate DSCP Classes to Egress Queues

If you choose to use the DSCP tags in your Access Control policy configuration, each DSCP value (0-63) that is relevant to
your configuration must be mapped to one of the four egress queues (Low - Highest). The default queue for all DSCP values is Low.To assign the queue mappings to the DSCP values, perform the following procedure.

1. From the main menu on the left side of the page, select **Bridge**.
   The **Bridge** folder expands.

2. From the **Bridge** folder, select **QoS**.
   The **QoS** folder expands.

3. From the **QoS** folder, select **DSCP**.
   The DSCP Class Mapping Page page is shown in Figure 73.

DSCP Class Mapping

| DSCP Mapping | Disabled ∨ |
| | Apply |

DSCP In	Queue	DSCP In	Queue	DSCP In	Queue	DSCP In	Queue
0-15	Ignore ∨	16-31	Ignore ∨	32-47	Ignore ∨	48-63	Ignore ∨
0	Low ∨	16	Low ∨	32	Low ∨	48	Low ∨
1	Low ∨	17	Low ∨	33	Low ∨	49	Low ∨
2	Low ∨	18	Low ∨	34	Low ∨	50	Low ∨
3	Low ∨	19	Low ∨	35	Low ∨	51	Low ∨
4	Low ∨	20	Low ∨	36	Low ∨	52	Low ∨
5	Low ∨	21	Low ∨	37	Low ∨	53	Low ∨
6	Low ∨	22	Low ∨	38	Low ∨	54	Low ∨
7	Low ∨	23	Low ∨	39	Low ∨	55	Low ∨
8	Low ∨	24	Low ∨	40	Low ∨	56	Low ∨
9	Low ∨	25	Low ∨	41	Low ∨	57	Low ∨
10	Low ∨	26	Low ∨	42	Low ∨	58	Low ∨
11	Low ∨	27	Low ∨	43	Low ∨	59	Low ∨
12	Low ∨	28	Low ∨	44	Low ∨	60	Low ∨
13	Low ∨	29	Low ∨	45	Low ∨	61	Low ∨
14	Low ∨	30	Low ∨	46	Low ∨	62	Low ∨
15	Low ∨	31	Low ∨	47	Low ∨	63	Low ∨

| Apply | Reset to Default |

Figure 73. DSCP Class Mapping Page

4. Select **Enabled** from the **DSCP Mapping** drop-down menu.

5. Click **Apply** under the **DSCP Mapping** drop-down menu.

Note

You can disable DSCP class mapping by selecting **Disabled** from the **DSCP Mapping** drop-down menu, then clicking **Apply** under the **DSCP Mapping** drop-down menu.

---

6. For each DSCP In value that is relevant to your configuration, select a queue (**Low**, **Medium**, **High**, **Highest**) in the **Queue** column.

   To set all queues in a **Queue** column to the same value, use the **Queue** drop-down menu in the first row to select a queue.

7. After you have completed this mapping process, click **Apply**.

   To return the DSCP class mapping to the default values, click the **Reset to Default** button.

8. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Queue Scheduling Algorithm

To change the scheduling algorithm for the egress queues, perform the following procedure.

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select **QoS**. The **QoS** folder expands.

3. From the **QoS** folder, select **Scheduling Algorithm**. The Scheduling Algorithm Page page is shown in Figure 74.

Figure 74. Scheduling Algorithm Page

4. In the **Scheduling Algorithm** list, select one of the following algorithms:

   Strict Priority - The port transmits all packets out of higher priority queues before transmitting any from the lower priority queues.

   Weighted Round Robin - The port transmits a set number of packets from each queue, in a round robin fashion, so that each has a chance to transmit traffic. See Table 4 on page 197 for number of packets versus the port egress queue.

5. Click **Apply**.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

IPv6 Traffic Class Mapping

You can create and delete entries for IPv6 traffic class mapping by following the procedures in the following sections:

❐ "Enable or Disable IPv6 Traffic Class Mapping"

❐ "Create IPv6 Traffic Class Entries" on page 205

❐ "Delete an IPv6 Traffic Class Entry" on page 206

Before mapping IPv6 traffic class priorities, you must disable the **Jumbo** frame parameter on each port. See the **Jumbo** parameter definition in "Displaying and Configuring Ports" on page 67.

Note

When **Jumbo** frames are enabled, IPv6 traffic class mapping cannot be enabled.

Enable or Disable IPv6 Traffic Class Mapping

To enable or disable IPv6 traffic class mapping, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**.
    The **Bridge** folder expands.

2. From the **Bridge** folder, select **QoS**.
    The **QoS** folder expands.

3. From the **QoS** folder, select **IPv6 Traffic Class Priority Settings**.
    The IPv6 Traffic Class Priority Settings page is shown in Figure 75.

Figure 75. IPv6 Traffic Class Priority Settings Page

4. Use the **State** radio buttons to select the IPv6 Traffic Class Priority state:

> **Enabled** - Will activate IPv6 Traffic Class Priority mapping. The other parameters on the web page will become active.

> **Disabled** - Will de-activate IPv6 Traffic Class Priority mapping. The other parameters on the web page will become inactive and will be greyed out so that data cannot be entered.

5. Click **Apply**.

Create IPv6 Traffic Class Entries

To create IPv6 traffic class priority entries, perform the following procedure:

1. Enter a value for the IPv6 packet header's 8 bit priority in the **IPv6 Traffic Class** field. The range is 0-255.

2. Select a queue (**Low**, **Medium**, **High**, **Highest**) from the **Class ID** drop-down menu.

3. Click the **Add** button.
   The entry appears in the table. See Figure 76.

Figure 76. IPv6 Traffic Class Priority Settings Page with Entries

4. For additional entries, repeat Step 1 through Step 3.

5. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Delete an IPv6 Traffic Class Entry

To delete an IPv6 traffic class priority entry, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.

2. From the **Bridge** folder, select **QoS**. The **QoS** folder expands.

3. From the **QoS** folder, select **IPv6 Traffic Class Priority Settings**.

4. Under the **Action** column, click the **Delete** button to delete the entry you want to delete.

   To delete all entries, click the **Delete All** button.

5. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Section III
Advanced Features

This section contains the following chapters:

Chapter 16

SNMPv1 and v2c

This chapter contains a description of SNMPv1 and SNMPv2c and the procedures for configuring with these protocols. This chapter contains the following sections:

> **Note**
> To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

SNMPv1 and SNMPv2c Overview

You can manage a switch by viewing and configuring the management information base (MIB) objects on the device with the Simple Network Management Program (SNMP). This chapter describes how to configure SNMPv1 and SNMPv2c. A Group Name, IP address of the switch and at least one community string is the minimum required to manage the switch using SNMPv1 and SNMPv2c. To configure SNMPv3, see "SNMPv3" on page 223 for more information.

In the SNMPv1 and SNMPv2c protocols, the terms agent and manager may be used. An agent is software which runs on managed equipment such as the AT-GS950/16 switch. A manager is a workstation or server that runs the SNMP Network Management System (NMS) software.

The NMS software is capable of querying status, modifying existing configurations, and loading new configurations via the agent in the managed equipment. The NMS and agent communicate with each other using variables organized into pre-defined hierarchies called Management Information Bases or MIBs.

To manage a switch using an SNMP application program, you must do the following:

- Activate SNMP management on your switch. Refer to "User Interface Configuration" on page 45. By default, the SNMP manager is enabled.

- Compile the Allied Telesis private MIB associated with your switch with the Network Management Software (NMS) on your management workstation.

- Configure the SNMP interface parameters in the AT-S114 Management Software.

Note

The MIB file is available from the Allied Telesis web site at **www.alliedtelesis.com/support/software**.
Enter your hardware product model in the **Search by Product Name** field; for example, enter "AT-GS950/16." Links for the latest product software and documentation are displayed. To obtain the latest MIB file, click the link of the most recent version of the AT-S114 Management Software.

Trap Receiver Attributes

A trap is a message sent by the agent to one or more managers to indicate the occurrence of a particular event on the device. There are numerous events that can trigger a trap. For instance, when the switch reboots or when the Spanning Tree Root Bridge changes. You use traps to monitor activities on the switch.

Trap receivers are the typically SNMP management stations, that you want to receive the traps sent by the switch. You specify a trap receiver by its IP address which is assigned to a specific community string.

The community string name is included when the switch sends a trap. The management station may use the community string as a verification of the trap source.

If you are not interested in having SNMP stations receive traps, then you do not need to enter any IP addresses of trap receivers.

Activate SNMP Interface

The SNMP interface is activated by default. If you want to de-activate it or re-activate it, go to "User Interface Configuration" on page 45.

SNMPv1 and SNMPv2c User and Group Names

SNMPv1 and SNMPv2c User Name and Group Name definitions is the basis for creating SNMP communities. Use the following sections to create and delete User and Group Names:

- "Create User and Group Names," next
- "Modify User and Group Names" on page 215
- "Delete User and Group Names" on page 215

A community string has attributes for controlling who can use the string and what the string allows a network management station to do on the switch.

The AT-S114 Management Software does not provide any default community strings. You must first define an SNMP User and Group Name on the SNMP User/Group page and then define a Community Name on the SNMP Community Table page.

Create User and Group Names

To create an SNMP User and Group Name, perform the following procedure:

1. From the main menu on the left side of the page, select the **SNMP** folder.
   The **SNMP** folder expands.

2. From the **SNMP** folder, select **SNMP User/Group**.
   The SNMP User/Group Page is displayed in Figure 77.

SNMP User/Group

| User Name: | | * (32 characters limit) |
| Group Name: | | * (32 characters limit) |

SNMP Version:	v1 ▼			encrypted
Auth-Protocol:	MD5 ▼		Password:	
Priv-Protocol:	DES ▼		Password:	

Add   Reset

User Name	Group Name	SNMP Version	Auth-Protocol	Priv-Protocol	Action
ReadOnly	ReadOnly	v1	None	None	Delete
ReadOnly	ReadOnly	v2c	None	None	Delete
ReadWrite	ReadWrite	v1	None	None	Delete
ReadWrite	ReadWrite	v2c	None	None	Delete

Figure 77. SNMP User/Group Page

> **Note**
>
> If you choose to use the default User and Group Names (ReadOnly and ReadWrite) that are already displayed in the table, proceed to Step 7 below.

3. Type a new **User Name**.
    Enter a name up to 32 characters in length.

4. Type a previously defined **Group Name**.
    Enter a name up to 32 characters in length.

5. Select either **v1** or **v2c** as the SNMP Version.

> **Note**
>
> The **encrypted** check-box and **Auth-Protocol**, **Priv-Protocol**, and **password** fields are intended for SNMPv3 configurations only and are not used for SNMPv1 or v2c configurations.

6. Click **Add**.
    See Figure 78 for an example of the SNMP User/Group page.

SNMP User/Group

User Name:		* (32 characters limit)
Group Name:		* (32 characters limit)
SNMP Version:	v1	encrypted
Auth-Protocol:	MD5	Password:
Priv-Protocol:	DES	Password:

Add Reset

User Name	Group Name	SNMP Version	Auth-Protocol	Priv-Protocol	Action
Jill	ATI-SJ	v2c	None	None	Delete
Holly	Contractors	v1	None	None	Delete
ReadOnly	ReadOnly	v1	None	None	Delete
ReadOnly	ReadOnly	v2c	None	None	Delete
ReadWrite	ReadWrite	v1	None	None	Delete
ReadWrite	ReadWrite	v2c	None	None	Delete

Figure 78. SNMP User/Group Page Example

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Modify User and Group Names

If you need to modify an entry in the SNMP User/Group page, you must first delete the entry and then re-enter it. For information about how to delete an entry in this table, see "Delete User and Group Names," next. To create a new entry in this table, see "Create User and Group Names" on page 213.

Delete User and Group Names

This procedure explains how to delete an entry on the SNMP User/Group page.

1. From the main menu on the left side of the page, select the **SNMP** folder.

   The **SNMP** folder expands.

2. From the **SNMP** folder, select **SNMP User/Group**.

   The SNMP User/Group Page is displayed. See Figure 77 on page 213.

3. In the **Action** column of the table, click **Delete** for the **User Name** and **Group Name** that you want to remove.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

SNMP Community Strings

A community string has attributes for controlling who can use the string and what the string will allow a network management station to do on the switch. The AT-S114 Management Software does not provide any default community strings. You must first define an SNMP User and Group Name on the SNMP User/Group page and then define a Community Name on the SNMP Community Table page.

Use the following sections to create, modify, and delete SNMP community strings:

- ■ "Create SNMP Community Strings," next
- ■ "Modify SNMP Community Strings" on page 217
- ■ "Delete SNMP Community Strings" on page 217

Create SNMP Community Strings

To create an SNMPv1 or SNMPv2c community string, do the following:

1. From the main menu on the left side of the page, select the **SNMP** folder.

    The **SNMP** folder expands.

2. From the **SNMP** folder, select **Community Table**.
    The Community Table Page is displayed. See Figure 79.

Figure 79. Community Table Page

3. Enter a new **Community Name**.

    A name can be up to 32 characters in length.

4. Enter a **User Name(View Policy)** that has been previously defined.

Note

This name must match one of the User Names displayed on the
SNMP User/Group page. See "Create User and Group Names" on
page 213. If you enter a user name that has not been pre-defined on
the SNMP User/Group page, the Community entry is displayed, but
the agent/manager communication fails.

5. Click **Add**.

    The values of the new **Community Name** and **User Name** are
    displayed. See Figure 80 for an example.

Figure 80. SNMP Community Table Page Example

6. From the main menu on the left side of the page, select **Save Settings
    to Flash** to permanently save your changes.

Modify SNMP Community Strings

If you need to modify a Community Table entry, you must first delete the
entry by using the procedure below and then re-enter it with the
modification by creating a new Community table entry. See "SNMPv1 and
SNMPv2c User and Group Names" on page 213.

Delete SNMP Community Strings

Use the following procedure to delete a community name of an SNMP
community from the Community Table.

1. From the main menu on the left side of the page, select the **SNMP**
    folder.
    The **SNMP** folder expands.

2. From the **SNMP** folder, select **Community Table**.
    The Community Table Page is shown in Figure 79 on page 216.

3. To delete a **Community Name**, click **Delete** next to the entry in the
    table that you want to remove.
    The deleted **Community Name** is no longer displayed in the
    Community table. No confirmation message is displayed.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

SNMP Traps

A Host IP address is used to specify a management device that needs to receive SNMP traps sent by the switch. This IP address is associated with the SNMP Version and a valid Community Name in the Host table of the switch.

Use the following sections to create, modify, and delete trap host table entries:

- "Create Trap Host Table Entry," next
- "Modify a Trap Host Table Entry" on page 220
- "Delete a Trap Host Table Entry" on page 221

Create Trap Host Table Entry

Use the following procedure to create a trap Host table entry:

1. From the main menu on the left side of the page, select the **SNMP** folder.
   The **SNMP** folder expands.

2. From the **SNMP** folder, select **Trap Management**.
   The Trap Management Page is displayed. See Figure 81.

Figure 81. Trap Management Page

3. Enable trap management by selecting the radio button next to **Enabled** at the top of the page. (By default, trap management is enabled.)

4. Click **Apply**.

5. Enter the **Host IP Address** for the management device that is to receive the SNMP traps in one of the **Host IP Address** fields:

> For an IPv4 address, click **IPv4**, then enter the address using xxx.xxx.xxx.xxx format.
>
> For an IPv6 address, click **IPv6**, then enter the address using xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx format.

6. Enter the **SNMP Version**, either **v1** or **v2c**, that is configured for the host management device.

7. Enter a **Community Name** that you have defined previously in the SNMP Community table.

Note

The **Community Name** must correlate with one of the communities displayed on the SNMP Community Table page. See "SNMP Community Strings" on page 216. If you enter a **Community Name** that has not been pre-defined, the Trap Host entry is displayed, but agent/manager communication fails.

---

8. Click **Add**.
   The new host is added to the table. An example of a host is shown in the table at the bottom of Figure 82.

Figure 82. Trap Management Page Example

9. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Modify a Trap Host Table Entry

If you need to modify an SNMP Trap entry, you must first delete the entry by using the procedure below and then re-enter it with the modification by creating a new SNMP trap- see "SNMP Traps" on page 219.

Delete a Trap Host Table Entry

Use the following procedure to delete a Host table entry:

1. From the main menu on the left side of the page, select the **SNMP** folder.
    The **SNMP** folder expands.

2. From the **SNMP** folder, select **Trap Management**.

3. The Trap Management Page is displayed. See Figure 81 on page 219.

4. To delete an entry in the host table, click **Delete** next to the entry in the table that you want to remove.
    The Host table entry is removed from the table. No confirmation message is displayed.

5. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Chapter 17

SNMPv3

This chapter contains a description of SNMPv3 and the procedures for configuring this protocol. This chapter contains the following sections:

Note

To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Overview

The SNMPv3 protocol builds on the existing SNMPv1 and SNMPv2c protocol implementation which is described in Chapter 16 on page 209. In SNMPv3, User-based Security Model (USM) authentication is implemented along with encryption, allowing you to configure a secure SNMP environment.

The SNMPv3 protocol uses different terminology than the SNMPv1 and SNMPv2c protocols. In the SNMPv1 and SNMPv2c protocols, the terms agent and manager are used. An agent is the software within an SNMP user, while a manager is an SNMP host. In the SNMPv3 protocol, agents and managers are called entities. In any SNMPv3 communication, there is an authoritative entity and a non-authoritative entity. The authoritative entity checks the authenticity of the non-authoritative entity. And, the non-authoritative entity checks the authenticity of the authoritative entity.

With the SNMPv3 protocol, you create users, determine the protocol used for message authentication and determine if data transmitted between two SNMP entities is encrypted. In addition, you can restrict user privileges by defining which portions of the Management Information Bases (MIB) that can be viewed by specific users. In this way, you restrict which MIBs a user can display and modify. In addition, you can restrict the types of messages, or traps, the user can send. (A trap is a type of SNMP message.) After you have created a user, you define SNMPv3 message notification. This consists of determining where messages are sent and what types of messages can be sent. This configuration is similar to the SNMPv1 and SNMPv2c configurations because you configure IP addresses of trap receivers, or hosts.

This section describes the features of the SNMPv3 protocol. The following subsections are included:

❑ "SNMPv3 Authentication Protocols"
❑ "SNMPv3 Privacy Protocol" on page 225
❑ "SNMPv3 MIB Views" on page 225
❑ "SNMPv3 Configuration Process" on page 226

SNMPv3 Authentication Protocols

The SNMPv3 protocol supports two authentication protocols— HMAC-MD5-96 (MD5) and HMAC-SHA-96 (SHA). Both MD5 and SHA use an algorithm to generate a message digest. Each authentication protocol authenticates a user by checking the message digest. In addition, both protocols use keys to perform authentication. The keys for both protocols are generated locally using the Engine ID and the user password. You can only modify a key by modifying the user password.

In addition, you have the option of assigning no user authentication. In this case, no authentication is performed for this user. You may want to make this configuration for someone with super-user capabilities.

SNMPv3 Privacy Protocol

After you have configured an authentication protocol, you have the option of assigning a privacy protocol if you have the encrypted version of the AT-S114 Management software. In SNMPv3 protocol terminology, privacy is equivalent to encryption. Currently, the DES protocol is the only encryption protocol supported. The DES privacy protocol requires the authentication protocol to be configured as either MD5 or SHA.

If you assign a DES privacy protocol to a user, then you are also required to assign a privacy password. If you choose to not assign a privacy value, then SNMPv3 messages are sent in plain text format.

SNMPv3 MIB Views

The SNMPv3 protocol allows you to configure MIB views for users and groups. The MIB tree is defined by RFC 1155 (Structure of Management Information). See Figure 83.
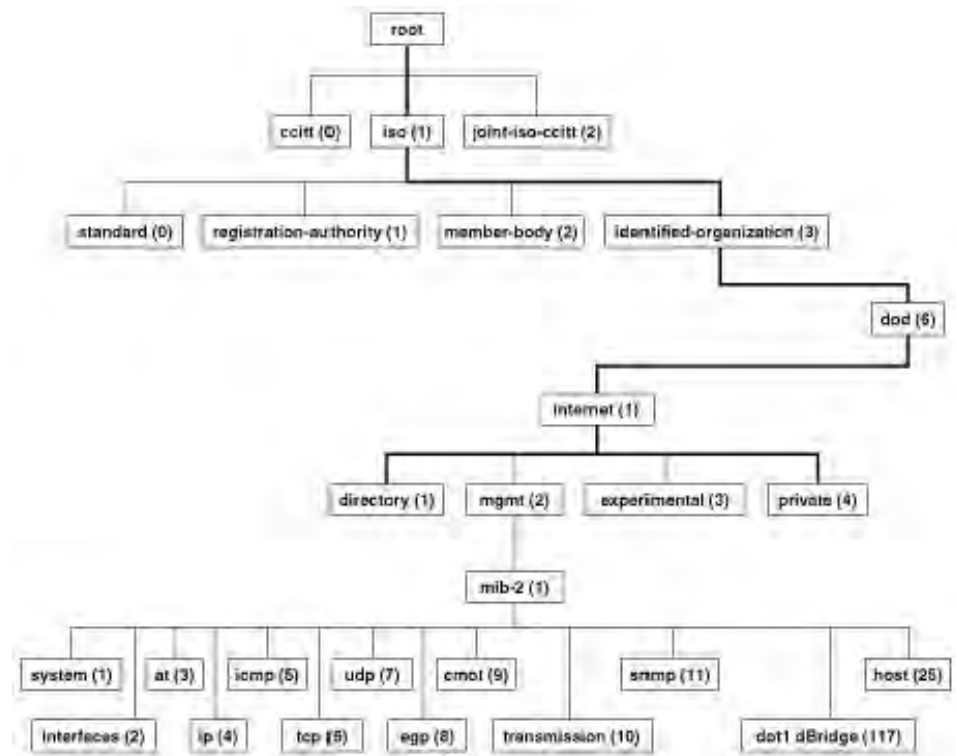
Figure 83. MIB Tree

The AT-S114 Management software supports the MIB tree, starting with the Internet MIBs, as defined by 1.3.6.1. There are two ways to specify an MIB view. You can enter the OID number of the MIB view or its equivalent text name. For example, to specify MIBs in the Internet view, you can enter the OID format "1.3.6.1" or the text name, "internet."

In addition, you can define an MIB view that the user can access or an MIB view that the user cannot access. When you want to permit a user to access an MIB view, you include a particular view. When you want to deny a user access to an MIB view, you exclude a particular view.

After you specify an MIB subtree view you have the option of further restricting a view by defining a subtree mask. The relationship between an MIB subtree view and a subtree mask is analogous to the relationship between an IP address and a subnet mask. The switch uses the subnet mask to determine which portion of an IP address represents the network address and which portion represents the node address. In a similar way, the subtree mask further refines the subtree view and enables you to restrict an MIB view to a specific row of the OID MIB table. You need a thorough understanding of the OID MIB table to define a subtree mask.

SNMPv3 Configuration Process

The SNMPv3 parameters are contained in the following tables for user configuration:

- SNMPv3 User/Group table
- SNMPv3 Access table
- SNMPv3 View table
- SNMPv3 Community table
- Trap Management

The SNMPv3 configuration information must be entered in a specific sequence:

Note

The SNMP Interface must be activated first. See "User Interface Configuration" on page 45.

---

1. You create a User Name and associated Group Name in the SNMPv3 User/Group table.

2. The View Names are defined in the Access table for each Group Name.

3. The MIB view is then defined in the SNMPv3 View table for each View Name.

4. You must enter information in the Community table based on a pre-defined User Name.

Note

The Community Strings do not have a default value defined and are initially blank.

---

5. Finally, the traps can be defined on the Trap Management page based on the Community or User Name.

See Figure 84 for an illustration of how the user configuration tables are linked.
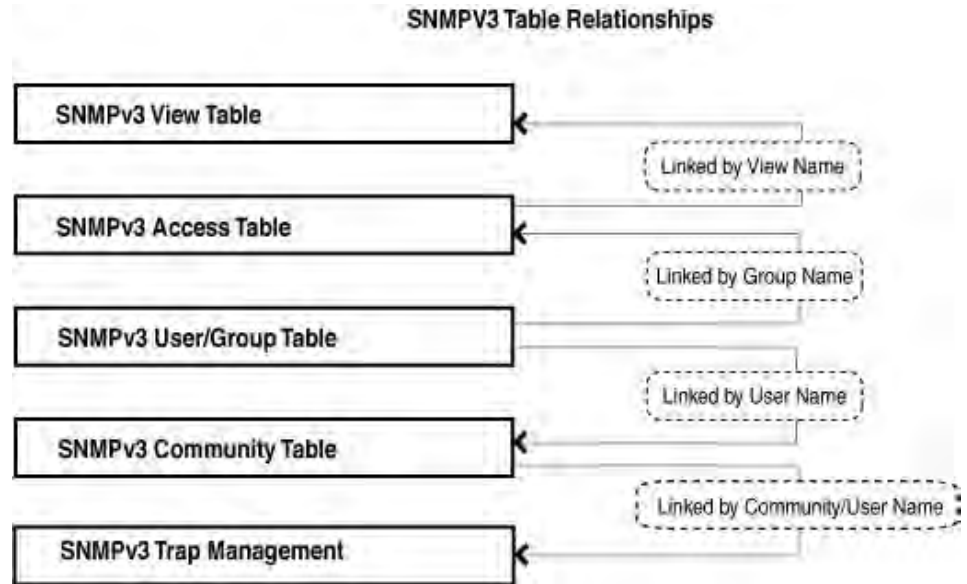
Figure 84. SNMPv3 Table Relationships

SNMPv3 User and Group Names

An SNMPv3 User Name and Group Name definition is the basis for all other SNMPv3 tables. You can create and delete View Names by following the procedures in the following sections:

❒ "Creating SNMPv3 User and Group Names"

❒ "Modifying SNMPv3 User and Group Names" on page 229

❒ "Deleting SNMPv3 User and Group Names" on page 230

Creating SNMPv3 User and Group Names

Use this procedure to create SNMPv3 User Names and Group Names:

1. From the main menu on the left side of the page, select the **SNMP** folder.

   The **SNMP** folder expands.

2. From the **SNMP** folder, select **SNMP User/Group**.

   The SNMP User/Group page is displayed. See Figure 77 on page 213.

   ***

   Note
   There are no default User Names or Group Names defined for SNMPv3.

   ***

3. Type a new **User Name**.

   Enter a name up to 32 characters in length.

4. Type a new **Group Name**.

   Enter a name up to 32 characters in length.

5. From the **SNMP Version** pull-down menu, select **v3**.

   The **encryption** check-box becomes active.

6. Check the **encryption** check-box.

   The **Auth-Protocol**, **Priv-Protocol**, and associated password fields become active.

7. Select one of the following choices for the **Auth-Protocol** field:

   MD5: The MD5 authentication protocol. SNMPv3 Users are authenticated with the MD5 authentication protocol after a message is received.

SHA - The SHA authentication protocol. Users are authenticated with the SHA authentication protocol after a message is received.

8. Enter the password for the **Auth-Protocol**.

9. Select one of the following choices for the **Priv-Protocol** field:

DES: Specifies DES encryption scrambles the SNMP data so that outside observers are prevented from seeing the data content.

none: Specifies no encryption is applied to SNMP data.

Note

If you specify a privacy password, the privacy protocol is set to DES, and you must also specify an authentication protocol and password.

---

10. Click **Add**.

The new User Name and Group Name are displayed on the SNMP User/Group page. See Figure 85.

SNMP User/Group

User Name:		* (32 characters limit)	
Group Name:		* (32 characters limit)	
SNMP Version:	v1		encrypted
Auth-Protocol:	MD5		Password:
Priv-Protocol:	DES		Password:

Add   Reset

User Name	Group Name	SNMP Version	Auth-Protocol	Priv-Protocol	Action
Jarad	Managers	v3	MD5	DES	Delete
Jordan	Managers	v3	MD5	DES	Delete
ReadOnly	ReadOnly	v1	None	None	Delete
ReadOnly	ReadOnly	v2c	None	None	Delete
ReadWrite	ReadWrite	v1	None	None	Delete
ReadWrite	ReadWrite	v2c	None	None	Delete

Figure 85. SNMP User Group, SNMPv3 Example

11. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Modifying SNMPv3 User and Group Names

If you need to modify an entry in the **SNMP User/Group** page, you must first delete the entry and then re-enter it. For information about how to delete an entry in this table, see "Deleting SNMPv3 User and Group Names" on page 230. For information about how to create a new entry in this table, see "Creating SNMPv3 User and Group Names" on page 228.

Deleting SNMPv3 User and Group Names

This procedure explains how to delete an entry on the SNMP User/Group page.

1. From the main menu on the left side of the page, select the **SNMP** folder.

   The **SNMP** folder expands.

2. From the **SNMP** folder, select **SNMP User/Group**.

   The SNMP User/Group Page is displayed. See Figure 77 on page 213.

3. In the **Action** column of the table, click **Delete** for the **User Name** and **Group Name** that you want to remove.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

SNMPv3 View Names

The SNMPv3 View names are defined in the SNMP Group Access table and are based on the User and Group Names.You can create and delete View Names with the following procedures:

❒ "Creating SNMPv3 View Names"

❒ "Modifying SNMPv3 View Names" on page 233

❒ "Deleting SNMPv3 View Names" on page 233

Creating SNMPv3 View Names

Before you can create an SNMPv3 View name, you must define a Group Name using the SNMP User/Group page. See "Creating SNMPv3 User and Group Names" on page 228.

Use this procedure to create SNMPv3 View Names.

1. From the main menu on the left side of the page, select the **SNMP** folder.

   The **SNMP** folder expands.

2. From the **SNMP** folder, select **Group Access Table**.

   The SNMP Group Access Table page is displayed. See Figure 86.

SNMP Group Access Table

Group Name:		* (32 characters limit)
Read View Name:		(32 characters limit)
Write View Name:		(32 characters limit)
Notify View Name:		(32 characters limit)
Security Model:	v1 ▾	
Security Level:	NoAuthNoPriv ▾	
	Add Reset	

Group Name	Read View	Write View	Notify View	Security Model	Security Level	Action
ReadOnly	ReadWrite	---	ReadWrite	v1	NoAuthNoPriv	Delete
ReadOnly	ReadWrite	---	ReadWrite	v2c	NoAuthNoPriv	Delete
ReadWrite	ReadWrite	ReadWrite	ReadWrite	v1	NoAuthNoPriv	Delete
ReadWrite	ReadWrite	ReadWrite	ReadWrite	v2c	NoAuthNoPriv	Delete

Figure 86. SNMP Group Access Table

3. Enter the **Group Name**.

Note

This entry must be pre-defined on the SNMP User/Group page. Refer to "Creating SNMPv3 View Names" on page 231.

---

4. Enter the **Read View Name**.

   This name is an optional field. It can be up to 32 characters in length.

5. Enter the **Write View Name**.

   This name is an optional field. It can be up to 32 characters in length.

6. Enter the **Notify View Name**.

   This name is an optional field. It can be up to 32 characters in length.

7. From the **Security Model** pull-down menu, select **v3**.

8. Enter the **Security Level** from the pull-down menu. The selection options are:

   NoAuthNoPriv: This selection is appropriate when no **Auth-Protocol** or **Priv-Protocol** (no encryption) are selected on the SNMP User/Group page.

   AuthNoPriv: Choose this selection when encryption has been enabled, but only the **Auth-Protocol** has a password assigned, and the **Priv-Protocol** has been selected as **none** on the SNMP User/Group page.

   AuthPriv: When both the **Auth-Protocol** or **Priv-Protocol** have been enabled, choose this selection.

9. Click the **Add** button.
   See Figure 87 on page 233 for an example.

SNMP Group Access Table

Group Name:		* (32 characters limit)
Read View Name:		(32 characters limit)
Write View Name:		(32 characters limit)
Notify View Name:		(32 characters limit)
Security Model:	v1	
Security Level:	NoAuthNoPriv	

Add   Reset

Group Name	Read View	Write View	Notify View	Security Model	Security Level	Action
Managers	---	---	---	v3	NoAuthNoPriv	Delete
ReadOnly	ReadWrite	---	ReadWrite	v1	NoAuthNoPriv	Delete
ReadOnly	ReadWrite	---	ReadWrite	v2c	NoAuthNoPriv	Delete
ReadWrite	ReadWrite	ReadWrite	ReadWrite	v1	NoAuthNoPriv	Delete
ReadWrite	ReadWrite	ReadWrite	ReadWrite	v2c	NoAuthNoPriv	Delete

Figure 87. SNMP Group Access Table Example for SNMPv3

10. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Modifying SNMPv3 View Names

If you need to modify an entry in the SNMP Group Access page, you must first delete the entry and then re-enter it. For information about how to delete an entry in this table, see "Deleting SNMPv3 View Names" on page 233. For information about how to create a new entry in this table, see "Creating SNMPv3 View Names" on page 231.

Deleting SNMPv3 View Names

This procedure explains how to delete an entry on the SNMP Group Access Table page.

1. From the main menu on the left side of the page, select the **SNMP** folder.

   The **SNMP** folder expands.

2. From the **SNMP** folder, select **SNMP Access Table**.

   The SNMP Group Access Table page is displayed. See Figure 86 on page 231.

3. In the **Action** column of the table, click **Delete** for the **View Name** that you want to remove.

   Note
   The views corresponding to the **ReadOnly** and **ReadWrite Group Names** are default values and cannot be removed.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

SNMPv3 View Table

The SNMPv3 View table specifies the MIB object access criteria for each View Name. If the View Name is not specified on this page, then it has access to all MIB objects. You can specify specific areas of the MIB that can be accessed or denied based on the entries in this table. You can create and delete entries in the View table by following the procedures in the following sections:

- "Creating SNMPv3 View Table Entries"
- "Modifying SNMPv3 View Table Entries" on page 235
- "Deleting SNMPv3 View Table Entries" on page 235

Creating SNMPv3 View Table Entries

This procedure explains how to create entries in the SNMPv3 View Table.

1. From the main menu on the left side of the page, select the **SNMP** folder.

   The **SNMP** folder expands.

2. From the **SNMP** folder, select **View Table**.

   The SNMP View Table page is displayed. See Figure 88.

Figure 88. SNMP View Table

3. Enter the **View Name**.

Note

This entry must be pre-defined on the SNMP User/Group page. See "Creating SNMPv3 View Names" on page 231.

---

4. Enter the **Subtree OID**.

5. Enter "1" for the **OID Mask**.

6. Enter the **View Type**. Choose from the following:

> **Included**: This selection allows the specified MIB object to be included in the view.

> **Excluded**: This selection blocks the view of the specified MIB object.

7. Click the **Add** button.

> The updated view is displayed in the View Table. See Figure 89.

Figure 89. SNMP View Table Page Example

8. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Modifying SNMPv3 View Table Entries

If you need to modify an entry in the View Table page, you must first delete the entry and then re-enter it. For information about how to delete an entry in this table, see "Deleting SNMPv3 View Table Entries". For information about how to create a new entry in this table, see "Creating SNMPv3 View Table Entries" on page 234.

Deleting SNMPv3 View Table Entries

1. From the main menu on the left side of the page, select the **SNMP** folder.

> The **SNMP** folder expands.

2. From the **SNMP** folder, select **View Table**.

> The SNMP View Table page is displayed. See Figure 88 on page 234.

> In the **Action** column of the table, click **Delete** for the View table entry that you want to remove.

Note

The views corresponding to the **ReadOnly** and **ReadWrite Group Names** are default values and cannot be removed.

3. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

SNMPv3 Traps

The creation, modification and deletion of traps for SNMPv3 is identical to the procedure for SNMPv1/v2. See "SNMP Traps" on page 219.

SNMP Engine ID

An SNMP agent has an engine ID to uniquely identify the agent in a device. In addition, the engine ID uniquely identifies MIB objects within a domain.

Following the RFC 3411 standard, the engine ID consists of the enterprise ID and the MAC address for the switch.

You can modify and reset the SNMP engine ID by following the procedures in the following sections:

❏ "Modifying SNMP Engine ID"
❏ "Resetting SNMP Engine ID"

Modifying SNMP Engine ID

This procedure explains how to modify the engine ID.

1. From the main menu on the left side of the page, select the **SNMP** folder.

   The **SNMP** folder expands.

2. From the **SNMP** folder, select **Engine ID**.

   The SNMP Engine ID Settings page is displayed. See Figure 90.

Figure 90. SNMP Engine ID Settings

3. Type the engine ID in the **Engine ID** field.

4. Click **Apply**.

5. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Resetting SNMP Engine ID

This procedure explains how to reset the engine ID or reset the engine ID to the default setting.

1. From the main menu on the left side of the page, select the **SNMP** folder.

   The **SNMP** folder expands.

2. From the **SNMP** folder, select **Engine ID**.

    The SNMP Engine ID Settings page is displayed. See Figure 90 on page 238.

3. Reset the engine ID:

    To reset the engine ID to the previous setting, click **Reset**.

    To reset the engine ID to the default setting, click **Reset to Default**.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Chapter 18

Access Control Configuration

This chapter contains a description of the AT-GS950/16 switch's Access Control Configuration feature and the procedures to create, modify, and delete an Access Control configuration. This chapter contains the following sections.

Overview

Access Control configuration allows you to control different aspects of the Ethernet traffic as it enters the switch ports and is processed through the switch. You can specify which traffic is permitted or denied to flow through the switch by setting up specific filtering criteria at an ingress port. You can also manage the switching priority of ethernet packets. All of this is done by specifying policies that define the filtering and priority behavior.

> **Note**
>
> Before you specify the Access Control policies, be sure to configure the QoS parameters. The QoS entries may have a direct effect on each policy's behavior. For more information, see Chapter 15, "Quality of Service and Class of Service" on page 193.

To define a policy, specify the Access Control configuration. Refer to "Policy Settings" on page 243. Each policy has a unique index number.

If your configuration requires a Committed Information Rate (CIR), you must first configure the CIR. Refer to "Rate Control Settings" on page 251.

If you define multiple policies for different ports, you can display the order that policies are applied to each port. Refer to "Policy Database" on page 254.

Policy Settings

The Policy Settings page lets you create one or multiple IPv4 and/or IPv6 policies for filtering and policing Ethernet traffic.

You can create, modify, or delete a policy by following the procedures in the following sections:

❒ "Create a Policy," next
❒ "Change a Policy Status" on page 247
❒ "Modify a Policy" on page 248
❒ "Delete a Policy" on page 249
❒ "View Specific Classifier Details" on page 249

Create a Policy

To create a policy, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
   The **Access Control Config** folder expands.

2. From the **Access Control Config** folder, select **Policy Settings**.
   The Policy Settings page is displayed. See Figure 91.

Figure 91. Policy Settings Page

3. Select one of the following **Policy type** buttons:

   To create an IPv4 policy, click **Add L2+IPv4**. The IPv4 Policy Settings page is displayed. See Figure 92 on page 244.

Figure 92. IPv4 Policy Settings Page

To create an IPv6 policy, click **Add IPv6**. The IPv6 Policy Settings page is displayed. See Figure 93.

Figure 93. IPv6 Policy Settings Page

4. Enter a number in the **Policy Index** field.
   The Policy Index must be a unique number within the range of
   1 - 65535 which identifies the policy. This field is mandatory.

5. Enter a number in the **Policy Sequence** field.
   The Policy Sequence must be a unique number within the range of
   1 - 65535. This field is mandatory.

   The Policy Sequence identifies the ranking of the specific policy and
   defines when it will be executed relative to the other policies. A policy
   with a Policy Sequence number 1 will be executed first, number 2 will
   be executed second, until the highest Policy Sequence number is
   reached which will be executed last. For the status of the order of the
   policies applied to specific ports, refer to "Policy Database" on
   page 254.

6. Enter a port or group of ports in the **Port List** field. The port list can be
   specified as a consecutive list, a non-consecutive list, or a combination
   of the two. At least one or more ports must be specified. For example,
   you can specify ports 1-3,5,8.

   Note

   You cannot combine members and non-members of a trunk in a port
   list. For example, if ports 3 and 4 are configured and active via the
   Trunking page, you would not be able to assign 1-4 in the port list,
   but you could assign 3 and 4.

   Note

   Policy Index, **Policy Sequence**, and **Port List** are required
   parameters when you create a policy.

   ---

7. Configure one or more of the remaining parameters, listed below:

   IPv4 **Source MAC Address** - Source MAC address in
   xx.xx.xx.xx.xx.xx format. Applies to IPv4 only.

   IPv4 Source MAC **Mask Length** - Length of the Source MAC Mask
   ranging from 1 - 48. Applies to IPv4 only.

   IPv4 **Destination MAC Address** - Destination MAC address in
   xx.xx.xx.xx.xx.xx format. Applies to IPv4 only.

   IPv4 Destination MAC **Mask Length** - Length of the Destination
   MAC Mask ranging from 1 - 48. Applies to IPv4 only.

   VLAN ID - A unique number identifying a VLAN ranging from 1 -
   4093.

   802.1p Priority - 802.1p priority level of the frame ranging from 0 -
   7.

IPv4 **Ether Type** - Protocol of the ethernet frame protocol ranging from 0000 - FFFF. Applies to IPv4 only.

Protocol - Packet protocol ranging from 0 - 255.

IPv4 Source IP Address - Source IPv4 address. Applies to IPv4 only.

IPv4 Source IP **Mask Length** - Mask length of the source IPv4 address ranging from 0 - 32. Applies to IPv4 only.

IPv4 Destination IP Address - Destination IPv4 address. Applies to IPv4 only.

IPv4 Destination IP **Mask Length** - Mask length of the destination IPv4 address ranging from 0 - 32. Applies to IPv4 only.

IPv6 Source IP Address - Source IPv6 address. Applies to IPv6 only.

IPv6 Source IP **Prefix Length** - Prefix length of the source IPv6 address ranging from 1 - 128. Applies to IPv6 only.

IPv6 Destination IP Address - Destination IPv6 address. Applies to IPv6 only.

IPv6 Destination IP **Prefix Length** - Prefix length of the destination IPv6 address ranging from 1 - 128. Applies to IPv6 only.

IPv4 **DSCP** - The Differentiated Services Code Point (DSCP) value in the IP header ranging from 0 - 63. Applies to IPv4 only.

IPv6 Traffic Class - The value for the IPv6 packet header's 8 bit priority ranging from 0 - 255. Applies to IPv6 only.

Source Layer 4 Port - Source Layer 4 port ranging from 1 - 65535.

Destination Layer 4 Port - Destination Layer 4 port ranging from 1 - 65535.

Policy Action - Use the **Policy Action** pull-down menu to select one of the following:

Deny - Drops ingress packets that conform to the **Replaced-CoS** or **Replaced-DSCP** policy setting. When selected, the **Replaced-CoS** and **Replaced-DSCP** fields become disabled.

Permit - Allows ingress packets that conform to the **Replaced-CoS** or **Replaced-DSCP** policy setting. When selected, the **Replaced-CoS** and **Replaced-DSCP** fields become enabled.

Replaced-CoS - CoS priority level ranging from 0 - 7. To set this parameter, click the **Replaced-CoS** radio button and enter the level.

Replaced-DSCP - DSCP priority level ranging from 0 - 63. To set this parameter, click the **Replaced-DSCP** radio button and enter the level. Applies to IPv4 only.

Rate Control Index - Rate Control index number for Committed Information Rate (CIR) ranging from 1 - 65535.

Note

This field must be pre-defined on the Rate Control Settings page - refer to "Rate Control Settings" on page 251 for more information.

8. Click **Add**.
   If you want to cancel the settings, click **Cancel**.
   After clicking **Add**, the policy entry is displayed in at the bottom of the table. If you do not see your new entry, you may need to navigate to another page of the table with the **First Page**, **Previous Page**, **Next Page**, and **Last Page** buttons located below the table. An example of a policy table entry is shown in Figure 94.

Policy Settings

| Policy type: | Add L2+IPv4 | Add IPv6 |

Free Policies : 197
Total Entries : 1   Delete All

Index	Classifier	Sequence	Deny/Permit	Replaced-CoS	Replaced-DSCP	Rate Control	Port List	Status	Action
2	Detail	1	Permit	0	Ignore	1	1	⊙ Enabled ○ Disabled	Modify Delete

Page 1/1 | First Page | | Previous Page | | Next Page | | Last Page | Page [ ] GO

Figure 94. Policy Settings Example

9. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Change a Policy Status

You can change the status of a policy to Enable or Disable. For example, if you want to retain the policy configuration for future use, but do not want to currently implement the policy, you can set the status to Disable.

To change the status of a policy, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
   The **Access Control Config** folder expands.

2. From the **Access Control Config** folder, select **Policy Settings**.
   An example of a policy entry on the Policy Settings page is displayed in Figure 94.

3. From the Policy Settings page, identify which policy whose status you want changed and click the **Enable** or **Disable** radio button in the Status column.

   Enable - If clicked, a message appears requesting whether you want to change the status to Enable. Click **OK** to enable or **Cancel** to cancel the action.

   Disable - If clicked, a message appears requesting whether you want to change the status to Disable. Click **OK** to enable or **Cancel** to cancel the action.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Modify a Policy

To modify the entries for a policy, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
   The **Access Control Config** folder expands.

2. From the **Access Control Config** folder, select **Policy Settings**.
   An example of a policy entry on the Policy Settings page is displayed in Figure 94 on page 247.

3. From the Policy Settings page, identify which policy you want to modify and click the **Modify** button in the Action column.
   The Modify Policy Settings page is displayed in Figure 95.

Figure 95. Modify Policy Page

4. Change the parameters as required. You cannot change the policy index number from this page.

> **Note**
> See "Create a Policy" on page 243 for definitions of each parameter.

5. Click **Apply**.
   The modified policy entry is displayed in the table at the bottom of the Policy Settings page.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Delete a Policy   To delete a policy entry, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
   The **Access Control Config** folder expands.

2. From the **Access Control Config** folder, select **Policy Settings**.
   An example of a policy entry on the Policy Settings page is displayed in Figure 94 on page 247.

3. From the Policy Settings page, identify which policy entry that you want to delete and click the **Delete** button in the Action column.
   The policy entry is deleted from the policy table.

   You can also use the **Delete All** button to delete all entries from the policy table.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

View Specific   To view the details of the packet settings for a specific policy, perform the
Classifier Details   following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
   The **Access Control Config** folder expands.

2. From the **Access Control Config** folder, select **Policy Settings**.
   The Policy Settings page is displayed. See Figure 94 on page 247 for an example of an entry in the Policy Settings page.

3. Click the **Detail** button under the Classifier column for classifier details of the policy you want to view. The Classifier Detail page appears. See Figure 96 on page 250.

Classifier Detail

Source MAC Address:	a4:54:86:12:00:00/24
Destination MAC Address:	45:2a:b5:00:00:00/24
802.1P Priority:	7
Ether Type:	806
VLAN ID:	10
IPv4 Source IP Address:	192.168.1.7/24
IPv4 Destination IP Address:	192.168.1.7/24
DSCP:	5
Protocol:	6
Source Layer 4 Port:	5
Destination Layer 4 Port:	10
Action:	Permit

Back

Figure 96. Classifier Detail Page

For a description of the displayed settings, refer to "Create a Policy" on page 243.

Rate Control Settings

The Rate Control Settings page lets you set the Committed Information Rate (CIR) for bandwidth restrictions. The CIR is the fixed bandwidth, in bits per second, for arriving or departing traffic.

The CIR can be used when different virtual connections share the same physical path, and certain connections require higher bandwidths than others. For example, a connection with a high proportion of video signals could be assigned a higher CIR than other connections requiring less bandwidth.

You can create, modify, or delete a rate control entry by following the procedures in the following sections:

❒ "Create a Rate Control Entry," next
❒ "Modify the Committed Rate" on page 252
❒ "Delete a Rate Control Entry" on page 253

Create a Rate Control Entry

To create a rate control entry, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
   The **Access Control Config** folder expands.

2. From the **Access Control Config** folder, select **Rate Control Settings**.
   The Rate Control Settings page is displayed. See Figure 97.

Figure 97. Rate Control Settings Page

3. Enter a number in the **Index** field within the range of 1 - 65535 to identify the rate control entry.

4. Enter a number in the **Committed Rate** field within the range of 1 - 15625 in 64 kbps to specify the bandwidth.

5. Click **Add**.
   The rate control entry is displayed at the bottom of the table. If you do not see your new entry, you may need to navigate to another page of the table with the **First Page**, **Previous Page**, **Next Page**, and **Last Page** buttons located below the table. An example of a rate control entry is shown in Figure 98.

Figure 98. Rate Control Settings Example

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Modify the Committed Rate

To modify the committed rate for a rate control entry, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
   The **Access Control Config** folder expands.

2. From the **Access Control Config** folder, select **Rate Control Settings**.
   The Rate Control Settings page is displayed. An example of the page with an entry is shown in Figure 98.

3. From the Rate Control page, identify which committed rate entry whose rate you want to modify and enter the new rate in the **64kbps x** field in the Committed Rate column.

4. Click the **Apply** button in the Action column.

5. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Delete a Rate Control Entry

To delete a rate control entry, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
   The **Access Control Config** folder expands.

2. From the **Access Control Config** folder, select **Rate Control Settings**.
   The Rate Control Settings page is displayed. An example of the page with an entry is shown in Figure 98 on page 252.

3. From the Rate Control page, identify which committed rate entry that you want to delete and click the **Delete** button in the Action column.
   The committed rate entry is deleted from the Committed Rate table.

   > **Note**
   >
   > You cannot delete a rate control entry if it is part of a policy's configuration. In this case, you must remove the rate control index from any policy's configuration that uses this index before you can delete the rate control entry.

   You can also use the **Delete All** button to delete all entries from the policy table.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Policy Database

The Policy Database page displays the status of the order that policies are applied to each port. You can order the display by Policy Index or Sequence number.

You can also display detailed information for each policy.

You can display a policy's sequence or detailed information by following the procedures in the following sections:

❒ "Display Policy Sequence," next
❒ "Display Specific Policy Information" on page 255

Display Policy Sequence

To display the policy sequence, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
   The **Access Control Config** folder expands.

2. From the **Access Control Config** folder, select **Policy Database**.
   The Policy Database page is displayed in Figure 99.
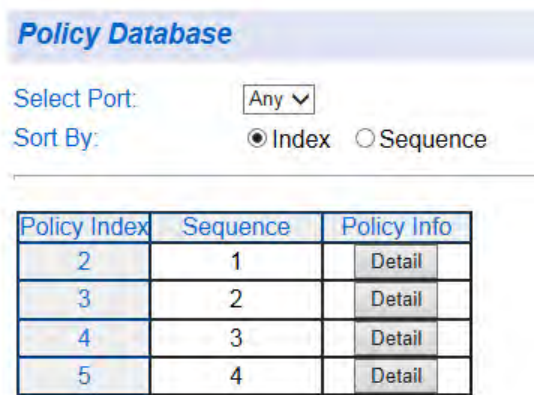
Figure 99. Policy Database Page

3. Select the switch port from the **Select Port** pull-down menu that you want to view.

4. Click either the **Index** or **Sequence** radio button to view the defined policies as follows:

   ■ **Index** - Select this radio button to view the defined Policies ordered by Policy Index.

   ■ **Sequence** - Select this radio button to view the sequence in which the Policies are applied.

Display Specific Policy Information

To display information for a specific policy, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
The **Access Control Config** folder expands.

2. From the **Access Control Config** folder, select **Policy Database**.
The Policy Database page is displayed in Figure 99 on page 254.

3. Select the switch port from the **Select Port** pull-down menu that you want to view.

4. Click the **Detail** button under the Policy Info column for details of the policy you want to view. The Policy Detail page appears. See Figure 100.

Policy Detail

Source MAC Address:	a4:54:86:12:00:00/24
Destination MAC Address:	45:2a:b5:00:00:00/24
802.1P Priority:	7
Ether Type:	806
VLAN ID:	10
IPv4 Source IP Address:	192.168.1.7/24
IPv4 Destination IP Address:	192.168.1.7/24
DSCP:	5
Protocol:	6
Source Layer 4 Port:	5
Destination Layer 4 Port:	10
Policy Sequence:	1
Action:	Permit
Replaced-CoS:	0
Replaced-DSCP:	Ignore
Rate Control Index:	1
Committed Rate:	64kbps
Port List:	1

Back

Figure 100. Policy Detail Page

For a description of the displayed settings, refer to "Create a Policy" on page 243.

5. To return to the Policy Database page, click the **Back** button.

Chapter 19
RMON

This chapter contains the following sections:

Overview

The RMON (Remote MONitoring) MIB is used with SNMP applications to monitor the operations of network devices. The switch supports the four RMON MIB groups listed here:

■ Statistic group— This group is used to view port statistics remotely with SNMP programs. For information about configuring a Statistics group, refer to "Port Statistics" on page 260.

■ History group— This group is used to collect histories of port statistics to identify traffic trends or patterns. For information about configuring a History group, refer to "Histories" on page 262.

■ Event group— This group is used with alarms to define the actions of the switch when packet statistic thresholds are crossed. For information about configuring an Event group, refer to "Events" on page 264.

■ Alarm group—This group is used to create alarms that trigger event log messages or SNMP traps when statistics thresholds are exceeded. For information about configuring an Alarm group, refer to "Alarms" on page 266.

Enable and Disable RMON

You can use your SNMP Network Management System (NMS) software and the RMON section of the MIB tree to view the RMON statistics, history and alarms associated with specific ports. Because RMON uses the SNMP agent for communicating with your NMS software, the SNMP Agent must be enabled, and the SNMP feature must be configured on your switch.

Because RMON works in conjunction with the SNMP agent, the SNMP agent must be enabled for the RMON feature to be active. See "User Interface Configuration" on page 45 for activating SNMP. For instructions on how to configure SNMP on your switch, refer to Chapter 16, "SNMPv1 and v2c" on page 209 or Chapter 17, "SNMPv3" on page 223.

Perform the following procedure to activate RMON:

1. From the main menu on the left side of the page, click the **RMON** folder.
   The **RMON** folder expands.

2. From the **RMON** folder, select **Global Settings**.
   The RMON Basic Settings Page is displayed. See Figure 101.
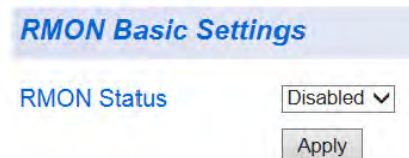
Figure 101. RMON Basic Settings Page

3. Select the **RMON Status** field and select one of the following choices from the pull-down menu:

   Enable: The RMON feature is active.

   Disable: The RMON feature is inactive.

   Note
   Ensure the that the SNMP agent is Enabled.
   ---

4. Click **Apply**.
   The RMON setting that you have selected is now active.

5. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Port Statistics

You can remotely view individual port statistics with RMON by using your SNMP NMS software and the RMON portion of the MIB tree.

Perform the following procedure to configure RMON port statistics for a specific port:

1. From the main menu on the left side of the page, click the **RMON** folder.

   The **RMON** folder expands.

2. From the **RMON** folder, select **Statistics**.

   The Ethernet Statistics Settings Page is displayed. See Figure 102.

Figure 102. Ethernet Statistics Settings Page

3. The following fields are listed:

   Index: This parameter specifies the ID number of the new group. The range is 1 to 65535.

   Port: This parameter specifies the port where you want to monitor the statistical information of the Ethernet traffic.

   Owner: This parameter is used to identify the person who created an entry. It is primarily intended for switches that are managed by more than one person and is an optional field.

4. Once you have configured the parameters, click **Add**.

   Your entry appears in the table at the bottom of the page. See Figure 103 on page 261.

—

Figure 103. Ethernet Statistics Configuration Example

5. If you want to configure RMON statistics for other ports, repeat Step 3 and Step 4.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Histories

RMON histories are snapshots of port statistics. They are taken by the switch at predefined intervals and can be used to identify trends or patterns in the numbers or types of ingress packets on the ports on the switch. The snapshots can be viewed with your SNMP NMS software with the history group of the RMON portion of the MIB tree.

A history group is divided into buckets. Each bucket stores one snapshot of statistics of a port. A group can have from 1 to 50 buckets. The more buckets in a group, the more snapshots it can store.

Perform the following procedure to configure RMON history:

1. From the main menu on the left side of the page, click the **RMON** folder.

    The **RMON** folder expands.

2. From the **RMON** folder, select **History**.

    The History Control Settings Page is displayed. See Figure 104.

Figure 104. History Control Settings Page

3. The following fields are listed:

    Index: This parameter specifies the ID number of the new group. The range is 1 to 65535.

    Port: This parameter specifies the port where you want to monitor the statistical information of the Ethernet traffic.

    Buckets Requested: This parameter defines the number of snapshots of the statistics for the port. Each bucket can store one

snapshot of RMON statistics. Different ports can have different numbers of buckets. The range is 1 to 50 buckets.

Interval: This parameter specifies how frequently the switch takes snapshots of the port's statistics. The range is 1 to 3600 seconds (1 hour). For example, if you want the switch to take one snapshot every minute on a port, you specify an interval of 60 seconds.

Owner: This parameter is used to identify the person who created an entry. It is primarily intended for switches that are managed by more than one person and is an optional field.

4. Once you have configured the parameters, click **Add**.

    Your entry appears in the table at the bottom of the page. See Figure 105.

Figure 105. History Control Configuration Example

5. If you want to configure additional RMON histories for other ports, repeat Step 3 and Step 4.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Events

An event specifies the action of the switch when the ingress packet activity on a port crosses a statistical threshold defined in an alarm. The choices are to log a message in the event log of the switch, send an SNMP trap to an SNMP workstation, or both. Since there are only three possible actions, and since events can be used with more than one alarm, you probably will not create more than three events - one for each of the three actions.

Perform the following procedure to configure RMON events.

1. From the main menu on the left side of the page, click the **RMON** folder.

   The **RMON** folder expands.

2. From the **RMON** folder, select **Event**.

   The RMON Event Settings Page is displayed. See Figure 106.

Figure 106. RMON Event Settings Page

3. The following fields are listed:

   Index: This parameter specifies the ID number of the new group. The range is 1 to 65535.

   Description: This parameter specifies a text description of the event that you are configuring.

   Type: This parameter specifies where to log the event when it occurs. The choices are to log a message in the event log of the switch, send an SNMP trap to the SNMP NMS software, or both.

Community: This parameter specifies the community where you want to send the SNMP trap.

Owner: This parameter is used to identify the person who created an entry. It is primarily intended for switches that are managed by more than one person and is an optional field.

4. Once you have configured the parameters, click **Add**.

   Your entry appears in the table at the bottom of the page. See Figure 107.

Figure 107. RMON Event Configuration Example

5. If you want to configure additional RMON events, repeat Step 3 and Step 4.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Alarms

RMON alarms are used to generate alert messages when packet activity on designated ports rises above or falls below specified threshold values. The alert messages can take the form of messages that are entered in the event log on the switch, traps that are sent to your SNMP NMS software, or both.

RMON alarms consist of two thresholds: a rising threshold and a falling threshold. The alarm is triggered if the value of the monitored RMON statistic of the designated port exceeds the rising threshold. The response of the switch is to enter a message in the event log, send an SNMP trap, or both. The alarm is reset if the value of the monitored statistic drops below the falling threshold.

The frequency with which the switch samples the thresholds of an alarm against the actual RMON statistic is controlled by a time interval parameter. You can adjust this interval for each alarm.

Here are the three components that comprise RMON alarms:

❐ RMON statistics group: A port must have an RMON statistics group configured if it is to have an alarm. When you create an alarm, you specify the port to which it is to be assigned, not by the port number, but rather by the ID number of the port's statistics group. (As explained in "Port Statistics" on page 260, statistics groups are also used to remotely view port statistics in the RMON portion of the MIB tree.)

❐ RMON event: An event specifies the action of the switch when the ingress packet activity on a port crosses a statistical threshold defined in an alarm. The choices are to log a message in the event log of the switch, send an SNMP trap to an SNMP workstation, or both. Since there are only three possible actions, and since events can be used with more than one alarm, you probably will not create more than three events.

❐ Alarm: The last component is the alarm itself. It defines the port statistic to be monitored and the rising and falling thresholds that trigger the switch to perform an event. The thresholds of an alarm can have the same event or different events. The switch supports up to eight alarms.

Perform the following procedure to configure RMON alarms.

1. From the main menu on the left side of the page, click the **RMON** folder.

   The **RMON** folder expands.

2. From the **RMON** folder, select **Alarm**.

The RMON Alarm Settings Page is displayed. See Figure 108.

Figure 108. RMON Alarm Settings Page

3. The following fields are listed:

Index: This parameter specifies the ID number of the new group. The range is 1 to 65535.

Interval: This parameter specifies the time (in seconds) over which the data is sampled. Its range is 1 to 2147483647 seconds.

Variable: This parameter specifies the RMON MIB object that the event is monitoring.

Sample type: This parameter defines the type of change that has to occur to trigger the alarm on the monitored statistic. There are two choices from the pull-down menu - **Delta value** and **Absolute value**. The Delta setting compares a threshold against the difference between the current and previous values of the statistic, while the Absolute setting compares a threshold against the current value of the statistic.

Rising Threshold: This parameter specifies a specific value or threshold level of the monitored statistic. When the value of the monitored statistic becomes greater than this threshold level, an alarm event is triggered. The parameter's range is 1 to 2147483647.

Falling Threshold: This parameter specifies a specific value or threshold level of the monitored statistic. When the value of the

monitored statistic becomes less than this threshold level, an alarm event is triggered. The parameter's range is 1 to 2147483647.

Rising Event Index: This parameter specifies the event index for the rising threshold. Its range is 1 to 65535. This field is mandatory and must match an Event Index that you previously entered in "Events" on page 264.

Falling Event Index: This parameter specifies the event index for the falling threshold. Its range is 1 to 65535. This field is mandatory and must match an Event Index that you previously entered in "Events" on page 264.

Owner: This parameter is used to identify the person who created an entry. It is primarily intended for switches that are managed by more than one person and is an optional field.

4. Once you have configured the parameters, click **Apply**.

Your entry appears in the table at the bottom of the page. See Figure 109.

Figure 109. RMON Alarm Configuration Example

5. If you want to configure additional RMON alarms, repeat Step 3 and Step 4.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Chapter 20
Voice VLAN

This chapter contains a description of the AT-GS950/16 switch's Voice VLAN feature and the procedures to create, modify, and delete a voice VLAN configuration. This chapter contains the following sections:

❑ "Overview" on page 270
❑ "General Guidelines" on page 273
❑ "Configuration" on page 274
❑ "OUI Setting" on page 277

Note
To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Overview

The AT-GS950/16 Voice VLAN feature is specifically designed to maintain high-quality, uninterrupted voice traffic through the switch. When talking on a Voice over IP (VoIP) phone, a user expects to have no interruptions in the conversation and excellent voice quality. The Voice VLAN feature can be configured to meet these requirements.

CoS with Voice VLAN

The Voice VLAN CoS parameter maintains the voice quality between the ingress and egress ports of the AT-GS950/16 switch. CoS must be enabled for the Voice VLAN CoS priority to take effect. The CoS priority level that you configure is applied to voice traffic on all ports of the voice VLAN.

Normally, most (non-Voice) Ethernet traffic traverses the AT-GS950/16 switch through lower-order egress queues. To avoid delays and interruptions in the voice data flow, the CoS priority level assigned to the voice VLAN should be mapped to a higher-order queue, and the scheduling algorithm should be set to Strict Priority. These settings ensure that the voice data packets are processed before other types of data so that the voice quality is maintained as the voice data passes through the AT-GS950/16 switch.

Note

For more information about how to configure these CoS parameters, see "Mapping CoS Priorities to Egress Queues" on page 198 and "Queue Scheduling Algorithm" on page 203.

Organization Unique Identifier (OUI)

Each IP phone manufacturer can be identified by one or more Organization Unique Identifiers (OUIs). An OUI is three bytes long and is usually expressed in hexadecimal format. It is imbedded into the first part of each MAC address of an Ethernet network device. You can find the OUI of an IP phone in the first three complete bytes of its MAC address. Typically, you will find that all of the IP phones you are installing have the same OUI.

The AT-GS950/16 switch identifies a voice data packet by comparing the OUI information in the packet's source MAC address with an OUI table that you configure when you initially set up the voice VLAN. This is important when the Auto-Detection feature is set for a dynamic voice VLAN port.

Note

See "Dynamic Auto-Detection vs Static Ports" on page 271 for more information about the Auto-Detection feature.

When you are configuring the voice VLAN parameters, you must enter the complete MAC address of at least one of your IP phones. An "OUI Mask" is automatically generated and applied by the AT-S114 management software to yield the manufacturer's OUI. If the OUI of the remaining phones from that manufacturer is the same, then no other IP phone MAC addresses need to be entered into the configuration.

However, it is possible that you can find more than one OUI from the same manufacturer among the IP phones you are installing. It is also possible that your IP phones are from two or more different manufacturers, in which case, you will find different OUIs for each manufacturer. If you identify more than one OUI among the IP phones being installed, then one MAC address representing each individual OUI must be configured in the voice VLAN. You can enter a total of 10 OUIs.

Dynamic Auto-Detection vs Static Ports

Prior to configuring the voice VLAN, you must configure a tagged VLAN which is the basis for the voice VLAN configuration. The VLAN must be configured with one or more tagged or untagged ports that will serve as the voice VLAN uplink/downlink. By default, a tagged or untagged port is a static member of a tagged VLAN.

> **Note**
> See "Create a Tagged VLAN" on page 166 for more information about configuring a tagged VLAN with "Not Member" and Static ports.

The ports that you choose to configure as dynamic Auto-Detection ports must be connected directly to an IP phone. When you initially define the ports of a tagged VLAN for your voice VLAN configuration, they must be configured as a "Not Member" ports. The "Not Member" ports are eligible to dynamically join the voice VLAN when voice data is detected with a pre-defined OUI in the source MAC address. The port will leave the voice VLAN after a specified timeout period. This port behavior is configured with the voice VLAN Auto-Detection feature.

> **Note**
> See "Organization Unique Identifier (OUI)" on page 270 for more information concerning OUIs.

For the Auto-Detection feature to function, your IP phone(s) must be capable of generating 802.1Q packets with imbedded VLAN ID tags. You must manually configure your IP phone(s) for the same VLAN ID as the AT-GS950/16 switch's voice VLAN ID. When voice data is detected on one of the "Not Member" ports, the packets from the IP phone will contain the voice VLAN ID so they are switched within the AT-GS950/16 switch's voice VLAN.

One or more ports in your voice VLAN must be configured as Static tagged or untagged members. Static VLAN members are permanent member ports of the voice VLAN, and there is no dependency on the configuration of the devices connected to the ports. These ports might be connected to other voice VLAN network nodes, such as other Ethernet switches, a telephone switch, or a DHCP server. The voice VLAN Auto-Detection feature cannot be enabled on Static tagged or tagged ports.

Note

Any Static tagged members of the voice VLAN are required to have the port VLAN ID (PVID) configured to be the same as the voice VLAN ID. This insures that all untagged packets entering the port are switched within the voice VLAN as the voice data passes through the AT-GS950/16 switch.

If the IP phone(s) that you are installing cannot be configured with a VLAN ID, then the switch ports should be configured as Static tagged ports within the voice VLAN.

Note

Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) is *not* supported on the AT-GS950/16 switch. Each IP phone that is VLAN aware should be manually configured for the VLAN ID that matches your AT-GS950/16 voice VLAN ID. Each of the AT-GS950/16 voice VLAN ports connected to an IP phone should be configured as "Not Member" ports of the tagged VLAN.

General Guidelines

Here is a summary of the rules to observe when you create a voice VLAN:

- One voice VLAN can be configured on the switch at any time.

- A voice VLAN is based on a pre-defined tagged VLAN.

- The voice VLAN Auto-Detection feature can only be enabled on ports that are initially defined as non-members of the tagged VLAN.

- On ports that are configured for the voice VLAN Auto-Detection feature, each IP phone must be manually configured per the manufacturer's instructions for the VLAN ID that matches your AT-GS950/16 voice VLAN ID.

- Member ports of a tagged VLAN are static and cannot have the voice VLAN Auto-Detection feature enabled.

- IP phones that are not VLAN aware should be connected to Static tagged ports of the voice VLAN.

- The voice VLAN uplink/downlink port(s) must be configured as Static tagged or tagged ports.

- Any Static tagged members of the voice VLAN are required to have the port VLAN ID (PVID) configured to be the same as the voice VLAN ID.

- The Organization Unique Identifier (OUI) is configured by entering an IP phone's MAC address into the configuration.

- Only one MAC address representing each unique OUI can be configured at one time.

- Up to 10 IP phone MAC addresses/OUIs can be configured at one time.

- Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) is not supported on the AT-GS950/16 switch.

Configuration

Prior to configuring your voice VLAN, you must first configure a tagged VLAN. This VLAN will be used as a basis for your voice VLAN.

Note

See "Create a Tagged VLAN" on page 166 for more information about configuring a tagged VLAN with Not Member and Static tagged ports.

The procedure described in this section allows you to configure a voice VLAN on the AT-GS950/16 switch.

To configure a voice VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Voice VLAN**. The **Voice VLAN** folder expands.

2. From the **Voice VLAN** folder, select **Voice VLAN Settings**. The AT-GS950/16 Voice VLAN Settings Page is displayed. See Figure 110 for a partial view of this page.
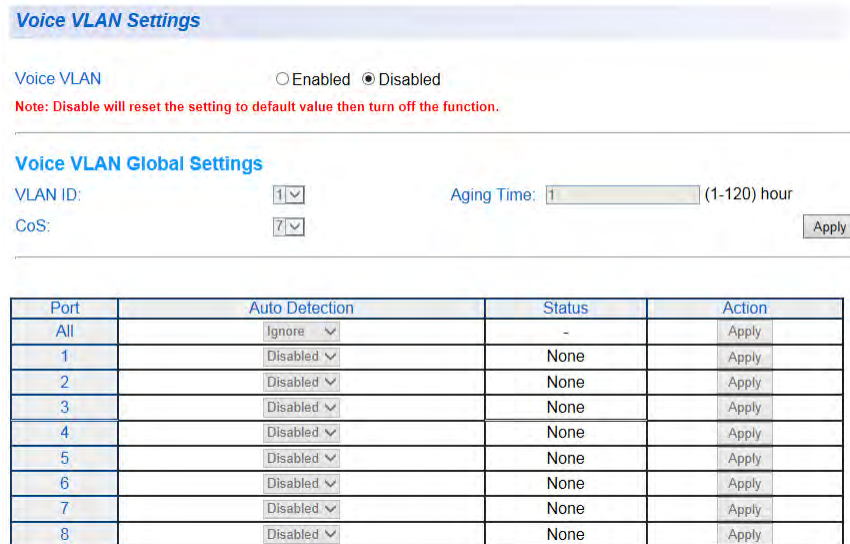
Figure 110. AT-GS950/16 Voice VLAN Settings Page

Before entering any configuration parameters, you must enable the voice VLAN to activate the other parameter fields in the Voice Vlan Global Settings section which are greyed out.

3. From the **Voice VLAN** field at the top of the page, select one of the following choices by clicking one of the radio buttons:

> **Enabled** - The voice VLAN feature is active. The other parameter fields in the voice VLAN Global Settings section become active and are eligible for data to be entered.

> **Disabled** - The voice VLAN feature is inactive. The other parameter fields in the voice VLAN Global Settings section become inactive and are grayed out so that data cannot be entered.

4. In the voice VLAN Global Settings section, enter the configuration information for the following parameters:

> **VLAN ID** - This parameter is the tagged VLAN ID that has been configured in "Tagged VLAN Configuration" on page 166 that you intend for the voice VLAN. It is a pull-down menu showing the tagged VLAN IDs that have been defined.

> **Aging Time** - This parameter indicates the amount of time, in hours, after the last IP phone's OUI was received on a port, after which this port will be removed from the voice VLAN. The range is 1 to 120 hours.

> **CoS** - This parameter is the CoS priority level assigned to the voice data packets received on each voice VLAN port.

Note

For the **CoS** priority to be effective, QoS must be **Enabled**. See "Mapping CoS Priorities to Egress Queues" on page 198 for information about enabling the QoS feature.

---

5. Click **Apply**. The values in the Voice VLAN Global Settings section take effect.

6. In the table at the bottom of the page, The voice VLAN **Auto Detection** status is defined. From the **Auto Detection** column, select one of the port rows and then one of the following choices from the pull-down menu:

> **Ignore** - This parameter indicates that the setting in the **All** row does not apply to the **Dynamic Vlan Status** field. In other words, each port is set individually.

> **Enabled** - The voice VLAN **Auto Detection** feature is activated for the port row selected.

> **Disabled** - The voice VLAN **Auto Detection** feature is de-activated for the port row selected.

Note

The voice VLAN Auto-Detection feature can only be enabled on "Not Member" ports of the voice VLAN. Member ports cannot have the voice VLAN Auto-Detection feature enabled. The **Status** column displays **Static** for the member ports. See "Dynamic Auto-Detection vs Static Ports" on page 271 for more information.

7. Click **Apply** in the **Action** column of the table.

8. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

OUI Setting

You can create and delete Voice VLAN OUI Settings by following the procedures in these sections:

- ❏ "Create OUI Setting"
- ❏ "Modify OUI Setting" on page 278
- ❏ "Delete OUI Setting" on page 278

Create OUI Setting

To create a Voice OUI configuration, perform the following procedure:

1. From the main menu on the left side of the page, select **Voice VLAN**. The **Voice VLAN** folder expands.

2. From the **Voice VLAN** folder, select **Voice VLAN OUI Settings**. The Voice VLAN OUI Settings Page is displayed. See Figure 111.

Figure 111. Voice VLAN OUI Settings Page

3. Enter a text description that helps you identify the manufacturer's OUI in the **User Defined OUI - Description** field. This parameter can be up to 20 characters in length.

4. Enter the MAC address in the **User Defined OUI - Telephony OUI** field of one of the IP phones with the manufacturer's OUI described in Step 3.

5. Click **Add**. The new OUI entry is displayed in the table at the bottom of the page.

6. If you find more than one OUI among the IP phones you are installing, enter one MAC address that represents each individual OUI by following Step 3 through Step 5. You can enter a total of 10 OUIs.

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Modify OUI Setting

To modify or delete an OUI, it must be first be deleted and then re-entered by following the procedure in "Create OUI Setting" on page 277.

Delete OUI Setting

To delete an OUI, perform the following procedure:

1. From the main menu on the left side of the page, select **Voice VLAN**. The **Voice VLAN** folder expands.

2. From the **Voice VLAN** folder, select **Voice VLAN OUI Settings**. The Voice VLAN OUI Settings Page is displayed. See Figure 111 on page 277.

3. To delete a specific OUI that had already been entered in the table at the bottom of the page, click on **Delete** in the **Action** column of the table. The specific OUI will be deleted from the table.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Chapter 21
Security

This chapter contains information about the Port-based security features and the procedures for setting this feature.

This chapter includes the following sections:

❑ "Port Access Control" on page 280
❑ "RADIUS Client" on page 286
❑ "TACACS+" on page 289
❑ "Dial-in User— Local Authentication" on page 292
❑ "Destination MAC Filter" on page 295

> **Note**
> To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Port Access Control

This section contains information and configuration procedures for the Port-based Access Control. The following information is provided:

❑ "Port Access Control Overview"

❑ "Port Access Control Configuration" on page 281

> **Note**
>
> After configuring the Port-based Network Access Control, you can choose to use the local authentication server in the AT-S114 for 802.1x authentication, a remote RADIUS server for 802.1x authentication, or TACACS+. See "Dial-in User— Local Authentication" on page 292, "RADIUS Client" on page 286, or "TACACS+" on page 289.

Port Access Control Overview

Port-based Network Access Control (IEEE 802.1x) is used to control who can send traffic through and receive traffic from a switch port. With this feature, the switch does not allow an end node to send or receive traffic through a port until the user of the node logs on by entering a user name and password.

This feature can prevent an unauthorized individual from connecting a computer to a port or using an unattended workstation to access your network resources. Only those users to whom you have assigned a user name and password are able to use the switch to access the network.

This feature can be used with one of the following authentication methods:

■ The RADIUS authentication protocol requires that a remote RADIUS server is present on your network. The RADIUS server performs the authentication of the user name and password combinations. See "Port Access Control Configuration" on page 281 and "RADIUS Client" on page 286 for more information.

> **Note**
>
> RADIUS with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server for this feature.

■ The TACACS+ authentication protocol requires that a TACACS+ server is present on your network. The TACACS+ server performs the authentication of the user name and password combinations. Refer to "Port Access Control Configuration" on page 281 and "TACACS+" on page 289 for more information.

■ The Dial-in User (local) authentication method allows you to set up the authentication parameters internally in the switch without an external server. In this case, the user name and password combinations are entered with an optional VLAN when they are defined. Based on these entries, the authentication process is done locally by the AT-S114 using a standard EAPOL transaction.

Port Access Control Configuration

To configure port-based access control, perform the following procedure:

1. Select the **Security** folder from the main menu on the left side of the page.
   The **Security** folder expands.

2. From the **Security** folder, select **Port Access Control**. The Port Access Control Settings Page is displayed. See Figure 112.

Figure 112. Port Access Control Settings Page

3. Configure the following parameters as required:

   NAS ID - This parameter assigns an 802.1x identifier to the switch that applies to all ports. The NAS ID can be up to 16 characters. Valid characters are 0 to 9, a to z, and A to Z. Spaces are allowed. Specifying an NAS ID is optional.

   Port Access Control - This parameter enables or disables Port Access Control. Select one of the following choices from the pull-down menu:

   Enable: The Port Access Control feature is activated.

   Disable: The Port Access Control feature is de-activated.

   Authentication Method - This parameter indicates the authentication method used by the switch. Select one of the following choices:

   RADIUS: This parameter configures port security for remote authentication. After completing Step 4 through Step 6, you must configure the "RADIUS Client" on page 286.

TACACS+: This parameter configures port security for TACACS+ authentication. After completing Step 4 through Step 6, you must configure the "TACACS+" on page 289.

Local: This parameter configures port security for local authentication. After completing Step 4 through Step 6, you must configure the parameters for "Dial-in User— Local Authentication" on page 292.

4. Click **Apply** when you are finished configuring the parameters.

5. To set the advanced configuration parameters, click **Settings**. The Port Access Control Settings page is expanded. See Figure 113.

Figure 113. Expanded Port Access Control Settings Page

6. Set the following parameters as needed:

Port: This parameter specifies the port being configured for authentication.

Authentication Mode: This parameter specifies the port-based authentication mode. The pull-down menu choices are as follows:

802.1x: 802.1x is specified as the authentication mode. This setting applies to configuration for RADIUS, TACACS+, or Dial-

In User authentication. For configuration information, see "RADIUS Client" on page 286, "TACACS+" on page 289, or "Dial-in User— Local Authentication" on page 292.

MAC Based: MAC Based authentication mode is specified. For more information about configuring this mode, see "Destination MAC Filter" on page 295.

Port Control: This parameter specifies the port-based authentication role. The pull-down menu choices are as follows:

Forced Unauthorized: This parameter sets the port to the 802.1x authenticator role, in the unauthorized state. Although the ports are in the authenticator role, the switch blocks all authentication on the ports, which means that no clients can log on and forward packets through them.

Auto: Sets the port to the 802.1x port-based authenticator role. Ports begin in the unauthorized state, forwarding only EAPOL frames, until a client has successfully logged on.

Forced Authorized: Sets a port to Forced-Authorized port control. Ports that are set to the force-authorized state transition to the authorized state without any authentication exchanges required. The ports transmit and receive traffic normally without 802.1x based authentication of the clients.

Re-authentication Status: This parameter activates or de-activates the reauthentication on the authenticator ports.

Enabled: Configures the port to activate reauthentication on the authenticator ports. The clients must periodically reauthenticate according to the time interval set with the Re-authentication Period.

Disabled: Configures the port to remove reauthentication from authenticator ports so that clients do not have to periodically reauthenticate after the initial authentication. Reauthentication is still required if there is a change to the status of the link between a client and the switch, or the switch is reset or power cycled.

Control Direction: The port authentication is set to **"Both"** meaning both transmit and receive packets are affected. You cannot change this parameter.

Supplicant Mode: This parameter specifies if one or more supplicants can be authenticated on a port.

Single: The port is set to permit only one supplicant to log on and forwards only the traffic of that supplicant. After one supplicant has logged on, the port discards packets from any other supplicant.

Multiple: The port is set to permit multiple clients on an authenticator port. An authenticator mode forwards packets from all clients once one client has successfully logged on.

Piggyback Mode: This mode is used in conjunction with the Multiple Supplicant Mode. This mode is typically used in situations where you want to add 802.1x port-based network access control to a switch port that is supporting multiple clients, but do not want to create individual accounts for all the clients on the RADIUS server. After one client has successfully logged on, the port permits the other clients to piggy-back onto the initial client's log on, so that they can forward packets through the port without being authenticated.

Enabled: The Piggyback Mode is enabled.

Disabled: The Piggyback Mode is disabled.

VLAN Assignment: This parameter enables the VLAN assignment that you select with the **Guest VLAN ID** parameter. Choose from the following:

Enabled: The VLAN Assignment is enabled.

Disabled: The VLAN Assignment is disabled.

Secure VLAN: This field is inactive.

Guest VLAN ID: This parameter specifies the VLAN ID that is designated as a Guest VLAN. The range is 0 to 4093, where 0 is disabled.

When a supplicant account is created on the RADIUS server, a VLAN identifier must be entered along with a user name and password combination or MAC address information. If the switch receives a valid VLAN ID or VLAN name from the RADIUS server, it moves the authenticator port to the designated Guest VLAN and changes the port to the authorized state.

Transmission Period: Sets the switch-to-client retransmission time for EAP request frames. The range is 1 to 65535 seconds.

Quiet Period: Sets the number of seconds that authenticator ports wait after a failed authentication before accepting authentication requests again. The range is 1 to 65535 seconds.

Supplicant Timeout: Sets the switch-to-client retransmission time for EAP request frames. The range is 1 to 65535 seconds.

Maximum Request: Specifies the maximum number of times authenticator ports transmit EAP Request packets to clients before timing out authentication sessions. The range is 1 to 10.

Re-authentication Period: Specifies the time interval for reauthentication of clients on an authenticator port. The range is 1 to 65535 seconds

Server Timeout: Sets the length of time the switch waits for a response from the authentication server. The range is 1 to 65535 seconds.

7. To permanently save your changes, select **Save Settings to Flash** from the main menu on the left side of the page.

RADIUS Client

You can use the RADIUS client with 802.1x port-based access control to authenticate which packets are forwarded through the switch. This section explains how to configure the RADIUS client on the switch and contains the following sections:

❒ "RADIUS Overview"
❒ "General Guidelines"
❒ "RADIUS Client Configuration" on page 287
❒ "RADIUS Accounting Status" on page 288

> **Note**
>
> To activate the RADIUS feature, you must also configure the port-based network access control feature. See "Port Access Control" on page 280.

> **Note**
>
> To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

RADIUS Overview

RADIUS (Remote Authentication Dial In User Services) is an authentication protocol for enhancing the security of your network. The protocol transfers the task of authenticating network access from a network device to an authentication protocol server.

The AT-S114 Management software comes with RADIUS client software. You can use the client software together with 802.1x port-based access control. To control which end users and end nodes can send packets through the switch, you can configure the RADIUS client using "RADIUS Client Configuration" on page 287.

General Guidelines

The following guidelines apply when using the RADIUS protocol.

❒ You must install RADIUS server software on a network server or management station. Authentication protocol server software is not available from Allied Telesis.

❒ The RADIUS server must communicate with the switch through a port that is an untagged member of the Default VLAN and is configured for Forced-Authorized (802.1x) port control.

❒ If the RADIUS server is on a different subnet from switch, be sure to specify a System Default Gateway in the IP Setup Page, so that the switch and server can communicate with each other via the gateway.

See "Configuration of IPv4 Address, Subnet Mask and Gateway Address" on page 32.

❒ You must specify the user name and password combinations when configuring the RADIUS server software on the authentication server.

Note

This guide does not explain how to configure RADIUS server software. Refer to the documentation that comes with the RADIUS server software for instructions.

❒ You must activate the RADIUS client software on the switch using the AT-S114 Management Software and configure the settings. This is explained in "Port Access Control Configuration" on page 281 and "RADIUS Client Configuration".

❒ For more information about the RADIUS authentication protocol, refer to the RFC 2865 standard.

RADIUS Client Configuration

To configure the RADIUS client, perform the following procedure:

1. From the main menu on the left side of the page, select the **Security** folder.
   The **Security** folder expands.

2. From the **Security** folder, select **RADIUS**.
   The RADIUS Page is displayed. See Figure 114.

Figure 114. RADIUS Page

3. Enter the RADIUS server's IP address using one of the **Server IP Address** fields:

   For an IPv4 address, click **IPv4**, then enter the address using xxx.xxx.xxx.xxx format.

   For an IPv6 address, click **IPv6**, then enter the address using xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx hexadecimal format.

4. Type the port number in the **Server Port** field that you want to assign to UDP.
   You may only assign one port number to this parameter.

5. Type the port number in the **Accounting Port** field that you want to assign to UDP.
   You may only assign one port number to this parameter.

6. To specify the server's encryption key, enter the encryption key in the **Shared Secret** field.

7. Click **Apply** to save your changes.

8. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

RADIUS Accounting Status

You can enable or disable RADIUS Accounting Request packets. These packets contain an Account-Status Type attribute that provides information related to a user's network access.

To enable or disable RADIUS Accounting Status, perform the following procedure:

1. From the main menu on the left side of the page, select the **Security** folder.
   The **Security** folder expands.

2. From the **Security** folder, select **RADIUS Accounting Settings**.
   The RADIUS Accounting Global Settings Page is displayed. See Figure 115.

Figure 115. RADIUS Accounting Global Settings Page

3. To enable RADIUS Accounting Status, select **Enabled** from the **RADIUS Accounting Status** drop-down menu.
   To disable RADIUS Accounting Status, select **Disabled** from the **RADIUS Accounting Status** drop-down menu.

4. Click **Apply** to save your changes.

5. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

TACACS+

You can use the TACACS+ client with 802.1x port-based access control to authenticate which packets are forwarded through the switch. This section explains how to configure TACACS+ on the switch and contains the following sections:

❐ "TACACS+ Overview"

❐ "General Guidelines"

❐ "TACACS+ Configuration" on page 290

> **Note**
> To activate the TACACS+ feature, you must also configure the port-based network access control feature. See "Port Access Control" on page 280.

> **Note**
> To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

TACACS+ Overview

TACACS+ (Terminal Access Controller Access-Control System Plus) is an authentication protocol for enhancing the security of your network. The protocol transfers the task of authenticating network access from a network device to an authentication protocol server.

TACACS+ is similar to RADIUS, however, certain differences are as follows:

■ TACACS+ separates authentication and authorization in a user profile, whereas, RADIUS combines authentication and authorization.

■ TACACS uses TCP instead of UDP.

The AT-S114 Management software comes with TACACS+ client software. You can use the TACACS+ software together with 802.1x port-based access control. To control which end users and end nodes can send packets through the switch, you can configure the TACACS+ client using "TACACS+ Configuration" on page 290.

General Guidelines

The following guidelines apply when using the TACACS+ protocol.

❐ You must install TACACS+ server software on a network server or management station. Authentication protocol server software is not available from Allied Telesis.

❐ The TACACS+ server must communicate with the switch through a port that is an untagged member of the Default VLAN and is configured for Forced-Authorized (802.1x) port control.

❐ If the TACACS+ server is on a different subnet from switch, be sure to specify a System Default Gateway in the IP Setup Page, so that the switch and server can communicate with each other via the gateway. See "Configuration of IPv4 Address, Subnet Mask and Gateway Address" on page 32.

❐ You must specify the user name and password combinations when configuring the TACACS+ server software on the authentication server.

Note

This guide does not explain how to configure TACACS+ server software. Refer to the documentation that comes with the TACACS+ server software for instructions.

❐ You must activate the TACACS+ software on the switch using the AT-S114 Management Software and configure the settings. This is explained in "Port Access Control Configuration" on page 281 and "TACACS+ Configuration".

TACACS+ Configuration

To configure TACACS+, perform the following procedure:

1. From the main menu on the left side of the page, select the **Security** folder.
   The **Security** folder expands.

2. From the **Security** folder, select **TACACS+**.
   The TACACS+ Page is displayed. See Figure 116.

Figure 116. TACACS+ Page

3. Enter the TACACS+ server's IP address using one of the **Server IP Address** fields:

   For an IPv4 address, click **IPv4**, then enter the address using xxx.xxx.xxx.xxx format.

For an IPv6 address, click **IPv6**, then enter the address using xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx hexadecimal format.

4. Type the port number in the **Server Port** field that you want to assign to TCP.
   You may only assign one port number to this parameter.

5. Type the timeout interval, in seconds, for the TACACS+ server in the **Timeout** field. This parameters determines the interval that the switch waits for responses from the TACACS+ server before declaring a timeout.

6. To specify the server's encryption key, enter the encryption key in the **Shared Secret** field.

7. Click **Apply** to save your changes.

8. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Dial-in User— Local Authentication

The Dial-in User feature provides the local authentication server for port security when a remote (RADIUS) or TACACS+ server is not available. This section includes the following:

❐ "Dial-In User Overview"

❐ "Dial-in User Configuration"

> **Note**
> To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Dial-In User Overview

The Dial-in User (local) authentication method allows you to set up 802.1x authentication parameters internally in the switch. In this case, the user name and password combinations are entered with an optional VLAN when they are defined. Based on these entries, the authentication process of a supplicant is done locally by the AT-S114 Management software using a standard EAPOL (EAP over LAN) transaction.

Dial-in User Configuration

The procedures in this section describe how to create, delete, and modify dial-in users. See the following procedures:

❐ "Add a Dial-in User"

❐ "Modify a Dial-in User" on page 294

❐ "Delete a Dial-in User" on page 294

Add a Dial-in User

To set up a user's dial-in access, do the following:

1. From the main menu on the left side of the page, select the **Security** folder.
    The **Security** folder expands.

2. From the **Security** folder, select **Dial-in User**.
    The Dial-in User page is displayed. See Figure 117 on page 293.

Figure 117. Dial-In User Page

3. In the **User Name** field, type a name for the user.

4. In the **Password** field, type a password for the user.

5. In the **Dynamic VLAN** field, enter the VID of the VLAN which you will allow the user to access. If you enter 0, this field will be ignored.

6. Click the **Add** button.
    The Dial-in User page is refreshed. See Figure 118.

Figure 118. Dial-In User Page Example

7. To permanently save these settings in the configuration file, select **Save Settings to Flash** from the main menu to permanently save your changes.

Modify a Dial-in User

To modify the settings for a dial-in user, do the following:

1. From the main menu on the left side of the page, select the **Security** folder.

   The **Security** folder expands.

2. From the **Security** folder, **Dial-in User**.

   The Dial-in User page is displayed. See Figure 117 on page 293.

3. In the list of dial-in users, highlight the user you want to modify.

   The user's information is displayed in fields above.

4. In the **Password** field, enter the new password.

5. In the **Dynamic VLAN** field, enter the new VID of the VLAN which you want the user to access.

6. Click **Apply**.

7. To permanently save these settings in the configuration file, select **Save Settings to Flash** from the main menu to permanently save your changes.

Delete a Dial-in User

To delete a dial-in user, perform the following procedure:

1. From the main menu on the left side of the page, select the **Security** folder.

   The Security folder expands.

2. From the **Security** folder, **Dial-in User**.

   The Dial-in User page is displayed. See Figure 117 on page 293.

3. In the list of dial-in users, highlight the user you want to delete.

4. Click **Delete**.
   The user name, password, and dynamic VLAN are removed from the Dial-in User page.

5. To permanently save these settings in the configuration file, select **Save Settings to Flash** from the main menu to permanently save your changes.

Destination MAC Filter

This section contains an explanation of the Destination MAC Filter feature, as well a procedure for configuring it. This section includes the following information:

❏ "Destination MAC Filter Overview"

❏ "Destination MAC Filter Configuration"

❏ "Delete Destination MAC Filter" on page 296

Destination MAC Filter Overview

The Destination MAC Filter feature prevents the AT-GS950/16 switch from forwarding packets to a specified device. On the Destination MAC Filter page of the AT-S114 Management software, enter the MAC address of the device that you want to filter.

After the switch receives a packet, it examines the destination MAC address of the packet. If the destination MAC address matches a MAC address set in the filter, the software prevents the switch from forwarding it and drops the packet.

You may want to block access to a device within your organization. For instance, you may not want users on the Sales group switch to have access to a server on the Accounting group switch. You can enter the MAC address of the Accounting server as a destination MAC address filter on the Sales group switch. When a packet destined for the Accounting server is received by the Sales group switch, the switch drops the packet.

The Destination MAC Filter is a subset of the static MAC address. For more information about MAC addresses, see Chapter 10, "Overview" on page 130.

Destination MAC Filter Configuration

To set the MAC address in the Destination MAC Filter, perform the following procedure:

1. From the main menu on the left side of the page, select the **Security** folder.

    The **Security** folder expands.

2. From the **Security** folder, select **Destination MAC Filter**.

    The Destination MAC Filter Page is displayed. See Figure 119 on page 296.
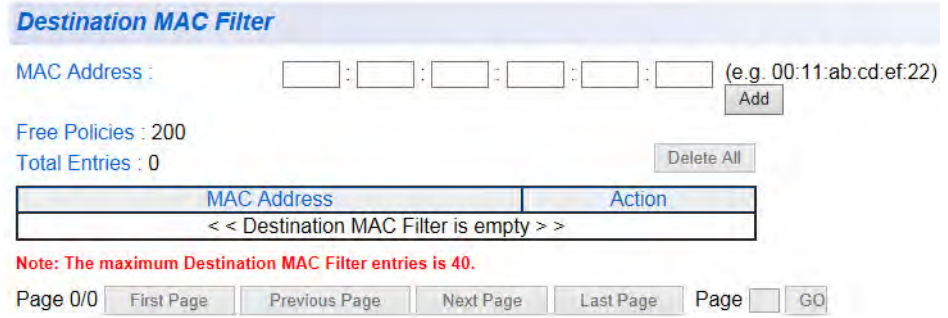
Figure 119. Destination MAC Filter Page

3. To enter the MAC address that you want filtered, enter the MAC address into the **MAC Address** field.

4. Click the **Add** button to save your entry. See Figure 120.
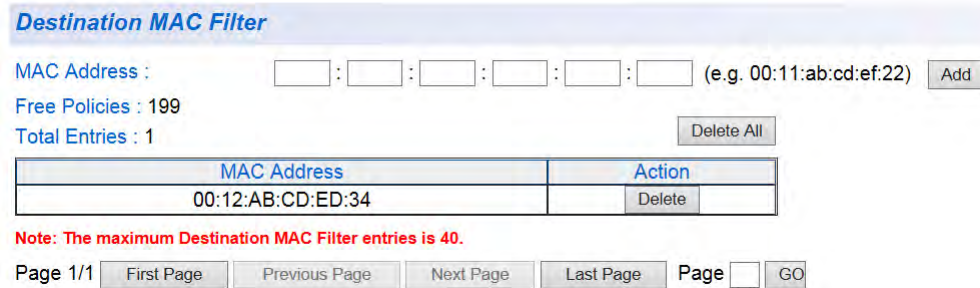
Figure 120. Destination MAC Filter Page Example

5. After you have configured a destination MAC address, the Destination MAC Filter Page is updated with the MAC address.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Delete Destination MAC Filter

To delete a MAC address from the Destination MAC Filter, perform the following procedure:

1. From the main menu on the left side of the page, select the **Security** folder.

   The **Security** folder expands.

2. From the **Security** folder, select **Destination MAC Filter**.

   The Destination MAC Filter Page is shown in Figure 120.

3. Select the **Delete** button next to the MAC address that you want to delete.
   The MAC address is removed from the MAC address table.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Chapter 22

DHCP Snooping

This chapter contains a description of the DHCP Snooping feature and the procedures for creating, modifying, and deleting the DHCP Snooping configuration. This chapter contains the following sections:

❑ "Overview" on page 300

❑ "General Guidelines" on page 302

❑ "General Configuration" on page 303

❑ "VLAN Setting" on page 306

❑ "Trusted and Untrusted Port Configuration" on page 308

❑ "Binding Database" on page 310

Note

To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Overview

The DHCP Snooping feature provides security by inspecting ingress packets for the correct IP and MAC address information. The DHCP Snooping feature defines the AT-GS950/16 ports as either trusted or untrusted. With DHCP Snooping enabled, two network security issues are addressed:

- All ingress DHCP packets are examined on the untrusted ports and only authorized packets are passed through the switch. Unwanted ingress DHCP packets are discarded. See "Unauthorized DHCP Servers" below.

- DHCP ingress packets on an untrusted port are inspected to insure that the source IP Address and MAC Address combination in each packet is valid when compared to the DHCP Snooping Binding Table. If a match is not found, the packet is discarded.

Trusted Ports   By definition, trusted ports inherently trust all ingress Ethernet traffic. There is no checking or testing on ingress packets for this type of port. A trusted port connects to a DHCP server in one of the following ways:

- Directly to the legitimate trusted DHCP Server

- A network device relaying DHCP messages to and from a trusted server

- Another trusted source such as a switch with DHCP Snooping enabled

Untrusted Ports   The Ethernet traffic on an untrusted port is inherently not trusted. The ingress packets are consequently tested against specific criteria to determine if they can be forwarded through the switch or should be immediately discarded. Untrusted ports are connected to DHCP clients and to traffic that originates outside of the LAN.

Unauthorized DHCP Servers   Normally in a network, a single DHCP server exists in a local area network (LAN). The DHCP server supplies network configuration information to individual devices on the network, including the assigned IP address for each host. A trusted DHCP server is connected to a trusted port on the switch.

It is possible that another unauthorized and unwanted DHCP server could be connected to the network. This situation can occur if a client on the network happens to enable a DHCP server application on his workstation or if someone outside the network attempts to send DHCP packets to your network. These situations pose a security risk.

A network device initially sends out a DHCPDISCOVER packet so that a DHCP server will respond. It waits for and then accepts the first DHCPOFFER packet from the server that it receives. This packet contains the DHCP server's IP address and mask. If the unauthorized DHCP server responds first, then the network device will use the information from the unintended DHCP server for the default gateway or DNS server.

Untrusted ports are connected to the DHCP clients and to traffic that originated outside the LAN. By definition, untrusted ports do not accept DHCP packets originating form a DHCP server and immediately drop them when they are detected. The DHCP packets types that are not accepted are DHCPOFFER and DHCPACK.

However, untrusted ports do accept both DHCP DISCOVER and DHCPREQUEST packets sent from DHCP clients. This behavior allows DHCP clients to respond to a trusted DHCP server and not respond to a DHCP server that is untrusted.

DHCP with Option 82

You can configure the AT-GS950/16 to pass DHCP packets containing Option 82 information through the switch without altering the information within the packet. You can also configure the AT-GS950/16 switch to insert DHCP Option 82 information directly into the DHCP packets as they pass through the switch.

General Guidelines

Here is a summary of the rules to observe when you configure DHCP Snooping:

- A trusted port is connected to one of the following:

    – Directly to the legitimate trusted DHCP Server.

    – A network device relaying DHCP messages to and from a trusted server.

    – Another trusted source, such as a switch with DHCP Snooping enabled.

- Untrusted ports are connected to DHCP clients and to traffic that originates outside of the local area network.

- The VLANs to which the DHCP Snooping feature applies must be specified in the DHCP Snooping VLAN Setting configuration.

- Any static IP addresses on the network must be manually added to the Binding Database.

General Configuration

You can enable DHCP Snooping and configure DHCP Snooping general settings on the switch by following the procedures in these sections:

❒ "Enabling DHCP Snooping"

❒ "Configuring DHCP Snooping General Settings" on page 304

Enabling DHCP Snooping

The following procedure describes how to enable or disable the DHCP Snooping feature on the AT-GS950/16 switch:

1. From the main menu on the left side of the page, select **DHCP Snooping**.

    The **DHCP Snooping** folder expands.

2. From the **DHCP Snooping** folder, select **General Settings**.
    The General Settings page is displayed. See Figure 121.

Figure 121. General Settings Page

3. In the **DHCP Snooping** field, select one of the following radio button choices:

    Enabled - This parameter activates the General Settings menus.

    Disabled - This parameter de-activates General Settings menus.

4. Click **Apply**.

    If you are configuring the general settings, skip to "Configuring DHCP Snooping General Settings" on page 304.

    If you want to enable or disable DHCP Snooping on the switch without configuring the general settings, proceed to Step 5.

5. From the main menu on the left side of the page, select **Save Settings to Flash** to activate or de-activate the DHCP Snooping feature on the AT-GS950/16 switch.

Configuring DHCP Snooping General Settings

The following procedure describes how to configure the DHCP Snooping feature on the AT-GS950/16 switch:

1. From the main menu on the left side of the page, select **DHCP Snooping**.

   The **DHCP Snooping** folder expands.

2. From the **DHCP Snooping** folder, select **General Settings**.
   The General Settings page is displayed. See Figure 121 on page 303.

3. From the **Pass Through Option 82** field, select one of the following choices from the pull-down menu:

   Enable - Allows an Option 82 packet to be passed through the AT-GS950/16 switch without being altered.

   Disable - Blocks an Option 82 packet from passing through the AT-GS950/16 switch.

4. From the **Verify MAC Address** field, select one of the following choices from the pull-down menu:

   Enable - The MAC address of each ingress ARP packet is validated when compared against the Binding Table entries. Invalid ARP packets are discarded.

   Disable - The MAC address of each ingress ARP packet is not validated against the Binding Table. All ARP packets are forwarded through the switch without regard to the IP and MAC Address information in the packet header.

5. From the **Backup Database** field, select one of the following choices from the pull-down menu:

   Enable - The AT-S114 Management Software saves a backup copy of the Binding Table to flash at a specified interval (Database Update Interval) of time.

   Disable - The AT-S114 Management Software does not save a backup copy of the Binding Table to flash.

6. Select an interval of time for the **Database Update Interval** field. The range of this interval is 600 to 86400 seconds.

7. From the **DHCP Option 82 Insertion** field, select one of the following choices from the pull-down menu:

Enable - The AT-S114 Management software inserts the DHCP Option 82 information into the DHCP packets.

Disable - The AT-S114 Management software does not insert the DHCP Option 82 information into the DHCP packets.

8. Click **Apply**. The values for the DHCP Snooping General Settings take effect.

9. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

VLAN Setting

You can create and delete DHCP Snooping VLAN settings by following the procedures in these sections:

❐ "Creating a VLAN"
❐ "Modifying a VLAN" on page 307
❐ "Deleting a VLAN" on page 307

Creating a VLAN

To define a VLAN that will be a part of the DHCP Snooping feature, do the following:

1. From the main menu on the left side of the page, select **DHCP Snooping**.

   The **DHCP Snooping** folder expands.

2. From the **DHCP Snooping** folder, select **VLAN Settings**.

   The VLAN Settings page is displayed. See Figure 122.

Figure 122. DHCP Snooping VLAN Settings Page

3. In the **VLAN ID** field, enter a VLAN ID that has been pre-defined.

   See "Tagged VLAN Configuration" on page 166 for information about configuring VLANs.

4. Click **Add**.

   The new VLAN ID entry is displayed in the table on the page.

5. If you find more than one VLAN ID to configure for DHCP Snooping, enter them one at a time by following Step 3 and Step 4.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Modifying a VLAN

To modify a VLAN ID, you must first delete it (by following the procedure outlined in "Deleting a VLAN" on page 307) and then re-enter it by following the procedure outlined in "Creating a VLAN" on page 306.

Deleting a VLAN

To delete a VLAN ID, do the following:

1. From the main menu on the left side of the page, select **DHCP Snooping**.

    The **DHCP Snooping** folder expands.

2. From the **DHCP Snooping** folder, select **VLAN Settings**.

    The VLAN Settings page is displayed. See Figure 122 on page 306.

3. To delete a VLAN ID, click the **Delete** button in the Action column of the table.
    The VLAN ID is removed from the table.

    To delete multiple VLAN IDs, click the **Delete All** button.
    All VLAN IDs are removed from the table.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Trusted and Untrusted Port Configuration

The following procedure describes how to configure the DHCP Snooping trusted interfaces on the AT-GS950/16 switch:

1. From the main menu on the left side of the page, select **DHCP Snooping**.

   The **DHCP Snooping** folder expands.

2. From the **DHCP Snooping** folder, select **Trusted Interfaces**.
   The AT-GS950/16 Trusted Interfaces page is displayed. See Figure 123 for a partial view of this page.

Port	Trust	Action
All	Ignore ▼	Apply
1	Disabled ▼	Apply
2	Disabled ▼	Apply
3	Disabled ▼	Apply
4	Disabled ▼	Apply
5	Disabled ▼	Apply
6	Disabled ▼	Apply
7	Disabled ▼	Apply
8	Disabled ▼	Apply

Figure 123. AT-GS950/16 Trusted Interfaces Page

3. From the **Trust** column, select one of the following choices from the pull-down menu:

   Disabled - This parameter defines the port as untrusted for the DHCP Snooping feature.

   Enabled - This parameter defines the port as trusted for the DHCP Snooping feature.

4. Click **Apply** for the port.
   The port is now configured for your selection.
   See Figure 124 on page 309 for a partial view of this page.

Trusted Interfaces

Port	Trust	Action
All	Ignore ▼	Apply
1	Enabled ▼	Apply
2	Enabled ▼	Apply
3	Enabled ▼	Apply
4	Enabled ▼	Apply
5	Disabled ▼	Apply
6	Disabled ▼	Apply
7	Disabled ▼	Apply
8	Disabled ▼	Apply

Figure 124. Trusted Interfaces Page Example

5. If you choose to configure other switch ports as trusted or untrusted, repeat Step 3 and Step 4.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Binding Database

The Binding Database displays learned and statically assigned MAC Address and IP Address information for each host on the local area network. Dynamically assigned IP addresses from the DHCP server will automatically populate the table on the Binding Database page as they are assigned by the server. Statically assigned IP addresses are entered manually by entering the host's address information and clicking on the **Add** button.

The following procedure describes how to configure the DHCP Snooping Binding Database on the AT-GS950/16 switch for static IP addresses and how to view the MAC Address and IP Address information for all of the hosts on your local area network:

1. From the main menu on the left side of the page, select **DHCP Snooping**.

   The **DHCP Snooping** folder expands.

2. From the **DHCP Snooping** folder, select **Binding Database**.
   The AT-GS950/16 Binding Database page is displayed. See Figure 125.

Figure 125. AT-GS950/16 Binding Database Page

Static IP Addresses

To enter a statically assigned IP address for a host, perform the following procedure:

1. Enter the host information into the following fields:

MAC Address - Enter the host's MAC Address.

IP Address - Enter the static IP Address assigned to the host using one of the **IP Address** fields:

For an IPv4 address, click **IPv4**, then enter the address using xxx.xxx.xxx.xxx format.

For an IPv6 address, click **IPv6**, then enter the address using xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx hexadecimal format.

VLAN - Enter the host's VLAN ID.

Port - Enter the port number where the host is connected.

Type - Because the IP Address being entered is static, select **Static**.

2. Click **Add**.
   The static address information is entered into the Binding Database. See Figure 126 for an example.

Figure 126. Binding Database Page Example

Viewing   A dynamically assigned IP address from the DHCP server automatically populates the table on the Binding Database page. You must enter statically assigned IP Addresses and their corresponding fields at the top of the web page. See "Static IP Addresses" on page 310 for more information.

The Binding Database table at the bottom of the web page displays the following information:

MAC Address - This parameter shows the host's MAC Address.

VLAN ID - This parameter shows the host's VLAN ID of which the DHCP client is a member.

IP Address - This parameter is the IP Address assigned by the DHCP server to the DHCP client.

Port - This parameter is the port number where the DHCP client is connected.

Type - This parameter indicates the following:

Learned - The host IP Address is dynamically assigned by the DHCP server.

Static - The host IP Address is statically assigned. See "Static IP Addresses" on page 310 for more information.

Lease Time - This parameter is the time that IP address assignment by the DHCP server is valid.

If the **Page** field located below the table displays a page number, then there are multiple pages of the table that you can navigate. Click on the **First Page**, **Previous Page**, **Next Page**, and **Last Page** buttons located below the table.

Chapter 23
LLDP

Link Layer Discovery Protocol (LLDP) allows Ethernet network devices, such as switches and routers, to receive and transmit device-related information to directly connected devices on the network and to store data that is learned about other devices. This chapter provides the following information:

❒ "Overview" on page 314
❒ "Global Configuration" on page 315
❒ "Neighbors Information" on page 318

Note

To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Overview

The data sent and received by LLDP are useful for many reasons. The switch can discover other devices directly connected to it. Neighboring devices can use LLDP to advertise some parts of their Layer 2 configuration to each other, which may highlight inconsistencies in the neighboring device's configuration which can then be corrected.

LLDP is a "one-hop" protocol. LLDP information can only be sent to and received by devices that are directly connected to each other, or connected via a hub or repeater. Devices that are directly connected to each other are called neighbors. Advertised information is not forwarded on to other devices on the network. Also, LLDP is a one-way protocol. That is, the information transmitted in LLDP advertisements flows in one direction only, from one device to its neighbors, and the communication ends there. Transmitted advertisements do not solicit responses, and received advertisements do not solicit acknowledgements. LLDP cannot solicit any information from other devices. LLDP operates over physical ports only. For example, it can be configured on switch ports that belong to static port trunks or LACP trunks, but not on the trunks themselves, and on switch ports that belong to VLANs, but not on the VLANs themselves.

Each port can be configured to transmit local information, receive neighbor information, or both. LLDP transmits information as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value elements (TLV), each of which contains a particular type of information about the device or port transmitting it.

Global Configuration

The LLDP Global Settings page has three sections:

❒ The top of the page contains the enabling or disabling LLDP selections and optional LLDP settings.

❒ The middle of the page contains LLDP System Information.

❒ The LLDP port settings are on the bottom of the page.

See Figure 127 for a partial view of the LLDP Global Settings page.

Figure 127. AT-GS950/16 LLDP Global Settings Page

Perform the following procedures to configure the global parameters for LLDP:

❒ "Enabling or Disabling LLDP" on page 316
❒ "Displaying System Information" on page 317
❒ "Setting Port States" on page 317

You must enable LLDP before changing the LLDP System Information settings or the port settings.

Enabling or Disabling LLDP

To enable or disable the LLDP feature, perform the following procedure:

1. From the main menu on the left side of the page, click the **LLDP** folder. The **LLDP** folder expands.

2. From the **LLDP** folder, select **LLDP Global Settings**.

3. For the **LLDP** parameter, select one of the following radio button choices:

   Enabled: The LLDP feature is active.

   Disabled: The LLDP feature is inactive.

   Note

   The LLDP feature is not dependent on the DHCP feature. As a result, the DHCP feature can be set to either Enabled or Disabled without affecting LLDP.

   ---

4. Click the **Apply** button to the right of the either the **Enabled** or **Disabled** radio buttons.

   The LLDP setting that you have selected is now active.

5. Below the **Enable** or **Disable** radio buttons, you may adjust the following parameters as needed, then click the **Apply** button in the area of these parameters:

   Message TX Hold Multiplier: Sets the hold multiplier value. The hold time multiplier is multiplied by the transmit interval to give the Time To Live (TTL) that the switch advertises to the neighbors. The range is from 2 to 10.

   Message TX Interval: Sets the transmit interval, which is the interval between regular transmissions of LLDP advertisements. The range is from 1 to 10 seconds.

   LLDP Reinit Delay: Sets the reinitialization delay, which is the number of seconds that must elapse after LLDP is disabled on a port before it can be reinitialized. The range is from 1 to 10 seconds.

   LLDP TX Delay: Sets the value of the transmission delay timer, which is the minimum time interval between transmissions of LLDP advertisements due to a change in LLDP local information. The range is from 1 to 8192 seconds.

6. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Displaying System Information

To display system information about the switch, do the following:

1. From the main menu on the left side of the page, click the **LLDP** folder. The **LLDP** folder expands.

2. From the **LLDP** folder, select **LLDP Global Settings**.

3. The following parameters display the system information:

   Chassis ID Subtype: This parameter describes the Chassis ID subtype which is "macAddress". You cannot change this parameter.

   Chassis ID: This parameter lists the MAC address of the switch. You cannot change this parameter.

   System Name: This parameter lists the system name of the switch. You can assign the system name. For more information, refer to "System Management Information" on page 30.

   System Description: This parameter lists the product name of the switch. You cannot change this parameter.

Setting Port States

Each port on the switch can be assigned an LLDP state as follows:

1. Refer to the lower section of Figure 127 on page 315 for the LLDP port states.

2. In the State column, select one of the following states from a port's pull-down menu:

   Disabled: Indicates LLDP is disabled on the port. The port cannot receive or transmit LLDP data packets.

   RxTx: Indicates LLDP is enabled on the port. The port can receive and transmit LLDP data packets.

   RxOnly: Indicates LLDP is enabled on the port. The port can receive LLDP data packets.

   TxOnly: Indicates LLDP is enabled on the port. The port can transmit LLDP data packets.

   To change the settings of all the ports to the same state, select a state setting next to All In the Port column.

3. In the Action column, click the **Apply** button that corresponds to the port to make the state change active.

4. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Neighbors Information

To view the information received from the neighboring network devices, perform the following procedure:

1. From the main menu on the left side of the page, click the **LLDP** folder. The **LLDP** folder expands.

2. From the **LLDP** folder, select **LLDP Neighbors Information**.

   The LLDP Neighbors Information Page is displayed. See Figure 128.

   LLDP Neighbors Information

Entity	Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description	Show Detail

   Page 0/0   First Page   Previous Page   Next Page   Last Page   Page [ ] GO
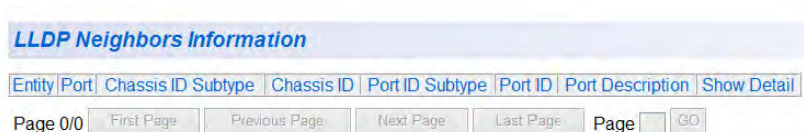
   Figure 128. LLDP Neighbors Information Page

   The following parameters are displayed when the switch receives LLDP information from neighboring devices in the LAN:

   Entity: This parameter is a number assigned to the reporting neighbors in the order that the LLDP information is received from them.

   Port: This parameter specifies the AT-GS950/16 local port number where the LLDP information was received.

   Chassis ID Subtype: This parameter describes the Chassis ID subtype of the neighboring network device which is reporting the LLDP information.

   Chassis ID: This parameter is the neighboring device's chassis ID.

   Port ID Subtype: This parameter describes the Port ID subtype of the neighboring network device's port that is connected directly to the AT-GS950/16 switch port.

   Port ID: This parameter specifies the neighboring network device's port number from which the LLDP information was transmitted.

   Port Description: This parameter describes the neighboring network device's port.

   Show Detail: If you click on this button, a detailed report of the neighboring network device will be displayed.

Chapter 24
Network Statistics

The sections in this chapter explain how to display traffic, error, and history statistics about the network traffic on the AT-GS950/16 switch and its ports. This chapter includes the following sections:

- ❒ "Overview" on page 320
- ❒ "Traffic Comparison Statistics" on page 321
- ❒ "Error Group Statistics" on page 325
- ❒ "Historical Status Statistics" on page 327

Note

To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Overview

Statistics provide important information for troubleshooting switch problems at the port level. The AT-S114 Management Software provides a versatile set of statistics charts that you can customize for your needs, including (depending upon the chart) the ports whose statistics you want to view and the color used to draw the chart.

Note

The Java SSV Helper plug-in must be installed and enabled on your browser to display these network traffic statistics charts.

There are three types of statistics charts:

❑ Traffic Comparison: Allows you to display a specified traffic statistic over all of the ports. You can select 24 statistic types and 12 colors for each port. This chart is described in "Traffic Comparison Statistics" on page 321.

❑ Error Group: This chart displays the discard and error counts for a specified port and is described in "Error Group Statistics" on page 325.

❑ Historical Status: Allows you to select from 12 statistics to view for a selection of ports for however long this chart is running on the management workstation. This chart is described in "Historical Status Statistics" on page 327.

Traffic Comparison Statistics

The Traffic Comparison chart allows you to display a specified traffic statistic over all of the ports. You can select 24 statistic types and 12 colors for each port.

To display traffic comparison statistics, perform the following procedure:

1. Select the **Statistics Chart** folder.

    The **Statistics Chart** folder expands.

2. From the **Statistics Chart** folder, select **Traffic Comparison**.

    The Traffic Comparison Chart page opens as shown in Figure 129.
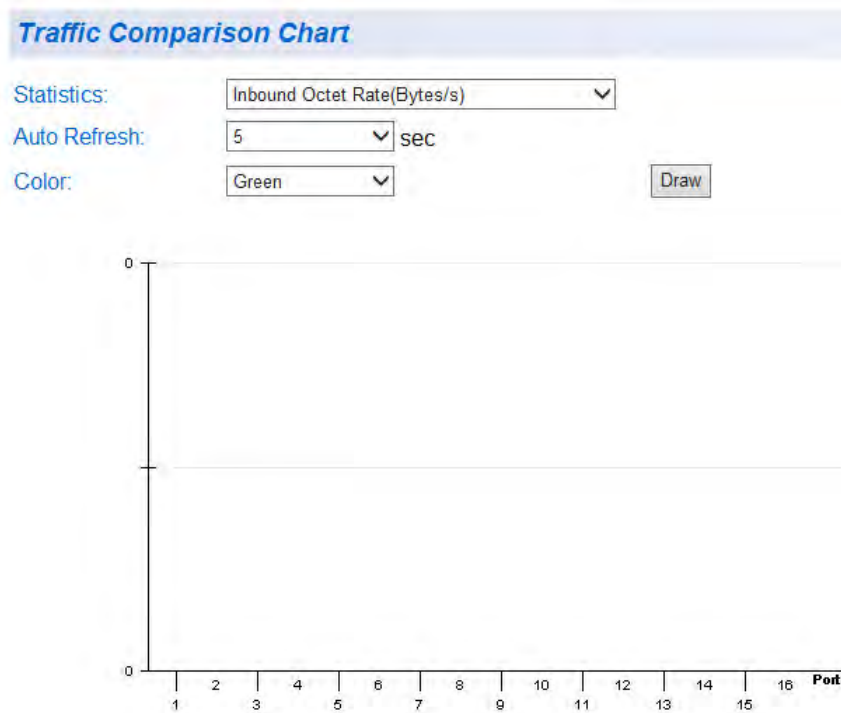
Figure 129. Traffic Comparison Chart Page

3. To view traffic statistics, click on the arrow next to "Statistics" and select one of the options in Table 5.

Table 5 Traffic Comparison Options

Option	Definition
Inbound Octet Rate (Bytes/s)	Measures the rate of inbound octet bits in bytes per second.
Inbound Unicast Packet Rate (Pkts/s)	Measures the rate of inbound unicast packets in packets per second.
Inbound Non-unicast Packet Rate (Pkts/s)	Measures the rate of inbound non-unicast packets in packets per second.
Inbound Discard Rate (Pkts/s)	Measures the rate of inbound discarded packets in packets per second.
Inbound Error Rate (Pkts/s)	Measures the rate of inbound errors in packets per second.
Outbound Octet Rate (Bytes/s)	Measures the rate of outbound octet bits in bytes per second.
Outbound Unicast Packet Rate (Pkts/s)	Measures the rate of outbound unicast packets in packets per second.
Outbound Non-unicast Packet Rate (Pkts/s)	Measures the rate of outbound non-unicast packets in packets per second.
Outbound Discard Rate (Pkts/s)	Measures the rate of outbound discarded packets in packets per second.
Outbound Error Rate (Pkts/s)	Measures the rate of outbound errors in packets per second.
Ethernet Undersize Packet Rate (Pkts/s)	Measures the rate of undersized Ethernet packets in packets per second.
Ethernet Oversize Packet Rate (Pkts/s)	Measures the rate of oversized Ethernet packets in packets per second.
Inbound Octets (Bytes)	Measures the number of inbound octet bits in bytes per second.
Inbound Unicast Packets (Pkts)	Measures the number of inbound unicast packets in packets per second.
Inbound Non-unicast Packets (Pkts)	Measures the number of inbound non-unicast packets (such as broadcast and multicast packets) in packets per second.
Inbound Discards (Pkts)	Measures the number of inbound discarded packets in packets per second.

Table 5 Traffic Comparison Options (Continued)

Option	Definition
Inbound Errors (Pkts)	Measures the number of inbound errors in packets per second.
Outbound Octets (Bytes)	Measures the number of outbound octet bits in bytes per second.
Outbound Unicast Packets (Pkts)	Measures the number of outbound unicast packets in packets per second.
Outbound Non-unicast Packets (Pkts)	Measures the number of outbound non-unicast (such as broadcast and multicast packets) packets in packets per second.
Outbound Discards (Pkts)	Measures the number of outbound discarded packets in packets per second.
Outbound Errors (Pkts)	Measures the number of outbound error packets in packets per second.
Ethernet Undersize Packets (Pkts)	Measures the number of undersized Ethernet packets in packets per second.
Ethernet Oversize Packets (Pkts)	Measures the number of oversized Ethernet packets in packets per second.

4. To select the amount of time before the screen is refreshed, select one of the options below and click **Auto Refresh**.

   - **5 seconds**
   - **10 seconds**
   - **15 seconds**
   - **30 seconds**

5. To select the color of the Traffic Comparison chart, select **Color**. Choose one of the following colors:

   - **Green**
   - **Blue**
   - **Red**
   - **Purple**
   - **Yellow**
   - **Orange**
   - **Gray**
   - **Light Red**
   - **Light Blue**
   - **Light Green**
   - **Light Yellow**
   - **Light Gray**

6. To create the Traffic Comparison chart, click **Draw**. See Figure 130 for an example of the Traffic Comparison chart with data.
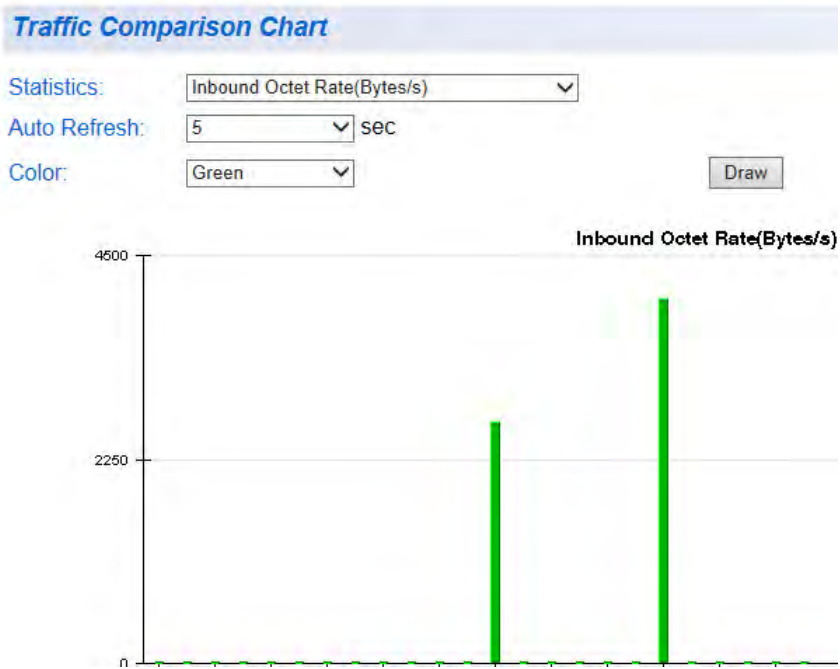
Figure 130. Traffic Comparison Page Example

7. From the menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Error Group Statistics

The Error Group chart displays the discard and error counts for a specified port.

To display error group statistics for a port, perform the following procedure:

1. Select the **Statistics Chart** folder.

   The **Statistics Chart** folder expands.

2. From the **Statistics Chart** folder, select **Error Group**.

   The Error Group Chart page is displayed in Figure 131.
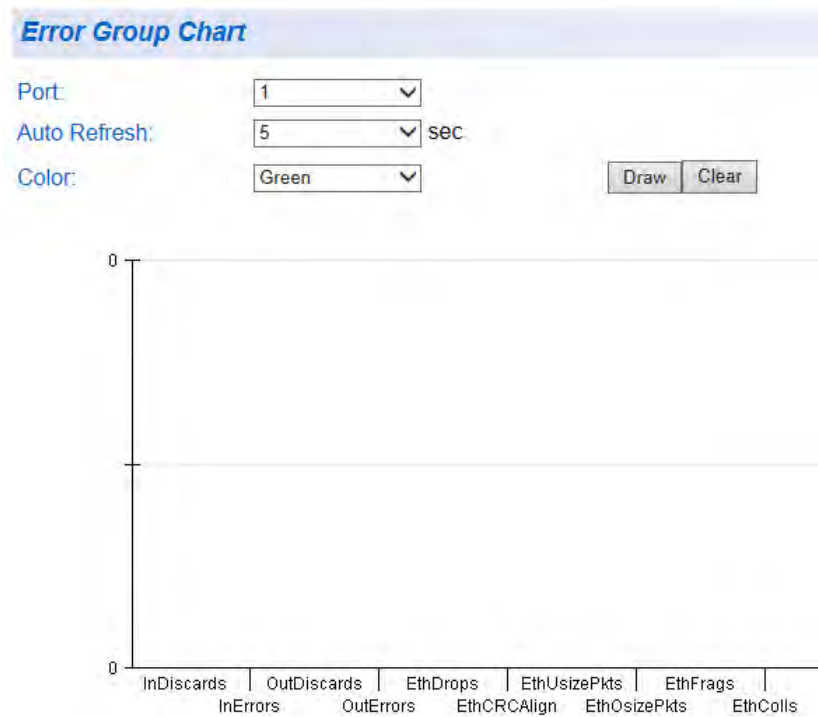
Figure 131. Error Group Chart Page

3. Select a port number from the pull-down menu next to **Port**.

4. To select the amount of time before the screen is refreshed, select one of the options below and click **Auto Refresh**.

    ■ **5 seconds**

    ■ **10 seconds**

    ■ **15 seconds**

    ■ **30 seconds**

5. To select the color of the Error Group chart, select **Color**. Choose one of the following colors:

    ■ **Green**

    ■ **Blue**

    ■ **Red**

    ■ **Purple**

    ■ **Yellow**

    ■ **Orange**

    ■ **Gray**

    ■ **Light Red**

    ■ **Light Blue**

    ■ **Light Green**

    ■ **Light Yellow**

    ■ **Light Gray**

6. To create the Error Group chart, click **Draw**.

7. From the menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Historical Status Statistics

The Historical Status chart allows you to select from 12 statistics to view for a selection of ports for however long this chart is running on the management workstation. To display historical status statistics for a port, perform the following procedure:

1. Select the **Statistics Chart** folder.

    The **Statistics Chart** folder expands.

2. From the **Statistics Chart** folder, select **Historical Status**.

    The Historical Status Chart page is displayed in Figure 132.
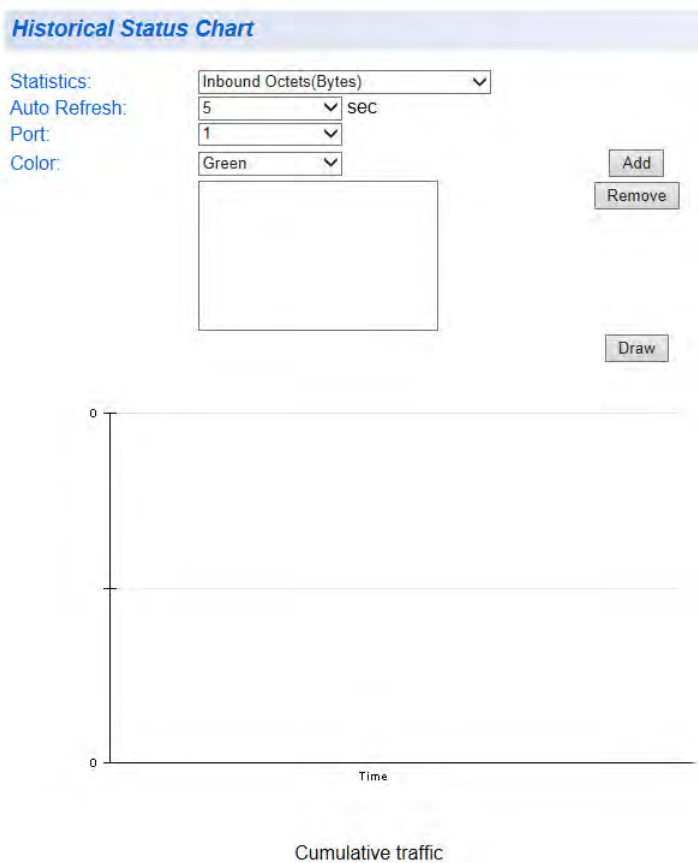
Figure 132. Historical Status Chart Page

3. To view historical statistics, click on the arrow next to "Statistics" and select one of the options in Table 6 on page 328.

Table 6 Historical Status Options

Option	Definition
Inbound Octets (Bytes)	Measures the number of inbound octet bits in bytes per second.
Inbound Unicast Packets (Pkts)	Measures the number of inbound unicast packets in packets per second.
Inbound Non-unicast Packets (Pkts)	Measures the number of inbound non-unicast packets (such as broadcast and multicast packets) in packets per second.
Inbound Discards (Pkts)	Measures the number of inbound discarded packets in packets per second.
Inbound Errors (Pkts)	Measures the number of inbound errors in packets per second.
Outbound Octets (Bytes)	Measures the number of outbound octet bits in bytes per second.
Outbound Unicast Packets (Pkts)	Measures the number of outbound unicast packets in packets per second.
Outbound Non-unicast Packets (Pkts)	Measures the number of outbound non-unicast (such as broadcast and multicast packets) packets.
Outbound Discards (Pkts)	Measures the number of outbound discarded packets.
Outbound Errors (Pkts)	Measures the number of outbound error packets.
Ethernet Undersize Packets (Pkts)	Measures the number of undersized Ethernet packets.
Ethernet Oversize Packet Rate (Pkts)	Measures the number of oversized Ethernet packets.

4. To select the amount of time before the screen is refreshed, select one of the options below and click **Auto Refresh**.

    ■ **5 seconds**

    ■ **10 seconds**

    ■ **15 seconds**

    ■ **30 seconds**

5. To select the color of the Historical Statistics chart, select **Color**. Choose one of the following colors:

    ■ **Green**

    ■ **Blue**

    ■ **Red**

    ■ **Purple**

    ■ **Yellow**

    ■ **Orange**

    ■ **Gray**

    ■ **Light Red**

    ■ **Light Blue**

    ■ **Light Green**

    ■ **Light Yellow**

    ■ **Light Gray**

6. To create the Historical Statistics chart, select **Add**.

7. To draw the Historical Statistics chart, click **Draw**. See Figure 133 on page 330 for an example of the Historical Statistics chart with data.
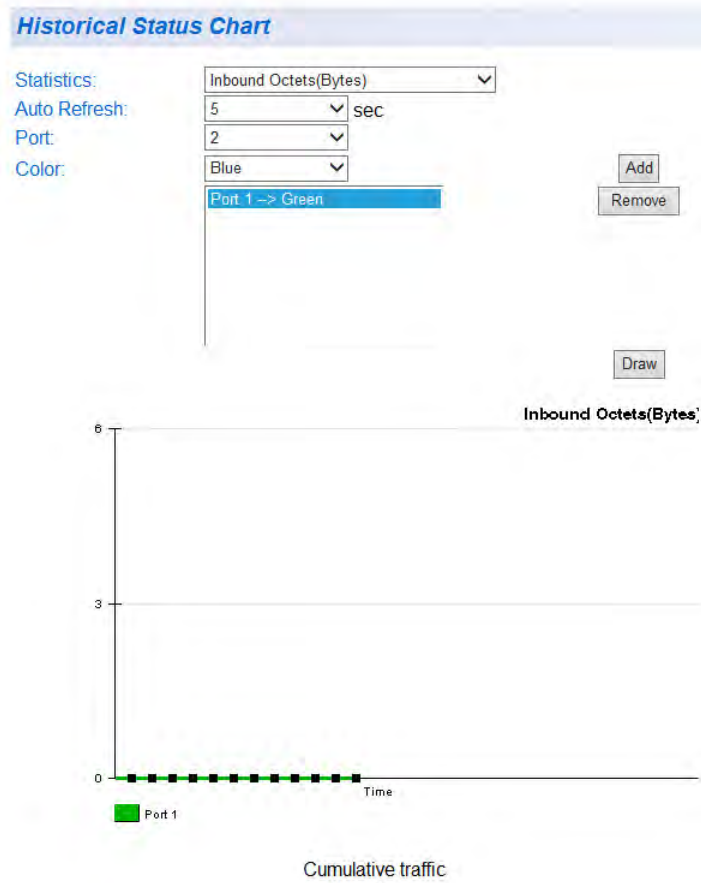
Figure 133. Historical Statistics Page Example

8. From the menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Section IV
Tools

This section contains the following chapters:

Chapter 25
Software/Configuration Updates

This chapter explains the methods for upgrading the AT-S114 Management Software on the switch and saving configuration files. This chapter contains the following sections:

□ "Overview" on page 334
□ "Upgrade Firmware Image via HTTP" on page 335
□ "Upgrade Firmware Image via TFTP" on page 337
□ "Download or Upload a Configuration File via HTTP" on page 339
□ "Download or Upload a Configuration File via TFTP" on page 343

Note

For information about how to obtain new releases of the AT-S114 Management Software, see "Allied Telesis Contact Information" on page 19.

Note

To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

Overview

You can use the Management Software Updates features to upgrade the AT-S114 Management Software to a new version, save a configuration file or load a configuration file. In addition, you can:

❒ Upload a configuration file from the switch onto a PC

❒ Download a configuration file from a PC onto the switch

There are two methods to upgrade the AT-S114 Management software or upload or download your configuration file:

❒ Using a web browser via HTTP

❒ Using a TFTP server

To perform one of these operations using HTTP, you only need to have access to an Internet browser. However, to perform one of these operations using TFTP, you must have access to a TFTP server.

In addition, you can save a configuration file from your AT-GS950/16 switch, which can be downloaded to other AT-GS950/16 switches on your network. This ensures identical configurations on all of your switches. In addition, loading an existing configuration saves time.

Upgrade Firmware Image via HTTP

This section describes how to upgrade a firmware image of the AT-S114 Management Software using HTTP on an Internet server. Before downloading a new version of the AT-S114 Management Software onto the switch with HTTP, note the following:

❐ The current configuration of the switch is retained when a new AT-S114 software image is installed. To return a switch to its default configuration values, see "Configure Factory Default Values" on page 358.

❐ When downloading the new image file, your switch must have an IP address and subnet mask assigned, either manually or via DHCP. For instructions on how to set the IP address and subnet mask on a switch, see "Configuration of IPv4 Address, Subnet Mask and Gateway Address" on page 32. To enable a DHCP client, see "DHCP Client Configuration" on page 53.

⚠️ **Caution**

Downloading a new version of management software onto the switch causes the device to reset. Some network traffic may be lost during the reset process.

This procedure assumes that you have already obtained the software and have stored it on the computer from which you will be performing this procedure.

To download the AT-S114 image software onto the switch using HTTP, perform the following procedure:

1. From the menu on the left side of the home page, select the **Tools** folder.
   This folder expands to show the **Firmware Upgrade** folder.

2. From the **Firmware Upgrade** folder, select **via HTTP**.

   The Firmware Upgrade via HTTP Page is displayed. See Figure 134.
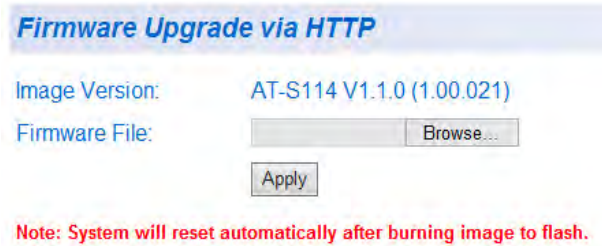
Figure 134. Firmware Upgrade via HTTP Page

3. Change the **Firmware File** parameter as necessary: Enter the path and the firmware file name, or click the **Browse** button and select the file name.

4. To begin the upgrade process on the switch, click **Apply**.

   The software begins to download onto the switch immediately. This process takes a few minutes. After the software download is complete, the switch initializes the software and reboots. You will lose your web browser connection to the switch during the reboot process.

Upgrade Firmware Image via TFTP

This section describes how to upgrade a firmware image of the AT-S114 Management software using TFTP on a TFTP server. Before downloading a new version of the AT-S114 Management Software onto the switch, note the following:

❐ The current configuration of a switch is retained when a new AT-S114 Management Software image is installed. To return a switch to its default configuration values, see "Configure Factory Default Values" on page 358.

❐ Your network must have a TFTP server.

❐ You must specify the path to the new AT-S114 image file on the TFTP server.

❐ Start the TFTP server software *before* you begin the download procedure.

⚠ **Caution**

Downloading a new version of management software onto the switch causes the device to reset. Some network traffic may be lost during the reset process.

This procedure assumes that you have already obtained the software and have stored it on the computer from which you will be performing this procedure.

To download the AT-S114 image software onto the switch using a TFTP server, perform the following procedure:

1. From the menu on the left side of the home page, select the **Tools** folder.

   This folder expands to show contents of the **Firmware Upgrade** folder.

2. From the **Firmware Upgrade** folder, select **via TFTP**.

   The Firmware Upgrade via TFTP page is shown in Figure 135 on page 338.

Firmware Upgrade via TFTP

Image Version: AT-S114 V1.1.0 (1.00.021)
TFTP Server IP: ◉ IPv4
○ IPv6
Image File Name: (Max. length: 64 characters)
Retry Count:
Apply

Note: System will reset automatically after burning image to flash.

Figure 135. Firmware Upgrade via TFTP Page

The **Image Version** shows the current version and date of software installed on the switch.

3. Change the following parameters as necessary:

> **TFTP Server IP**: The IP address of the TFTP server from which you are downloading the new software:
>
>> For an IPv4 address, click **IPv4**, then enter the address using xxx.xxx.xxx.xxx format.
>>
>> For an IPv6 address, click **IPv6**, then enter the address using xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx hexadecimal format.
>
> **Image File Name**: The full name of the AT-S114 file (including the file extension) you are downloading.
>
> **Retry Count**: The number of times the firmware upgrade is retried. The range is 1 - 20.

4. To activate your changes on the switch, click **Apply**.

The software immediately begins to download onto the switch. This process takes a few minutes. After the software download is complete, the switch initializes the software and reboots. You will lose your web browser connection to the switch during the reboot process.

Download or Upload a Configuration File via HTTP

This section describes how to download or upload a configuration file using HTTP on an Internet server. For example, you can save the switch's configuration file to your PC, then the saved file can be transferred to other switches.

Before you download or upload a configuration file via HTTP, note the following:

❒ You must be able to access the new AT-S114 configuration file from your PC when uploading a file from a PC to the switch.

❒ The switch that you are working with must have an IP address and subnet mask assigned, either manually or via DHCP. For instructions on how to manually set the IP address and subnet mask on a switch, see "Configuration of IPv4 Address, Subnet Mask and Gateway Address" on page 32. To enable a DHCP client, see "DHCP Client Configuration" on page 53.

To download an AT-S114 configuration file to your PC or upload an AT-S114 configuration file onto the switch using a web browser, perform the following procedure:

1. From the menu on the left side of the home page, select the **Tools** folder.

   The **Tools** folder expands.

2. From the **Tools** folder, select **Config File Backup/Restore** folder.

   The **Config File Backup/Restore** folder expands.

3. From the **Config File Backup/Restore** folder, select **via HTTP**.

   The Configuration File Backup/Restore via HTTP page is displayed. See Figure 136.

Figure 136. Configuration File Backup/Restore via HTTP Page

Configuration File Download

To download or save the AT-S114 configuration file from the switch to your PC, perform the following procedure:

1. Click the **Backup** button. Select this button to download a configuration file from the switch to your PC.
    The message shown in Figure 137 is displayed.

Figure 137. Save Configuration File Message

2. Save the configuration file to your PC:

    Clicking **Save** automatically saves the file to your PC without letting you choose the location.

    Clicking **Save As** lets you choose the location. When the **Save As** window is displayed, save the file in the appropriate directory.

    The message shown in Figure 138 is displayed indicating the download has completed.

Figure 138. Download Complete Message
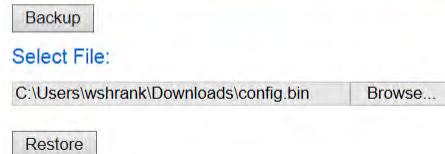
Note
If you clicked **Save** and want to see the location of the file, click the **View downloads** button in the Download Complete Message.

Configuration File Upload

To upload an AT-S114 configuration file from your PC to the switch, perform the following procedure:

1. Click the **Browse** button under the **Select File** field and select the path and file name.
   The path and file name are displayed in the **Select File** field. See Figure 139.

Figure 139. Select File Field with Path Location

2. Click the **Restore** button.
   The upload process begins immediately.

⚠ **Caution**

If you are uploading a configuration file, the file will be implemented immediately after upload. A short interruption in network service will be experienced while the new configuration file is loaded.

Note

If the IP address contained in the new configuration file is different than the one you currently have in your browser URL, you will loose connectivity with the AT-S114 Management software on the AT-GS950/16 switch after the new configuration file is loaded. If this is the case, you can identify the new IP address by using the ATI Web Discovery Tool. See"DHCP and ATI Web Discovery Tool" on page 52 for more information.

3. A message shown in Figure 140 will be displayed indicating that the upload has been completed. Click **OK**.
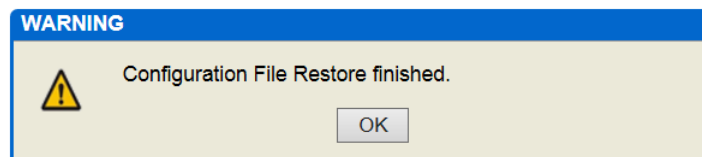
Figure 140. Configuration File Restore Finished Message

4. If you cannot access the Configuration File Backup/Restore via HTTP page, refresh the page and log back into the AT-S114 web interface.

Download or Upload a Configuration File via TFTP

This section describes how to download or upload a configuration file using TFTP on a TFTP server. Before you download or upload a configuration file onto the switch using TFTP, note the following:

❐ Your network must have a TFTP server.

❐ You must specify the path to the configuration file on the TFTP server.

❐ Start the TFTP server software *before* you begin the download procedure.

To download an AT-S114 configuration file onto a TFTP server or upload an AT-S114 configuration file onto the switch using a TFTP server, perform the following procedure:

1. From the menu on the left side of the home page, select the **Tools** folder.
   The **Tools** folder expands.

2. From the **Tools** folder, select the **Config File Backup/Restore** folder.
   The **Config File Backup/Restore** folder expands.

3. From the **Config File Backup/Restore** folder, select **via TFTP**.
   The Configuration Backup/Restore via TFTP Page is displayed. See Figure 141.
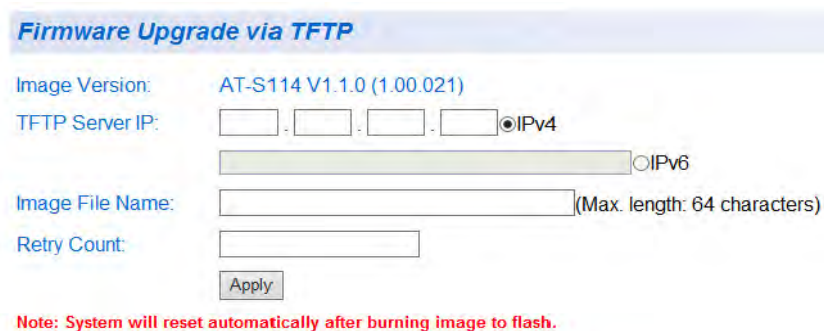

Figure 141. Configuration Backup/Restore via TFTP Page

Configuration File Download

To download an AT-S114 configuration file to a TFTP server, perform the following procedure:

1. Enter the IP address of the TFTP server in the field next to the **TFTP Server IP** parameter.

   For an IPv4 address, click **IPv4**, then enter the address using xxx.xxx.xxx.xxx format.

   For an IPv6 address, click **IPv6**, then enter the address using xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx hexadecimal format.

2. Enter the name of the configuration file in the field next to the **Config File Name** parameter.

3. Select the **Backup** button.
    A message is displayed indicating that the file has downloaded.

Configuration File Upload

To upload an AT-S114 configuration file onto the switch, perform the following procedure:

1. Enter the IP address of the TFTP server in the field next to the **TFTP Server IP** parameter.

    For an IPv4 address, click **IPv4**, then enter the address using xxx.xxx.xxx.xxx format.

    For an IPv6 address, click **IPv6**, then enter the address using xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx hexadecimal format.

2. Select the **Restore** button.

3. The software immediately begins to upload the configuration file from the TFTP server to the switch.

⚠️ **Caution**

If you are uploading a configuration file, the file will be implemented immediately after upload. A short interruption in network service will be experienced while the new configuration file is loaded.

Note

If the IP address contained in the new configuration file is different than the one you currently have in your browser URL, you will loose connectivity with the AT-S114 Management software on the AT-GS950/16 switch after the new configuration file is loaded. If this is the case, you can identify the new IP address by using the ATI Web Discovery Tool. See"DHCP and ATI Web Discovery Tool" on page 52 for more information.

Chapter 26
Cable Diagnostics

This chapter provides procedures to run cable diagnostics on the cables connected to the switch ports. If a port is selected, a cable must be connected to it for meaningful test results to be displayed.

Note
To permanently save your new settings or any changes to the configuration file, select **Save Settings to Flash** from the main menu on the left side of the page.

To run these cable diagnostics, perform the following procedure:

1. From the main menu on the left side of the page, click the **Tools** folder.

   The **Tools** folder expands.

2. From the **Tools** folder, select **Cable Diagnostics**.

   The Cable Diagnostics page is displayed. See Figure 142.
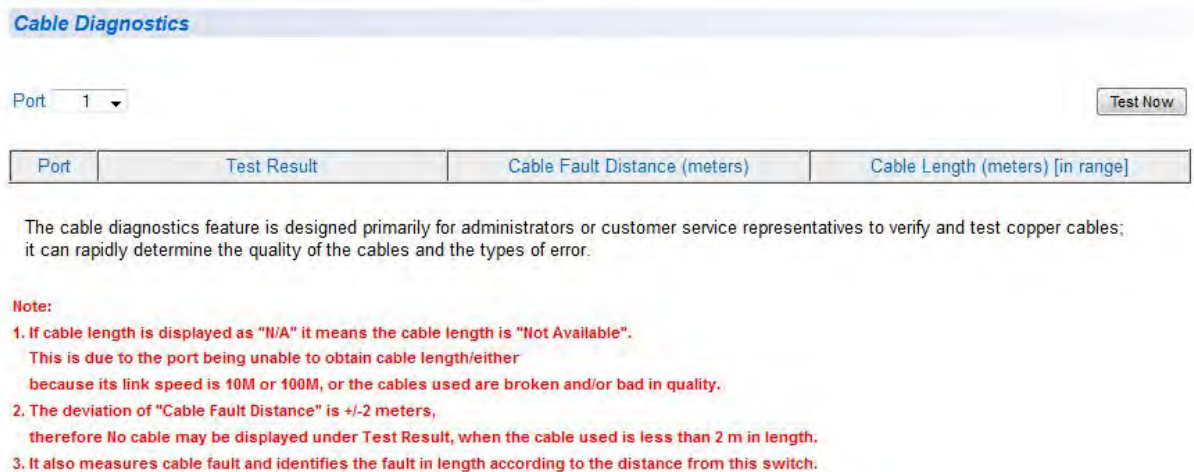
Figure 142. Cable Diagnostics Page

3. Select the **Port** number from the pull-down menu.

4. Click **Test Now**.

5. The following information is displayed:

Port: This parameter displays the port (cable) selected.

Test Results: Displays the diagnostic results for each pair in the cable. One of the following cable status parameters is displayed:

OK: There is not problem detected with the cable.

Open in Cable: There is an open wire within the cable.

Short in Cable: Two wires are shorted together within the cable.

Cross talk in Cable: There is crosstalk detected between one pair of wires and another pair within the cable.

Cable Fault Distance: This parameter specifies the distance from the switch port to the cable fault.

Cable Length: This parameter specifies the length of the cable connected to the switch port.

Note

If length is displayed as "N/A" it means the cable length is "Not Available". This is due to the port being unable to obtain cable length, either because its link speed is 10M or 100M, or the cables used are broken and/or of bad quality.

Note

The deviation of "Cable Fault Distance" is +/-2 meters, therefore No cable may be displayed under Test Result, when the cable used is less than 2 m in length.

Chapter 27
LED ECO Mode

This chapter provides the procedures to enable and disable the LED ECO mode.

The LED ECO Mode can be used to conserve additional power on the port LEDs. This eco-friendly feature turns off the port LEDs on the switch to save power when they are not necessary.

The LED ECO Mode can be turned off when you need to see the port LEDs on the switch.

This chapter contains the following sections:

❒ "Enable LED ECO Mode" on page 348
❒ "Disable LED ECO Mode" on page 349

Enable LED ECO Mode

To enable LED ECO Mode, perform the following procedure:

1. From the main menu on the left side of the page, select the **Tools** folder.
   The **Tools** folder expands.

2. From the **Tools** folder, select **LED ECO Mode**.
   The LED ECO Mode page is displayed. See Figure 143.
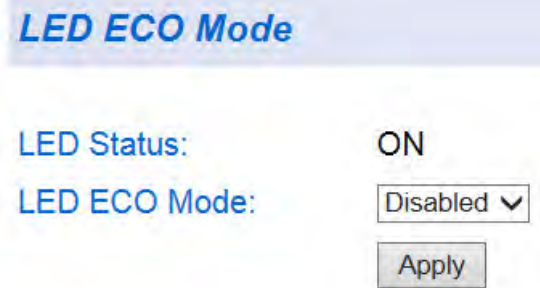
Figure 143. LED ECO Mode Page

3. Select **Enabled** from the **LED ECO Mode** pull-down menu.

4. Click **Apply**.
   The port LEDs turn off, and the LED Status changes to OFF. See Figure 144.
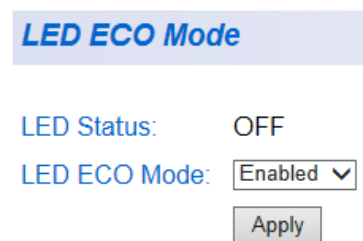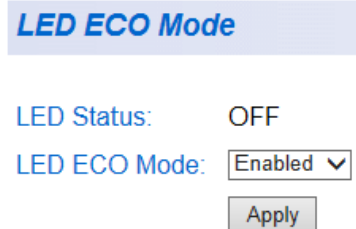
Figure 144. LED ECO Mode Enabled

5. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Disable LED ECO Mode

To disable LED ECO Mode, perform the following procedure:

1. From the main menu on the left side of the page, select the **Tools** folder.
   The **Tools** folder expands.

2. From the **Tools** folder, select **LED ECO Mode**.
   The LED ECO Mode page is displayed. See Figure 145.

LED ECO Mode

LED Status: OFF
LED ECO Mode: Enabled ▾

Apply

Figure 145. LED ECO Mode in Enabled State

3. Select **Disabled** from the **LED ECO Mode** pull-down menu.

4. Click **Apply**.
   The port LEDs turn on, and the LED Status changes to ON. See Figure 146.

LED ECO Mode

LED Status: ON
LED ECO Mode: Disabled ▾

Apply

Figure 146. LED ECO Mode Disabled

5. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Chapter 28

Energy-Efficient Ethernet

This chapter provides the procedures to enable and disable the IEEE 802.3az Energy-Efficient Ethernet (EEE) feature.

EEE allows for less power consumption during periods of no data activity to reduce overall power consumption, but still retains full network performance.

When EEE is enabled, the power reduction results from putting the circuitry driving the Ethernet line into Sleep mode when there is no data activity. When data activity resumes, the Ethernet line circuitry wakes up and resumes normal operation.

In this way, networking energy consumption can be reduced without adversely affecting network performance.

This chapter contains the following sections:

Enable EEE

To enable EEE, perform the following procedure:

1. From the main menu on the left side of the page, select the **Tools** folder.
   The **Tools** folder expands.

2. From the **Tools** folder, select **IEEE 802.3az EEE**.
   The IEEE 802.3az EEE page is displayed. See Figure 147.

   IEEE 802.3az EEE

   IEEE 802.3az EEE Status: Disabled ⌄

   Apply

Figure 147. IEEE 802.3az EEE Page

3. Select **Enabled** from the **IEEE 802.3az EEE Status** pull-down menu.

4. Click **Apply**.

5. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Disable EEE

To disable EEE, perform the following procedure:

1. From the main menu on the left side of the page, select the **Tools** folder.
   The **Tools** folder expands.

2. From the **Tools** folder, select **IEEE 802.3az EEE**.
   The IEEE 802.3az EEE page is displayed. See Figure 147 on page 352.

3. Select **Disabled** from the **IEEE 802.3az EEE Status** pull-down menu.

4. Click **Apply**.

5. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Chapter 29

Rebooting the AT-GS950/16

This chapter provides the procedures for rebooting the AT-GS950/16 switch by using the **Normal** reboot function provided in the AT-S114 management software.

Note

Alternately, you can reboot the AT-GS950/16 switch by pressing the front panel eco-friendly switch between 5 to 9 seconds.

In addition to rebooting the switch in the AT-S114 management software, you have the option to reset the configuration parameters on the switch to the original factory default settings. There are two ways to accomplish this:

■ Press the front panel eco-friendly button for more than 10 seconds and release it.

■ Reboot the switch in the AT-S114 management software and follow the procedures to reset to factory defaults.

Note

Refer to the AT-GS950 Installation guide for more information about how to use the eco-friendly button to reboot or reset the switch.

Note

The AT-S114 Management software default values are listed in "AT-GS950/16 Default Parameters" on page 387.

The following procedures are included in this chapter:

Switch Reboot

The following procedure outlines how to reboot your AT-GS950/16 switch.

⚠️ **Caution**

This procedure reboots the switch and reloads the AT-S114 Management software configuration from flash memory. Insure that your current configuration is saved before rebooting the switch by selecting **Save Settings to Flash** from the main menu on the left side of the page to permanently save your changes.

All configuration parameters that have not been previously saved are lost. After the switch is reboots, they are reset to the values stored in the flash memory.

⚠️ **Caution**

This procedure causes the switch to reboot. The switch does not forward network traffic during the reboot process. Some network traffic may be lost.

1. From the main menu on the left side of the page, select the **Tools** folder.
   The **Tools** folder expands.

2. From the **Tools** folder, select **Reboot**.
   The Factory Default Reset/Reboot Page is displayed. See Figure 148.

Figure 148. Factory Default Reset/Reboot Page

3. Go to the lower part of the page to the Reboot section.

4. In the **Reboot Type** field, select **Normal** from the pull-down menu. When the switch is rebooted with this selection, all configuration parameters that are saved in flash memory are loaded into the switch's active memory.

> **Note**
>
> Two additional options are available in the **Reboot Type** field. The procedures for these options are described in "Configure Factory Default Values".

5. Click **Apply**.
    The switch immediately begins to reload the AT-S114 Management software and configuration parameters. This process takes approximately two minutes to complete. You cannot manage the device during the reboot. After the reboot is finished, you can log in again if you want to continue to manage the switch.

Configure Factory Default Values

The following procedure returns all AT-S114 Management software parameters to their factory default values and deletes all tagged and port-based VLANs on the switch.

> **Note**
>
> The AT-S114 Management software factory default values are listed in "AT-GS950/16 Default Parameters" on page 387.

> ⚠️ **Caution**
>
> This procedure causes the switch to reboot. The switch does not forward network traffic during the reboot process. Some network traffic may be lost.

1. From the main menu on the left side of the page, select the **Tools** folder.
   The **Tools** folder expands.

2. From the **Tools** folder, select **Reboot**.
   The Reboot Page is displayed. See Figure 148 on page 356.

3. Go to the lower part of the page to the Reboot section.

4. In the **Reboot Type** field, use the pull-down menu to select one of the following options:

   Normal - This setting reloads all configuration parameters that are saved in flash memory. See "Switch Reboot" on page 356 for more information when using this selection.

   Factory Default - Resets all switch parameters to the factory default settings, including the IP address, subnet mask, and gateway address.

> ⚠️ **Caution**
>
> This setting will cause the IP address to be reset to 192.168.1.1. You will loose connectivity with the switch management software after the reboot is completed, but you can log in again with this IP address.

   Factory Default Except IP - Resets all switch parameters to the factory default settings, but retains the current IP address, subnet mask, and gateway settings saved in flash memory. If the DHCP client is enabled, it remains enabled after this reset and assignment of the IP

address, subnet mask, and gateway settings are managed by the DHCP server.

5. Click **Apply**.
    The switch begins the reboot process. You must wait approximately two minutes for the switch to complete the reboot process before you can re-establish your management session and network traffic begins flowing normally again.

Password Protection of Factory Reset

If your switch is located in a controlled environment, such as a locked switching closet or limited access equipment room, it may be desirable to have the ability to easily reset the switch to factory defaults at any time by using either the front panel eco-friendly switch or the AT-S114 management software.

However, if your switch is installed in an uncontrolled environment, you may want to protect the switch's configuration from unwanted or accidental resets. The AT-S114 management software allows you to disable the factory default reset feature and lock it with your own password. When this is done, two areas are affected:

- The reset and factory default reset features on the front panel eco-friendly switch are disabled.

- The factory default reset feature in the AT-S114 management software is disabled. However, you can still reset the switch via the management software without affecting the switch's configuration.

The factory default reset can be enabled again by using the password that you initially defined when disabling this function.

⚠ **Caution**

Because you define this password as part of the process of disabling this function, Allied Telesis has no knowledge of it. You are responsible for keeping the password in a safe place. If it is lost, Allied Telesis does not have a way to help you recover it.

See "Disabling Factory Default Reset Feature" on page 360 for information about how to disable the factory default reset feature.

Disabling Factory Default Reset Feature

The factory default reset feature allows anyone to reset the switch to the factory default configuration. You may disable this feature. More details are available concerning "Password Protection of Factory Reset" on page 360.

To disable the factory default reset feature, perform the following procedure:

1. From the main menu on the left side of the page, select the **Tools** folder.
   The **Tools** folder expands.

2. From the **Tools** folder, select **Reboot**.
   The Factory Default Reset/Reboot Page is displayed. See Figure 148 on page 356.

3. Go to the Factory Default Reset section on the upper part of the page. You will find a field called **Factory Default Reset**. This selection allows you to reset the switch configuration to the factory default settings given in "Multiple Spanning Tree Protocol" on page 87 by using the **Reboot** procedures outlined in "Configure Factory Default Values" on page 358.

4. To disable the factory default reset feature, select **Disable** on the pull-down menu of the **Factory Default Reset** field.
   The Factory Default Reset/Reboot Page changes to include fields for entering a password. See Figure 149.
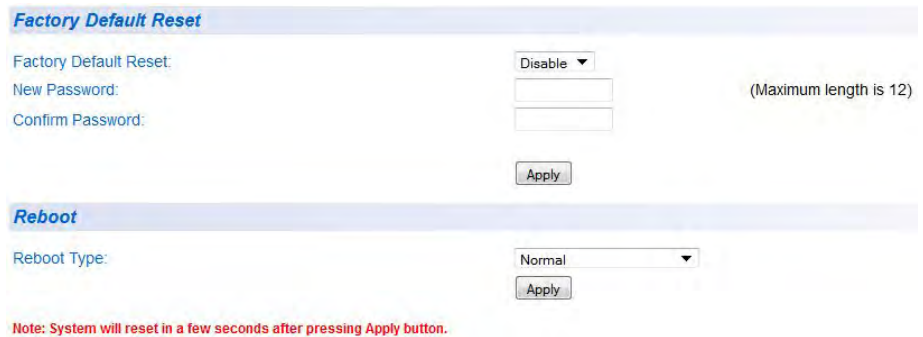
Figure 149. Factory Default Reset/Reboot Page with Password Entry

5. In the **New Password** field, enter a password of up to 12 characters in length. It is case-sensitive. There is not a default password for this field.

⚠ **Caution**
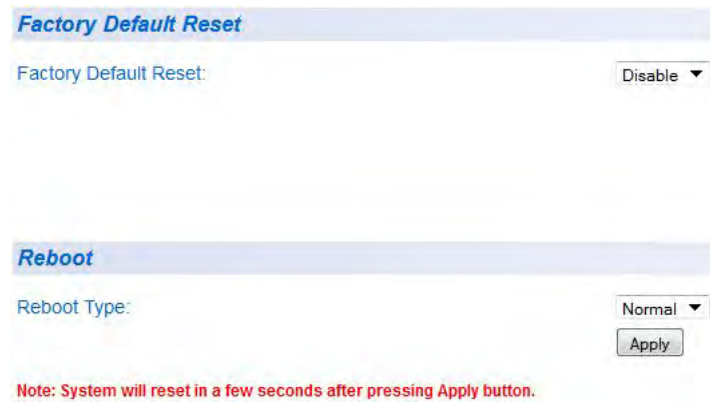
Because you define this password as part of the process of disabling this function, Allied Telesis has no knowledge of it. You are responsible for keeping the password in a safe place. If it is lost, Allied Telesis does not have a way to help you recover it.

6. Re-enter the same password in the **Confirm Password** field.

7. Click **Apply**.
   The following message is displayed:

   By clicking on Accept, the Factory Default Reset function will be Disabled on both the switch management software and the physical front panel ecoFriendly button. If you loose this password, ATI cannot recover it for you.
   By Clicking on Cancel, the "Factory Default Reset" function will

remain Enabled on both the switch management software and the physical front panel ecoFriendly button.

8. Click **Accept** on the message.
   The Factory Default Reset page changes and displays the Factory Default Reset feature as **Disabled**. See Figure 150.

Figure 150. Factory Default Reset Disabled Page

9. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Enabling Factory Default Reset

If the Factory Default Reset feature is disabled, and you choose to **Enable** it, perform the following procedure:

1. From the main menu on the left side of the page, select the **Tools** folder.
   The **Tools** folder expands.

2. From the **Tools** folder, select **Reboot**.
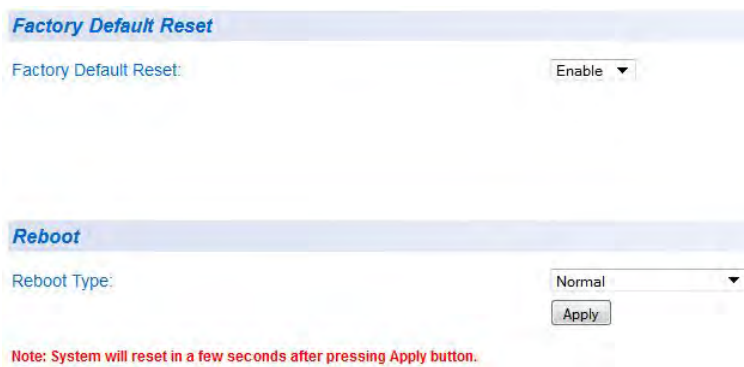   The Factory Default Reset/Reboot Page is displayed. See Figure 150.

3. Go to the Factory Default Reset section on the upper part of the page.
   The **Factory Default Reset** field should be set to **Disable**.

Note

If the **Factory Default Reset** field is already set to **Enable**, you do not need to continue with this procedure.

---

4. To enable the factory default reset feature, select **Enable** on the pull-down menu of the **Factory Default Reset** field.
   The Factory Default Reset/Reboot Page changes to include a **Password** field for entering a password. See Figure 151 on page 363.

Factory Default Reset

Factory Default Reset: Enable ▼

Password: [ ]   (Maximum length is 12)

Note: Enter P/W and click "Apply" to enable "Factory Default Reset" feature

Apply

Reboot

Reboot Type: Normal ▼

Apply

Note: System will reset in a few seconds after pressing Apply button.

Figure 151. Factory Default Reset/Reboot Page with Password Entry

5. Enter the same password that you defined when you previously set the **Factory Default Reset** field to **Disable**.

6. Click **Apply**.
The initial Factory Default Reset/Reboot Page is displayed with the **Factory Default Reset** field **Enabled**. See Figure 148 on page 356. In the Reboot section, the **Reboot Type** field now includes the options presented in its pull-down menu for returning the switch configuration to the factory default values. See "Configure Factory Default Values" on page 358 for more information.

7. From the main menu on the left side of the page, select **Save Settings to Flash** to permanently save your changes.

Chapter 30

Pinging a Remote System

This chapter provides the procedure for pinging a node on your network from the AT-GS950/16 switch. This procedure is useful in determining whether an active link exists between the switch and another network device.

Note

The device you are pinging must be a member of the default VLAN and within the same local area network as your switch. In other words, the port on the switch through which the node is communicating with the switch must be an untagged or tagged member of the Default VLAN.

To ping a network device, perform the following procedure:

1. From the main menu on the left side of the page, select the **Tools** folder.
   The **Tools** folder expands.

2. From the **Tools** folder, select **Ping**.
   The Ping Test Settings Page is displayed. See Figure 152.

Figure 152. Ping Test Settings Page

3. Configure the following parameters:

Destination IP Address - The IP address of the node you want to ping:

For an IPv4 address, click **IPv4**, then enter the address using xxx.xxx.xxx.xxx format.

For an IPv6 address, click **IPv6**, then enter the address using xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx hexadecimal format.

Timeout Value - Specifies the length of time, in seconds, the switch waits for a response before assuming that a ping has failed.

Number of Ping Requests - Specifies the number of ping requests you want the switch to perform.

4. Click **Start**.

5. To view the ping results, click **Show Ping Results**.
A sample Ping Test Results Page is displayed. See Figure 153.

Ping Test Result

RESULT
Destination IP Address: 192.168.1.3
Pass: 100%
Average Time: 10 ms

Back To Ping Test

Figure 153. Ping Test Results Page

The following information is displayed:

Destination IP Address - Indicates the IP address of the unit that receives the ping.

Pass - Indicates the percentage of times the ping passed.

Average Time - Indicates the time, in milliseconds, the ping was received.

6. Click **Back to Ping Test** to return to the Ping Test Settings Page.

Appendix A
MSTP Overview

This appendix provides background information about the Multiple Spanning Tree Protocol (MSTP) and includes the following sections:

❒ "Overview" on page 368
❒ "Multiple Spanning Tree Instance (MSTI)" on page 370
❒ "General Guidelines" on page 373
❒ "VLAN and MSTI Associations" on page 374
❒ "Ports in Multiple MSTIs" on page 375
❒ "Multiple Spanning Tree Regions" on page 376
❒ "Associating VLANs to MSTIs" on page 381
❒ "VLANs Across Different Regions" on page 383
❒ "Summary of Guidelines" on page 385

Note

To configure the MSTP feature on the AT-GS950/16 switch, go to "Multiple Spanning Tree Protocol" on page 87 for more information.

Overview

In the AT-GS950/16, STP and RSTP are referred to as single-instance spanning trees that search for physical loops across all VLANs in a bridged network. When loops are detected, the active protocol stops the loops by placing one or more bridge ports in a blocking state. See Chapter 4, "STP and RSTP" on page 71 for more information.

As explained in "Spanning Tree and VLANs" on page 78, STP and RSTP can result in VLAN fragmentation where VLANs that span multiple bridges are connected together with untagged ports. The untagged ports creating the links can represent a physical loop in the network, which are blocked by spanning tree. This can result in a loss of communication between different parts of the same VLAN.

One way to resolve this, other than by not activating spanning tree on your network, is to link the switches using tagged ports, which can handle traffic from multiple VLANs simultaneously. The drawback to this approach is that the link formed by the tagged ports can create a bottleneck to your Ethernet traffic, resulting in reduced network performance.

Another approach is to use the Multiple Spanning Tree Protocol (MSTP) feature. This spanning tree shares many of the same characteristics as RSTP in that it features rapid convergence and has many of the same parameters. But the main difference is that while RSTP, just like STP, supports only a single-instance spanning tree, MSTP supports multiple spanning trees within a network.

The following sections describe some of the terms and concepts related to MSTP. If you are not familiar with spanning tree or RSTP, you should first review the Chapter 4, "STP and RSTP" on page 71.

Note

Do not activate MSTP on the AT-GS950/16 switch without first familiarizing yourself with the following concepts and guidelines. Like STP and RSTP, you must activate this MSTP protocol on a switch and then configure the protocol parameters.

Note

The implementation of MSTP in the management software complies fully with the new IEEE 802.1s standard and should be interoperable with any other vendor's fully compliant 802.1s implementation.

Multiple Spanning Tree Instance (MSTI)

The individual spanning trees in MSTP are referred to as Multiple Spanning Tree Instances (MSTIs). An MSTI can span any number of AT-GS950 switches. The switch can support up to 31 MSTIs at a time.

Before creating an MSTI, you first enable MSTP. Then you must assign the MSTI a unique number, referred to as the MSTI ID. The range is 1 to 31. After you have selected an MSTI ID, you define the scope of the MSTI by assigning one or more VLANs to it. An instance can contain any number of VLANs, but a VLAN can belong to only one MSTI at a time.

Resolving VLAN Fragmentation

Following are several examples of how MSTP can be applied.

Figure 154 illustrates two AT-GS950/16 switches, each containing the two VLANs, Sales and Production. The ports of each VLAN on each switch are connected with a direct link using untagged ports. If the switches were running STP or RSTP, one of these two links would be blocked because the links constitute a physical loop. Which link would be blocked depends on the STP or RSTP bridge settings. In Figure 154, the link between the two ports of the Production VLAN is blocked, resulting in a loss of communications between the two parts of the Production VLAN.
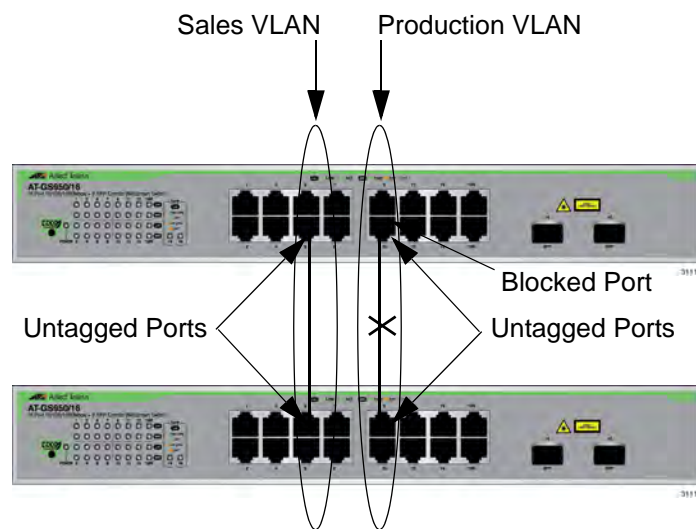
Figure 154. VLAN Fragmentation with STP or RSTP

Figure 155 on page 371 illustrates the same two AT-GS950/16 switches and the same two virtual LANs. But in this example, the two switches are running MSTP, and the two VLANs have been assigned different spanning tree instances. Now that they reside in different MSTIs, both links remain active, enabling the VLANs to forward traffic over their respective direct link.

Figure 155. MSTP Example of Two Spanning Tree Instances
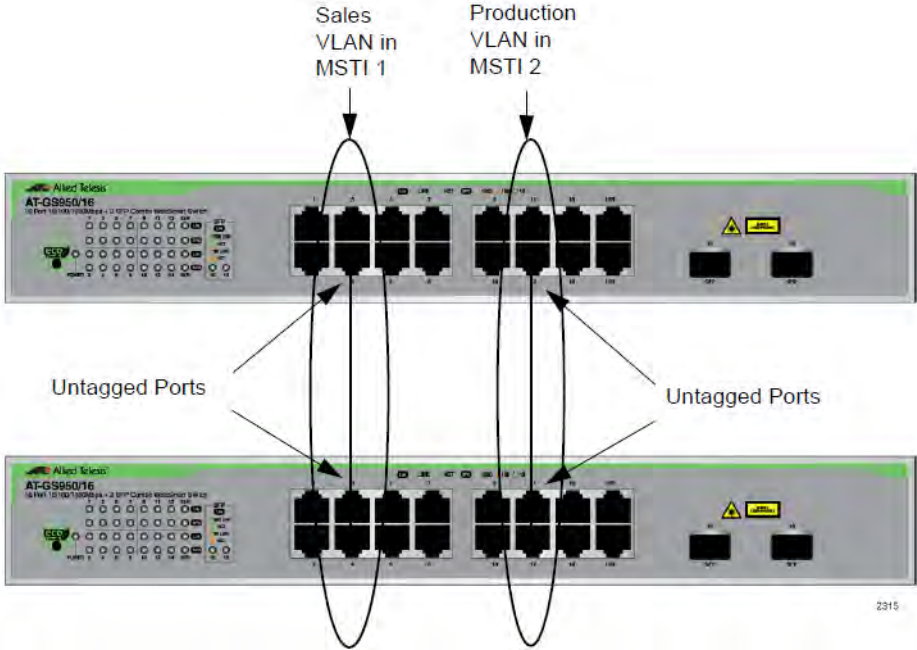
Multiple VLANs Assigned to an MSTI

An MSTI can contain more than one VLAN. This is illustrated in Figure 156 on page 372 where there are two AT-GS950/16 switches with four VLANs. There are two MSTIs, each containing two VLANs. MSTI 1 contains the Sales and Presales VLANs, and MSTI 2 contains the Design and Engineering VLANs.
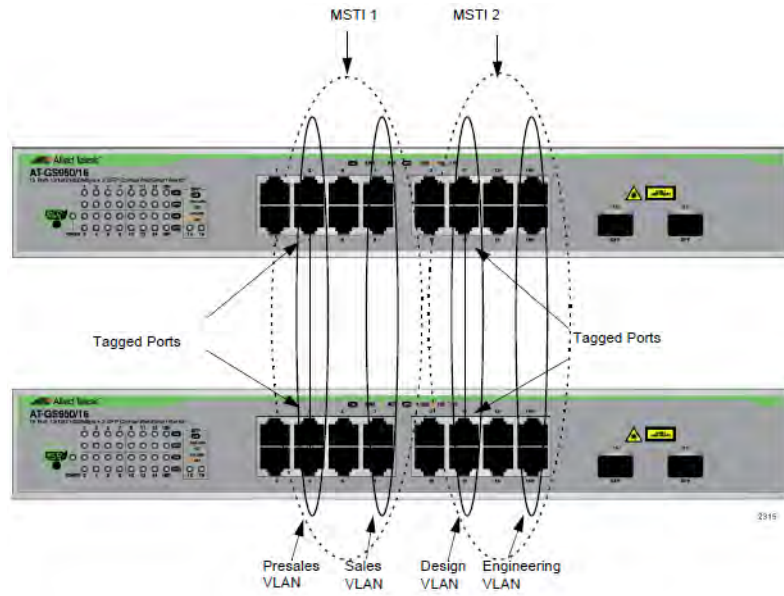
Figure 156. Multiple VLANs in an MSTI

In this example, because an MSTI contains more than one VLAN, the links between the VLAN parts are made with tagged (not untagged) ports so that they can carry traffic from more than one virtual LAN. Referring again to Figure 156, the tagged link in MSTI 1 is carrying traffic for both the Presales and Sales VLANs between the two switches, while the tagged link in MSTI 2 is carrying traffic for the Design and Engineering VLANs.

General Guidelines

Here are the guidelines for MSTIs:

❐ The AT-GS950/16 switch can support up to 31 spanning tree instances, including the CIST.

❐ An MSTI can contain any number of VLANs.

❐ A VLAN can belong to only one MSTI at a time.

❐ A switch port can belong to more than one spanning tree instance at a time by being an untagged and tagged member of VLANs belonging to different MSTIs. This is possible because a port can be in different MSTP states for different MSTIs simultaneously. For example, a port can be in the MSTP blocking state for one MSTI and the forwarding state for another spanning tree instance. For further information, refer to "Ports in Multiple MSTIs" on page 375.

VLAN and MSTI Associations

Part of the task of configuring MSTP involves assigning VLANs to spanning tree instances. The mapping of VLANs to MSTIs is called *associations*. A VLAN, either port-based or tagged, can belong to only one instance at a time, but an instance can contain any number of VLANs.

Ports in Multiple MSTIs

A port can be a member of more than one MSTI at a time if it is a tagged member of one or more VLANs assigned to different MSTIs. In this circumstance, a port might be have to operate in different spanning tree states simultaneously, depending on the requirements of the MSTIs. For example, a port that belongs to two different VLANs in two different MSTIs might operate in the forwarding state in one MSTI and the blocking state in the other.

A port's MSTI parameter settings are divided into two groups. The first group is referred to as generic parameters. These are set just once on a port and apply to all the MSTIs in which the port is a member. One of these parameters is the external path cost, which sets the operating cost of a port connected to a device outside its region. A port, even if it belongs to multiple MSTIs, can have only one external path cost. Another generic parameter designates a port as an edge port or a point-to-point port.

The second group of port parameters can be set differently for each MSTI in which a port is a member. One parameter, the internal path cost, specifies the operating cost of a port when it is connected to a bridge in the same MSTP region. The other parameter in this group sets the port priority, which acts as a tie breaker when two or more ports have equal costs to a regional root bridge.

Multiple Spanning Tree Regions

Another important concept of MSTP is *regions*. An MSTP region is defined as a group of bridges that share exactly the same MSTI characteristics. Those characteristics are:

❐ Region name
❐ Region revision
❐ VLANs
❐ VLAN to MSTI ID associations

A *region name* is a name assigned to a region to identify it. You must assign each region exactly the same name for each bridge in that region, even the same upper and lowercase lettering. Identifying the regions in your network is easier if you choose names that are characteristic of the functions of the nodes and bridges of the region. Examples are Sales Region and Engineering Region.

The *region revision* is an arbitrary number assigned to a region. This number can be used to keep track of the revision level of a region's configuration. For example, you might use this value to maintain the number of times you revise a particular MSTP region. It is important that each bridge in a region has the same region revision number. Practically, however, it is not important that you maintain this number.

The bridges of a particular region must also have the same VLANs. The names of the VLANs and the VIDs must be same on all bridges of a region.

Finally, each of the VLANs across the bridges must be associated to the same MSTI IDs.

If any of the above information is different on two bridges, MSTP considers the bridges as residing in different regions.

Table 7 on page 377 illustrates the concept of regions. It shows one MSTP region consisting of two AT-GS950/16 switches. Each switch in the region has the same configuration name and revision level. The switches also have the same five VLANs, and the VLANs are associated with the same MSTIs.

Table 7. MSTP Region

Configuration Name: Marketing Region, Revision Level 1	
Switch 1	**Switch 2**
MSTI ID 1: VLAN: Sales (VID 2) VLAN: Presales (VID 3)	MSTI ID 1: VLAN: Sales (VID 2) VLAN: Presales (VID 3)
MSTI ID 2: VLAN: Accounting (VID 4)	MSTI ID 2: VLAN: Accounting (VID 4)

The AT-GS950/16 switch determines regional boundaries by examining the MSTP BPDUs received on the ports. A port that receives an MSTP BPDU from another bridge with regional information different from its own is considered to be a boundary port and the bridge connected to the port as belonging to another region.

The same is true for any ports connected to bridges running the single-instance spanning tree STP. Those ports are also considered as part of another region.

Each MSTI functions as an independent spanning tree within a region. Consequently, each MSTI must have a root bridge to locate physical loops within the spanning tree instance. An MSTI's root bridge is called a *regional root*. The MSTIs within a region may share the same regional root or they can have different regional roots.

A regional root for an MSTI must be within the region where the MSTI is located. An MSTI cannot have a regional root that is outside its region.

A regional root is selected by a combination of the *MSTI Bridge Priority* value and the bridge's MAC address. The MSTI priority is analogous to the RSTP bridge priority value. Where they differ is that while the RSTP bridge priority is used to determine the root bridge for an entire bridged network, the MSTI priority is used only to determine the regional root for a particular MSTI.

The range for this parameter is the same as the RSTP bridge priority; from 0 to 61,440 in sixteen increments of 4,096. To set the parameter, you select the increment that represents the desired MSTI priority value according to Table 8.

Table 8. Regional Bridge Priority Value Increments

Bridge Priority Selections	
0	32768
4096	36864
8192	40960
12288	45056
16384	49152
20480	53248
24576	57344
28672	61440

MST Region Guidelines

Following are several points to remember about regions.

❒ A network can contain any number of regions, and a region can contain any number of switches.

❒ The AT-GS950/16 switch can belong to only one region at a time.

❒ A region can contain any number of VLANs.

❒ All of the bridges in a region must have the same configuration name, revision level, VLANs, and VLAN to MSTI associations.

❒ An MSTI cannot span multiple regions.

❐ Each MSTI must have a regional root for locating loops in the instance. MSTIs can share the same regional root or have different roots. A regional root is determined by the MSTI Bridge Priority value and a bridge's MAC address.

❐ The regional root of an MSTI must be in the same region as the MSTI.

Common and Internal Spanning Tree (CIST)

MSTP has a default spanning tree instance called the Common and Internal Spanning Tree (CIST). This instance has an MSTI ID of 0.

This instance has unique features and functions that make it different from the MSTIs that you create yourself. First, you cannot delete this instance or change its MSTI ID. Second, when you create a new port-based or tagged VLAN, it is by default associated with the CIST and is automatically given an MSTI ID of 0. The Default VLAN is also associated by default with CIST.

Another critical difference is that when you assign a VLAN to another MSTI, it still partially remains a member of CIST. This is because CIST is used by MSTP to communicate with other MSTP regions and with any RSTP and STP single-instance spanning trees in the network. MSTP uses CIST to participate in the creation of a spanning tree between different regions and between regions and single-instance spanning tree, to form one spanning tree for the entire bridged network.

MSTP uses CIST to form the spanning tree of an entire bridged network because CIST can cross regional boundaries, while an MSTI cannot. If a port is a boundary port, that is, if it is connected to another region, that port automatically belongs solely to CIST, even if it was assigned to an MSTI, because only CIST is active outside of a region.

As mentioned earlier, every MSTI must have a root bridge, referred to as a regional root, in order to locate loops that might exist within the instance. CIST must also have a regional root. However, the CIST regional root communicates with the other MSTP regions and single-instance spanning trees in the bridged network.

The CIST regional root is set with the *CIST Priority* parameter. This parameter, which functions similar to the RSTP bridge priority value, selects the root bridge for the entire bridged network. If the AT-GS950/16 switch has the lowest CIST Priority value among all the spanning tree bridges, it functions as the root bridge for all of the MSTP regions, and STP and RSTP single-instance spanning trees in the network.

MSTP with STP and RSTP

MSTP is fully compatible with STP and RSTP. If a port on the AT-GS950/16 switch running MSTP receives STP BPDUs, the port only sends STP BPDU packets. If a port receives RSTP BPDUs, the port sends MSTP BPDUs because RSTP can process MSTP BPDUs.

A port connected to a bridge running STP or RSTP is considered to be a boundary port of the MSTP region and the bridge as belonging to a different region.

An MSTP region can be considered as a virtual bridge. The implication is that other MSTP regions, and STP and RSTP single-instance spanning trees, cannot discern the topology or constitution of an MSTP region. The only bridge they are aware of is the regional root of the CIST instance.

Associating VLANs to MSTIs

When you are using Multiple Spanning Tree, Allied Telesis recommends that you assign each of the VLANs to one of the existing MSTIs on a switch. You should not leave any VLAN unassigned, including the Default VLAN. This is to prevent the blocking of a port that should be in the forwarding state. The reason for this guideline is explained below.

An MSTP BPDU contains information identifying the Multiple Spanning Tree instance that is associated with the port transmitting the BPDU packet. By default, all ports of the AT-GS950/16 switch belong to the CIST instance. So the CIST identification is always included in the BPDU. If the port is also a member of a VLAN that has been assigned to an MSTI, that information is included in the BPDU too.

This is illustrated in Figure 157. Port 1 in switch A is a member of the Default VLAN and has been assigned to MSTI ID 10, and port 8 is a member of VLAN 3 assigned to MSTI ID 10. The BPDUs transmitted by port 8 to switch B indicate that the port is a member of both CIST 0 and MSTI 15, while the BPDUs from port 1 indicate the port is a member of the CIST 0 and MSTI 10.
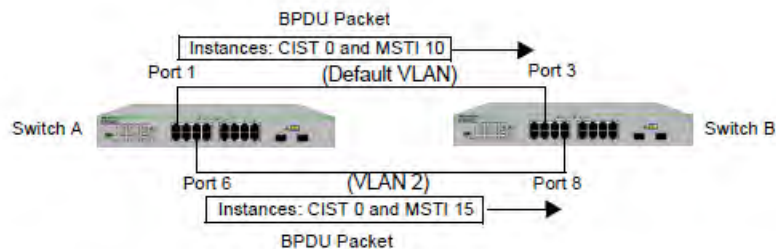
Figure 157. CIST and VLAN Guideline - Example 1

At first glance, it might appear that because both ports belong to CIST, a loop would exist between the switches and that MSTP would block a port to stop the loop. However, within a region, MSTI takes precedence over CIST. When switch B receives a packet from switch A, it uses MSTI, not CIST, to determine whether a loop exists. And because both ports on switch A belong to different MSTIs, switch B determines that no loop exists.

A problem can arise, however, if you assign certain VLANs to MSTIs while leaving others assigned only to CIST. Figure 158 on page 382 illustrates the issue. The network is similar to the previous example. The primary difference is that the VLAN 2 containing port 1 on Switch A has not been assigned to an MSTI and only belongs to CIST (MSTI ID 0).
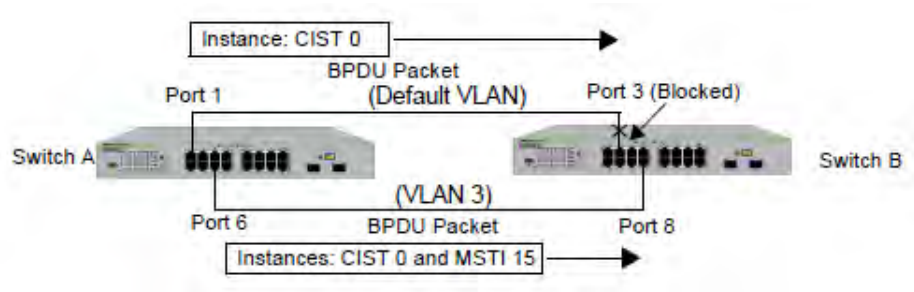
Figure 158. CIST and VLAN Guideline - Example 2

When port 3 on switch B receives a BPDU, the switch notes the port sending the packet belongs only to CIST 0. Therefore, switch B uses CIST 0 in determining whether a loop exists. The result would be that the switch detects a loop because the other port is also receiving BPDU packets from CIST 0. Switch B would block port 3 to cancel the loop.

To avoid this issue, always assign all VLANs on a switch, including the Default VLAN, to an MSTI. This guarantees that all ports on the switch have an MSTI ID and helps to ensure that loop detection is based on MSTI, not CIST.

VLANs Across Different Regions

Special consideration needs to be taken into account when you connect different MSTP regions or an MSTP region and a single-instance STP or RSTP region. Unless planned properly, VLAN fragmentation can occur between the VLANS of your network.

As mentioned previously, only the CIST can span regions. An MSTI cannot. Consequently, you may run into a problem if you use more than one physical data link to connect together various parts of VLANs that reside in bridges in different regions. The result can be a physical loop, which spanning tree disables by blocking ports.

This is illustrated in Figure 159. The example shows two switches, each residing in a different region. Port 7 in switch A is a boundary port. It is an untagged member of the Accounting VLAN, which has been associated with MSTI 4. Port 6 is a tagged and untagged member of two different VLANs, both associated to MSTI 12.

If both switches were a part of the same region, there would be no problem because the ports reside in different spanning tree instances. However, in this example, the switches are part of different regions, and MSTIs do not cross regions. Consequently, the result is that spanning tree would determine that a loop exists between the regions, Switch B would block a port and the Accounting VLAN would be disabled between the two regions.
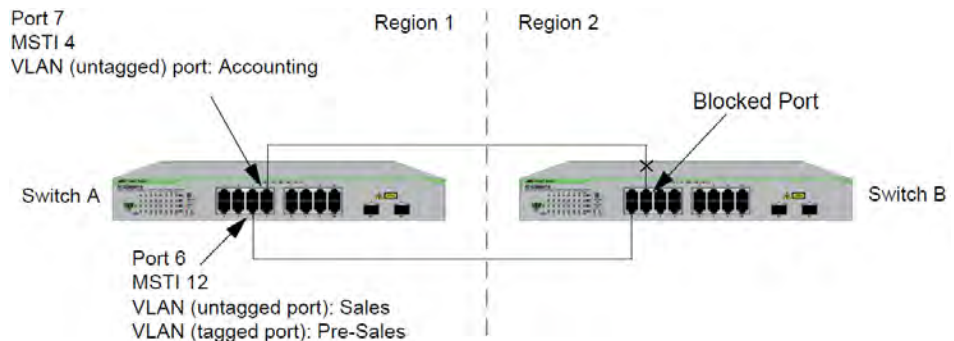
Figure 159. Spanning Regions - Example 1

There are several ways to address this issue. One is to configure only one MSTP region for each subnet in your network. This will eliminate the potential situation of a loop and blocked port(s) between multiple regions.

Another approach is to configure multiple regions in a subnet and group the VLANs that need to span two or more regions into the same MSTI. If other VLANs also exist that do not span multiple regions, they can be assigned to other MSTIs within their respective region.

Here is an example. Assume that you have two regions that contain the following VLANS:

Region 1 VLANs	Region 2 VLANs
Accounting	Accounting
Sales	Sales
Pre-Sales	Pre-Sales
Marketing	Technical Support
Product Management	Software Engineering
Project Management	Hardware Engineering

The 2 regions share 3 VLANs: Accounting, Sales, and Presales. You can group these 3 VLANs into the same MSTI in each region. For instance, for Region 1 you might group the 3 VLANs in MSTI 12, and in Region 2 you could group them into MSTI 16. After they are grouped, you can connect the VLANs across the regions using a link of untagged/tagged ports as shown in Figure 160.
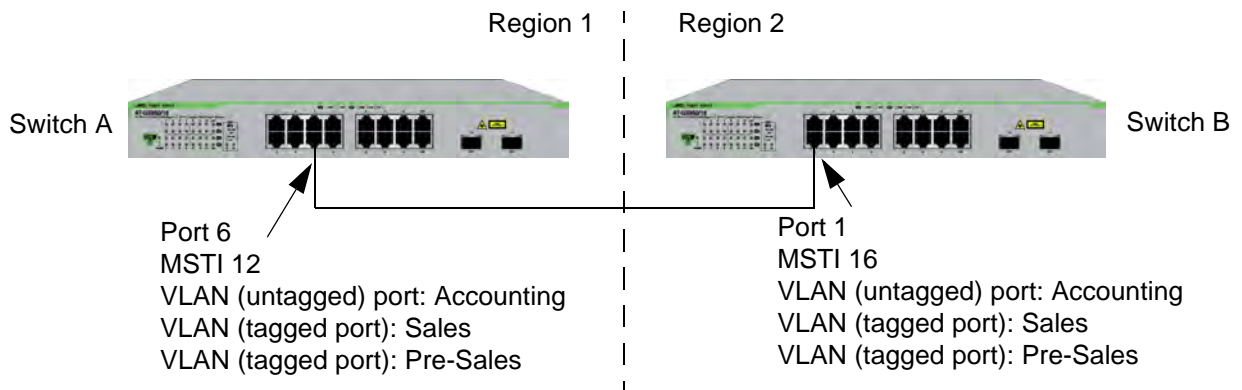
Figure 160. Spanning Regions without Blocking

Summary of Guidelines

Careful planning is essential for the successful implementation of MSTP. This section reviews all of the rules and guidelines mentioned in earlier sections and contains a few extra ones:

- The AT-GS950/16 switch can support up to 32 multiple spanning tree instances, including the CIST, at a time.

- An MSTI can contain any number of VLANs.

- A VLAN can belong to only one MSTI at a time.

- An MSTI ID can be from 1 to 31.

- The CIST ID value cannot be changed.

- A switch port can belong to more than one spanning tree instance at a time. This allows you to assign a port as an untagged and tagged member of VLANs that belong to different MSTIs. What makes this possible is a port's ability to be in different MSTP states for different MSTIs simultaneously. For example, a port can be in the MSTP blocking state for one MSTI and the forwarding state for another spanning tree instance.

- A network can contain any number of regions, and a region can contain any number of AT-GS950/16 switches.

- The AT-GS950/16 switch can belong to only one region at a time.

- A region can contain any number of VLANs.

- All of the bridges in a region must have the same configuration name, revision level, VLANs, and VLAN to MSTI associations.

- An MSTI cannot span multiple regions.

- Each MSTI must have a regional root for locating loops in the instance. MSTIs can share the same regional root or have different roots. A regional root is determined by the MSTI priority value and a bridge's MAC address.

- The regional root of an MSTI must be in the same region as the MSTI.

- The CIST must have a regional root for communicating with other regions and single-instance spanning trees.

- MSTP is compatible with STP and RSTP.

A port transmits CIST information even when it is associated with another MSTI ID. However, in determining network loops, MSTI takes precedence over CIST. (This is explained more in "Associating VLANs to MSTIs" on page 381).

Appendix B

AT-GS950/16 Default Parameters

Table 9 lists the factory default settings for the AT-S114 Management software on the AT-GS950/16 switch. The Parameters reflect the fields found on each web page.

Table 9. AT-S114 Management Software Default Settings

Parameter	AT-GS950/16 Default Setting	Specifications
System/Management		
System Description	AT-GS950/16	-
System Object ID	1.3.6.1.4.207.1.4.166	-
System Name	none	0 - 15 characters
System Location	none	0 - 30 characters
System Contact	none	0 - 30 characters
System/IP Setup		
IP Address	192.168.1.1	IPv4 address in xxx.xxx.xxx.xxx hex format; except 127.0.0.1
Subnet Mask	255.255.255.0	IPv4 address in xxx.xxx.xxx.xxx hex format; except 127.0.0.1
Default Gateway Address	0.0.0.0	IPv4 address in xxx.xxx.xxx.xxx hex format; except 127.0.0.1
DHCP Mode (Client)	Disabled	Enabled/Disabled
System/IP Access List		
IP Restriction Status	Disabled	Enabled/Disabled

Table 9. AT-S114 Management Software Default Settings (Continued)

Parameter	AT-GS950/16 Default Setting	Specifications
IP address	none	IPv4 address in xxx.xxx.xxx.xxx hex format; except 127.0.0.1 / IPv6 address in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx hex format
IP address entries	10 entries	10 entries
System/Administration		
User Name	manager	1 - 12 characters
Password	friend	1 - 12 characters
System/User Interface		
SNMP Agent	Enabled	Enabled/Disabled
Web Server Status	Enabled	Enabled/Disabled
Web Idle Timeout	10 Minutes	3 - 60 Minutes
System/System Time		
Clock Mode	Local Time	SNTP/Local Time
Date Setting(YYYY:MM:DD)	2009/1/1	-
Time Setting(HH:MM:SS)	00:15:59	-
SNTP Primary Server	0:0:0:0	IPv4 address in xxx.xxx.xxx.xxx format / IPv6 address in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx format
SNTP Secondary Server	0:0:0:0	IPv4 address in xxx.xxx.xxx.xxx format / IPv6 address in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx format
SNTP Poll Interval	1 Minute	1 - 60 Minutes
Time Zone	(GMT +09:00)Osaka, Sapporo, Tokyo	GMT -12:00 to GMT +13:00

Table 9. AT-S114 Management Software Default Settings (Continued)

Parameter	AT-GS950/16 Default Setting	Specifications
Daylight Savings Time Status	Disabled	Enabled/Disabled
From (Month:Day:HH:MM)	January:01:00:00	-
To (Month:Day:HH:MM)	January:01:00:00	-
DST Offset	1 hr	-
System/SSL Settings		
SSL Settings	Disabled	Enabled/Disabled
System/DHCP Auto Configuration Settings		
Auto Configuration State	Disabled	Enabled/Disabled
System/System Log Configuration		
Syslog Status	Disabled	Enabled/Disabled
Time Stamp	Enabled	Enabled/Disabled
Messages Buffered Size	50	1 - 200
Syslog Server IP	0.0.0.0	IPv4 address in xxx.xxx.xxx.xxx format / IPv6 address in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx format
Facility	local0	local0 - local 7
Logging Level	info	0 - Emergency level 1 - Alert level 2 - Critical level 3 - Error level 4 - Debug level 5 - Notification level 6 - Informational level 7 - Debug

Table 9. AT-S114 Management Software Default Settings (Continued)

Parameter	AT-GS950/16 Default Setting	Specifications
Physical Interface		
Port	All, 1 - 16	-
Trunk	-	-
Type	1000TX	-
Link Status	Down	Up/Down
Admin Status	Enabled	Enabled/Disabled
Mode	Auto	Auto/10Half/10Full/100Half/100Full/1000Full
Jumbo	Enabled	Enabled/Disabled
Flow Control	Disabled	Enabled/Disabled
EAP Pass	Disabled	Enabled/Disabled
BPDU	Enabled	Enabled/Disabled
Bridge/Spanning Tree/RSTP		
Global RSTP Status	Disabled	Enabled/Disabled
Protocol Version	RSTP	STP/RSTP/MSTP
Bridge Priority	32768	0 - 61440 in 4096 increments
Bridge Hello Time	2 seconds	1 - 10 seconds
Bridge Maximum Age	20 seconds	6 - 40 seconds
Bridge Forward Delay	15 seconds	4 - 30 seconds
Port STP Status	Enabled	Enabled/Disabled
Port Priority	128	0 - 240, 16 steps
Port Admin Cost	0	0 - 200,000,000
Edge	Auto	Auto/ForceTrue/ForceFalse
P2P	Auto	Auto/ForceTrue/ForceFalse
Migrate	Disabled	Disabled/Restart

Table 9. AT-S114 Management Software Default Settings (Continued)

Parameter	AT-GS950/16 Default Setting	Specifications
Bridge/Spanning Tree/MSTP		
Global MSTP Status	Disabled	Enabled/Disabled
Maximum MST Instances	31	1 - 31
Bridge Priority	32768	0 - 61440
Configuration Name	MAC Address of AT-GS950/16 switch	-
Revision Level	0	0 - 65535
Bridge Maximum Age	20 Seconds	6 - 40 Seconds
Bridge Forward Delay	15 Seconds	4 - 30 Seconds
Maximum Hop Count	20	6 - 40
Transmit Hold Count	6	1 - 10
MSTP Instance ID	none	1 - 31
Mapped VLAN	none	-
Admin Cost	0	0 - 200,000,000
Priority	128	0 - 240, 16 steps
Port MSTP Status	Enable	Enable/Disable
Hello Time	2	1 - 9 seconds
Restricted Role	False	True/False
Restricted TCN	False	True/False

Table 9. AT-S114 Management Software Default Settings (Continued)

Parameter	AT-GS950/16 Default Setting	Specifications
Port State	Disable	Enable/Disable/Ignore
Bridge/Trunk Config/Trunking		
Trunk Status	Disabled	Active/Passive/Manual/Disabled
Bridge/Trunk Config/LACP Group Status		
System Priority	32768	32768
System ID	MAC Address of AT-GS950/16 switch	-
Port Priority	0	0 - 65535
Bridge/Mirroring		
Mirroring Status	Disabled	Enabled/Disabled
Mirroring Port	1	All, 1 - 16
Ingress Mirrored Port	-	All, 1 - 16
Egress Mirrored Port	-	All, 1 - 16
Bridge/Loopback Detection		
State	Disabled	Enabled/Disabled
Interval	2 seconds	1 - 32767 seconds
Recover Time	60 seconds	0 or 60 - 1000000
Port	-	All, 1 - 16
Loopback Detection State	Disabled	Enabled/Disabled
Bridge/Static Unicast		
802.1Q VLAN	-	ID 1 - 4093
Port-Based VLAN Index	-	ID 1 - 52
MAC Address	none	xx:xx:xx:xx:xx:xx hex format

Table 9. AT-S114 Management Software Default Settings (Continued)

Parameter	AT-GS950/16 Default Setting	Specifications
Port Member	-	All, 1 - 16
Bridge/Static Multicast		
802.1Q VLAN	-	ID 1 - 4093
Port-Based VALN Index	-	ID 1 - 52
Group MAC Address	none	01:00:5E:00:01:00 - 01:00:5E:7F:FF:FF
Group Member	-	All, 1 - 16
Static Multicast group number	256 entries (shared with IGMP Snooping)	-
Bridge/IGMP Snooping		
IGMP Snooping Status	Disabled	Enabled/Disabled
IGMP Snooping Age-Out Timer	260 seconds	130 - 153025 seconds
Querier Status	Disabled	Enabled/Disabled
Query Interval	125 seconds	6 - 600 seconds
Max Response Time	10 seconds	10 - 25 seconds
Robustness Variable	2	2 - 255
Last Member Query Interval	1 second	1 - 25 seconds
Router Timeout	250 seconds	120 - 1200 seconds
Bridge/Storm Control		
Storm Control DLF	Disabled	Enabled/Disabled
Storm Control Broadcast Control Status	Disabled	Enabled/Disabled
Storm Control Multicast Control Status	Disabled	Enabled/Disabled
Storm Control Threshold	64 pps x 22194	64 pps x 1 - 22194

Table 9. AT-S114 Management Software Default Settings (Continued)

Parameter	AT-GS950/16 Default Setting	Specifications
Ingress Rate Limiting Bandwidth	64 kbps x rate limit	where rate limit (1 - 15625)
Ingress Rate Limiting Status	Disabled	Enabled/Disabled
Egress Rate Limiting Bandwidth	64Kbps X rate limit	where rate limit (1 - 15625)
Egress Rate Limiting Status	Disabled	Enabled/Disabled
Bridge/VLAN		
VLAN Mode	All ports - 802.1Q Tagged VLAN	802.1Q Tagged VLAN or Port-Based VLAN on any port
Tagged VLAN ID	none	2 - 4093
Tagged VLAN Name	none	0 - 32 characters
Tagged Management VLAN	Enabled on DefaultVLAN Disabled on all other VLANs	Always Enabled on Default/VLAN Enabled/Disabled on all other VLANs
Port-Based VLAN Index	none	1 - 52
Port-Based VLAN Name	none	0 - 32 characters
Port-Based Port	Not Member	VLAN Member or Not Member for each port
Port Settings PVID	1	1 - 4093
Port Settings Acceptable Frame Types	All	All/Tagged/Untagged and Priority Tagged
Port Settings Ingress Filtering	Enabled	Enabled/Disabled
Forwarding Table Learning Mode	IVL	IVL/SVL
Private VLAN Source Port	1	All, 1 - 16
Private VLAN Forwarding Ports	All, 1 - 16	All, 1 - 16

Table 9. AT-S114 Management Software Default Settings (Continued)

Parameter	AT-GS950/16 Default Setting	Specifications
Bridge/GVRP		
GVRP Status	Disabled	Enabled/Disabled
Dynamic Vlan Status	Enabled	Enabled/Disabled
Restricted VLAN Registration	Disabled	Enabled/Disabled
GarpJoinTime	200 milli-seconds	10 - 1073741810 milli-seconds
GarpLeaveTime	600 milli-seconds	30 - 2147483630 milli-seconds
GarpLeaveAllTime	10000 milli-seconds	40 - 2147483640 milli-seconds
Bridge/QoS		
QoS Status	Disabled	Enabled/Disabled
Queue for Traffic Classes	Low	Low, Medium, High, Highest
Port Priority	0	0 - 7
DSCP Mapping/ Queue	Low	Low, Medium, High, Highest
Scheduling Algorithm	Strict Priority	Strict Priority/Weighted RoundRobin
SNMP/View Table		
View Name	ReadWrite	1 - 32 characters
Subtree OID	1	-
OID Mask	1	-
View Type	included	included/excluded
SNMP/Group Access Table		
Group Name	ReadOnly/ReadWrite	-
Read View Name	ReadWrite	-
Write View	None	-
Notify View Name	ReadWrite	-
Security Model	v1	v1/v2c/v3
Security Level	NoAuthNoPriv	NoAuthNoPriv/AuthNoPriv/AuthPriv

Table 9. AT-S114 Management Software Default Settings (Continued)

Parameter	AT-GS950/16 Default Setting	Specifications
SNMP User/Group		
User Name	none	1 - 32 characters
Group Name	none	1 - 32 characters
SNMP Version	v1	v1/v2c/v3
encrypted	not checked	not checked/checked
Auth-Protocol	MD5	MD5/SHA
Password	none	-
Priv-Protocol	DES	DES/none
Password	none	-
SNMP/Community Table		
Community Name	none	1 - 32 characters
User Name (View Policy)	none	1 - 32 characters
SNMP/Trap Management		
Trap	Enabled	Enabled/Disabled
Host IP Address	none	IPv4 address in xxx.xxx.xxx.xxx format / IPv6 address in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx format
SNMP Version	v1	v1/v2c/v3NoAuthNoPriv/v3AuthNoPriv/ v3AuthPriv
Community Name/ User Name	none	1 - 32 characters
Access Control Configuration		
Policy Index	none	1 - 65535
Source MAC Address	none	xx:xx:xx:xx:xx:xx hex format
Source MAC Mask Length	none	1 - 48
Destination MAC Address	none	xx:xx:xx:xx:xx:xx hex format

Table 9. AT-S114 Management Software Default Settings (Continued)

Parameter	AT-GS950/16 Default Setting	Specifications
Destination MAC Mask Length	none	1 - 48
VLAN ID	none	0 - 4093
802.1p Priority	none	0 - 7
Ether Type	none	0000 - FFFF (Hex)
DSCP	none	0 - 63
Protocol	none	1 - 255
Source IP Address	none	IPv4 address in xxx.xxx.xxx.xxx hex format / IPv6 address in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx hex format
Source IP Mask Length	none	1 - 32
Destination IP Address	none	IPv4 address in xxx.xxx.xxx.xxx hex format / IPv6 address in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx hex format
Destination IP Mask Length	none	1 - 32
Source Layer 4 Port	none	1 - 65535
Policy Sequence	none	1 - 65535
Destination Layer 4 Port	none	1 - 65535
Rate Control Index	none	1 - 65535
Replaced DSCP	none	0 - 63
Replaced CoS	none	0 - 7
Policy Action Deny/ Permit	Permit	Permit/Deny
Rate Control Index	none	1 - 65535
Committed Rate	none	64 kbps x 1 - 15625
Port List	none	Any combination of ports 1 - 16

Table 9. AT-S114 Management Software Default Settings (Continued)

Parameter	AT-GS950/16 Default Setting	Specifications
RMON		
RMON Status	Disable	Disable/Enable
Statistics Index	none	1 - 65535
Statistics Port	none	-
Statistics Owner	none	-
History Index	none	1 - 65535
History Port	none	-
History Buckets Requested	none	1 - 50
History Interval	none	1 - 3600 seconds
History Owner	none	-
Alarms Index	none	1 - 65535
Alarms Interval	none	1 to 2147483647 seconds
Alarms Variable	none	-
Alarms Sample Type	Absolute value	Absolute value/Delta value
Alarms Rising Threshold	none	1 to 2147483647 seconds
Alarms Falling Threshold	none	1 to 2147483647 seconds
Alarms Rising Event Index	none	1 - 65535
Alarms Falling Event Index	none	1 - 65535
Alarms Owner	none	-
Event Index	none	1 - 65535
Event Description	none	1 - 32 characters
Event Type	None	None/Log/SNMP Trap/Log and Trap
Event Community	none	-

Table 9. AT-S114 Management Software Default Settings (Continued)

Parameter	AT-GS950/16 Default Setting	Specifications
Event Owner	none	1 - 32 characters
Voice VLAN		
Voice VLAN	Disabled	Enabled/Disabled
VLAN ID	1	-
Aging Time	1 hour	1 - 120 hours
COS	7	0 - 7
Auto-Detection	Disabled	Enabled/Disabled
User defined OUI - Description	none	-
User defined OUI - Telephone	none	xx:xx:xx:xx:xx:xx hex format
Security		
Port Access Control NAS ID	fsNas1	1 - 16 characters
Port Access Control	Disabled	Disabled/Enabled
Port Access Control Authentication Method	Local	Local/Radius/TACACS+
Port Number	port 1	ports 1 - 16
Authentication Mode	802.1X	802.1X/MAC Based
Port Control	Force Authorized	Force Authorized/Force Unauthorized/Auto
Re-authentication Status	Disabled	Disabled/Enabled
Supplicant Mode	Single	Single/Multiple
Piggyback Mode	Disabled	Disabled/Enabled
VLAN Assignment	Disabled	Disabled/Enabled
Guest VLAN ID	none	1 - 4093
Transmission Period	30 seconds	1 - 65535 seconds
Quiet Period	60 seconds	1 - 65535 seconds
Supplicant Timeout	30 seconds	1 - 65535 seconds

Table 9. AT-S114 Management Software Default Settings (Continued)

Parameter	AT-GS950/16 Default Setting	Specifications
Maximum Request	2	2 - 10
Re-authentication Period	3600 seconds	1 - 65535 seconds
Server Timeout	30 seconds	1 - 65535 seconds
Dial-In User Name	none	1 - 23 characters
Dial-In User Password	none	1 - 23 characters
Dial-In User Dynamic VLAN	none	1 - 4093 where 0 means ignore
RADIUS Server IP	0.0.0.0	IPv4 address in xxx.xxx.xxx.xxx hex format / IPv6 address in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx hex format
RADIUS Server Port	1812	1 - 65535
RADIUS Accounting Port	1813	1 - 65535
RADIUS Shared Secret	none	1 - 32 characters
RADIUS Accounting Status	Enabled	Enabled/Disabled
TACACS+ Server Priority	1	1 - 5
TACACS+ Server IP Address	0.0.0.0	IPv4 address in xxx.xxx.xxx.xxx hex format / IPv6 address in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx hex format
TACACS+ Server Port	49	1 - 65535
TACACS+ Timeout	5 seconds	1 - 255 seconds
TACACS+ Shared Secret	none	1 - 32 characters

Table 9. AT-S114 Management Software Default Settings (Continued)

Parameter	AT-GS950/16 Default Setting	Specifications
Destination MAC Filter MAC Address	none	Rule: 1. Does not support Multicast MAC address (01:xx:xx:xx:xx:xx) 2. Does not support VRRP MAC address (00:00:5E:xx:xx:xx) 3. First 4 bits must be zero 4. Address cannot be all zeros 5. Cannot add CPU MAC 6. Up to 128 MAC address entries
DHCP Snooping		
General Setting DHCP Snooping	Disabled	Enabled/Disabled
General Setting Pass Through Option 82	Disabled	Enabled/Disabled
General Setting Verify MAC Address	Enabled	Enabled/Disabled
General Setting Backup Database	Disabled	Enabled/Disabled
General Setting Database Update Interval	1200 seconds	600 - 86400 seconds
General Setting DHCP Option 82 Insertion	Disabled	Enabled/Disabled
VLAN Settings VLAN ID	none	1 - 4093
Trusted Interfaces - Trust	Enabled	Enabled/Disabled
Binding Database MAC Address	none	xx:xx:xx:xx:xx:xx hex format
Binding Database IP Address	none	IPv4 address in xxx.xxx.xxx.xxx hex format / IPv6 address in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx hex format
Binding Database VLAN	none	1 - 4093

Table 9. AT-S114 Management Software Default Settings (Continued)

Parameter	AT-GS950/16 Default Setting	Specifications
Binding Database Port	port 1	All, 1 - 16
Binding Database Type	Static	Dynamic/Static
Binding Database Lease Time	none	10 - 4,294,967,295 seconds
LLDP		
LLDP	Disabled	Enabled/Disabled
Message TX Hold Multiplier	4	2 - 10
Message TX Interval	30 seconds	5 - 32768 seconds
LLDP Reinit Delay	2 seconds	1 - 10 seconds
LLDP TX Delay	2 seconds	1 - 8192 seconds
Global Settings Port State	Disabled	Disabled/RxTx/RxOnly/TxOnly
Statistics Chart		
Traffic Comparison Statistics	Inbound Octet Rate (Bytes/s)	24 statistics
Traffic Comparison Auto Refresh	5 seconds	5/10/15/30 seconds
Traffic Comparison Color	Green	12 colors
Error Group Port	1	ports 1 - 16
Error Group Auto Refresh	5 seconds	5/10/15/30 seconds
Error Group Color	Green	12 colors
Historical Status Statistics	Inbound Octet Rate (Bytes)	12 statistics
Historical Status Auto Refresh	5 seconds	5/10/15/30 seconds

Table 9. AT-S114 Management Software Default Settings (Continued)

Parameter	AT-GS950/16 Default Setting	Specifications
Historical Status Port	1	ports 1 - 16
Historical Status Color	Green	12 colors
Tools		
Firmware Upgrade via HTTP Firmware File	none	-
Firmware Upgrade via TFTP TFTP Server IP	none	IPv4 address in xxx.xxx.xxx.xxx hex format; except 127.0.0.1 / IPv6 address in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx hex format
Firmware Upgrade via TFTP Image File Name	none	1 - 64 characters (special characters are dependent on OS file name limitation)
Firmware Upgrade via TFTP Retry Count	none	1 - 20
Configuration File Upload/Download via HTTP Select File	none	-
Configuration File Upload/Download via TFTP TFTP Server IP	none	IPv4 address in xxx.xxx.xxx.xxx hex format; except 127.0.0.1 / IPv6 address in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx hex format
Configuration File Upload/Download via TFTP Config File Name	none	1 - 64 characters (special characters are dependent on OS file name limitation)
Cable Diagnostics Port	1	1 - 16
LED ECO Mode	Disable	Enable/Disable
IEEE 802.3az EEE	Disabled	Enabled/Disabled
Reboot Factory Default Reset	Enabled	Enabled/Disabled

Table 9. AT-S114 Management Software Default Settings (Continued)

Parameter	AT-GS950/16 Default Setting	Specifications
Reboot selection	Normal	Normal/Factory Default/Factory Default Except IP
Ping - Destination IP Address	0.0.0.0	IPv4 address in xxx.xxx.xxx.xxx hex format / IPv6 address in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx hex format
Ping - Timeout Value	3 seconds	1 - 5 seconds
Ping - Number of Ping Requests	10	1 - 10 times