Adtran

Adtran Switch Engine (ASE)

Configuring Layer 2 Services

Configuration Guide

6AMCCG0003-29C
June 2022

To the Holder of this Document

The contents of this manual are current as of the date of publication. Adtran reserves the right to change the contents without prior notice.

Trademark Information

“Adtran” and the Adtran logo are registered trademarks of Adtran, Inc. Brand names and product names included in this document are trademarks, registered trademarks, or trade names of their respective holders.

Disclaimer of Liability

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products are given “as is”, and any liability arising in connection with such hardware or software products shall be governed by Adtran’s standard terms and conditions of sale unless otherwise set forth in a separately negotiated written agreement with Adtran that specifically applies to such hardware or software products.

To the fullest extent allowed by applicable law, in no event shall Adtran be liable for errors in this document for any damages, including but not limited to special, indirect, incidental or consequential, or any losses, such as but not limited to loss of profit, revenue, business interruption, business opportunity or data, that may arise from the use of this document or the information in it.

Be advised that certain security risks are inherent in the use of any telecommunications or networking equipment, including but not limited to, toll fraud, Denial of Service (DoS) attacks, loss or theft of data, and the unauthorized or illegal use of said equipment. ADTRAN OFFERS NO WARRANTIES, EITHER EXPRESSED OR IMPLIED, REGARDING THE PREVENTION, DETECTION, OR DETERRENCE OF TOLL FRAUD, NETWORKING ATTACKS, OR UNAUTHORIZED, ILLEGAL, OR IMPROPER USE OF ADTRAN EQUIPMENT OR SOFTWARE. THEREFORE, ADTRAN IS NOT LIABLE FOR ANY LOSSES OR DAMAGES RESULTING FROM SUCH FRAUD, ATTACK, OR IMPROPER USE, INCLUDING, BUT NOT LIMITED TO, HUMAN AND DATA PRIVACY, INTELLECTUAL PROPERTY, MATERIAL ASSETS, FINANCIAL RESOURCES, LABOR AND LEGAL COSTS. Ultimately, the responsibility for securing your telecommunication and networking equipment rests with you, and you are encouraged to review documentation regarding available security measures, their configuration and implementation, and to test such features as is necessary for your network.

Adtran
901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35814-4000
Phone: (256) 963-8000

Service and Warranty

For information on the service and warranty of Adtran products, visit the Adtran website at http://www.adtran.com/warranty-terms.

Contact Information

To contact Adtran, choose one of the following methods:

Department	Contact Information	
Customer Care	From within the U.S.: From outside the U.S.:	(888) 4ADTRAN ((888)-423-8726) +1 (256) 963-8716
Technical Support	Support Community: Product Support:	www.supportcommunity.adtran.com www.adtran.com/support
Training	Email: Adtran University:	training@adtran.com www.adtran.com/training
Sales	For pricing and availability:	1 (800) 827-0807

Document Revision History

Rev	Date	Description
Rev A	06/2019	Initial Release
Rev B	05/2020	Added note about copying the CPU when using Port Mirroring; also updated document template and supported hardware.
Rev C	06/2022	Put into new template with updated branding. Removed voice VLAN information.

Table of Contents

1. Overview

This document provides an overview of several Layer 2 services and protocols and their configuration on ADTRAN switch engine (ASE) products. Included in this guide are brief introductions to the following Layer 2 services: Link Aggregation (LAG), Link Aggregation Control Protocol (LACP), Media Access Control (MAC) Address Table, Virtual LANs (VLANs), Port Mirroring and Remote Mirroring (RMirror), Generic VLAN Registration Protocol (GVRP), and multiple spanning tree protocols. Also included are the configuration procedures for these features, using both the graphical user interface (GUI) and command line interface (CLI), configuration examples, and a brief troubleshooting section.

The following sections give a brief technological overview of some of the Layer 2 protocols and services provided on the ASE device, as well as a short description of the component parts of these services and their configuration processes on the ASE switch.

Static Link Aggregation (LAG) and Link Aggregation Control Protocol (LACP)

Link Aggregation (LAG), a Layer 2 service defined in the IEEE 802.3ad standard, allows ASE switches to aggregate Ethernet ports between devices. Multiple Ethernet ports can be bundled to form a single logical channel, which increases the link speed for multiple sessions beyond the limits of a single port and increases redundancy on the switch. Configuration of the LAG feature on the ASE device includes creating a LAG group, specifying the ports to add to the group, and defining the aggregation mode.

The Link Aggregation Control Protocol (LACP), also defined in the IEEE 802.3ad standard, is the control protocol used to dynamically create a single logical port from the bundling of several physical Ethernet ports. LACP also functions by linking grouped ports across devices, and operates in one of three modes: active, passive, or static. In active mode, ports transmit LACP frames to connected devices no matter the mode of the connected group. In passive mode, ports transmit LACP frames to connected devices only when they receive LACP frames first. In static mode, LAG configurations are initialized on both components at the same time without the use of LACP, and LAG is always on.

When LACP is used between linked devices, by default, if a better, or higher priority, link becomes available, the link communication switches to the higher priority link. This revertive behavior allows connected devices to utilize the best link for communication and allows for redundancy when links become inactive or go into standby mode. When LACP is configured to be non-revertive, the ability to switch back between links is disabled. Non-revertive behavior can be beneficial when traffic disruption must be avoided. Link priority and timeout settings can be configured on each LACP group to specify which links are used as active or backup links, thus improving communication redundancy and utilizing the dynamic behavior of LACP.

LAG and LACP aggregation modes are set at a Global level across the ASE device, and are used to specify the method for forwarding traffic to destinations based on source or destination Media Access Control (MAC) addresses, IP addresses, or Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port numbers. The forwarding mode is specified once on the ASE device, and applies to all configured LAG and LACP groups.

Media Access Control (MAC) Address Table

The MAC address table is used in Layer 2 switching to keep a record of source and destination MAC addresses for traffic sent over the network. When a traffic packet is sent from one device to another, through the ASE switch, the MAC address table is automatically populated with the source MAC address through MAC address learning. If the destination device is not known, the traffic is flooded to all devices connected to the switch. When a reply is detected, that MAC address is matched with the source MAC address already in the MAC address table, and any further communication between the devices is limited to the same source and destination MAC addresses, without any need to send the traffic to all connected devices. When MAC addresses are learned and added to the table in this manner, they are considered dynamic MAC address table entries. MAC address learning can be configured to automatically learn any source MAC addresses that have not been encountered before, which is the default behavior, and can also be configured to include the learning of secure source MAC addresses, which are not typically added to the MAC address table. MAC address learning behavior is configured at an interface level, on a per-port basis, as well as at a Global level, on a per-virtual local area network (VLAN) basis.

MAC addresses can also be added to the table manually, resulting in static MAC address entries in the MAC address table.

Because the MAC address table holds each pair of source and destination MAC addresses for communication between devices, the number of entries in the table can become quite lengthy. To maintain the table, entries are deleted automatically based on a configurable amount of time. If the specified amount of time is reached, without communication from the source MAC address, the entry is considered aged and is deleted from the table.

Configuration of the MAC address table in the ASE device includes specifying the aging time for table entries, adding static entries to the table when necessary, and configuring the MAC address learning behavior (optional).

Virtual Local Area Networks (VLANs)

VLANs are Layer 2 structures, defined in the IEEE 802.1Q standard, that create logically separated networks operating in the same manner as physical LANs, but without the dependence on physical connection to the same LAN segment. VLANs can be used to separate network traffic by IP subnet, in which case traffic is forwarded only to members of the VLAN and bypasses devices not part of the particular VLAN. Using VLANs in the network can provide additional network security, broadcast and congestion control, and traffic management.

By using VLANs, a switched network can consist of multiple segments, each with its own separate broadcast and multicast domains. VLANs can be configured statically, where each port is assigned to a specific VLAN, or VLANs can be dynamically configured, based on MAC address. Separation of network segments allows for data and users to be isolated, without access to data in a different VLAN, provides the isolation of broadcast and multicast messages on different segments which increases network performance, and also results in easier network management by the logical groupings of users and endpoints.

For example, in a basic VLAN configuration, as shown in *Figure 1 on page 6*, VLANs have been created on two ASE switches in which ports one to ten on Switch A are assigned to VLAN 100, and ports 11 to 20 on Switch A are assigned to VLAN 200. Because Switch A and Switch B share a high-speed link (a Gigabit Ethernet trunk link), then Switch B can also have ports one to ten assigned to VLAN 100 and ports 11 to 20 assigned to VLAN 200. With this configuration, traffic can flow across multiple devices to multiple endpoints on different VLANs.

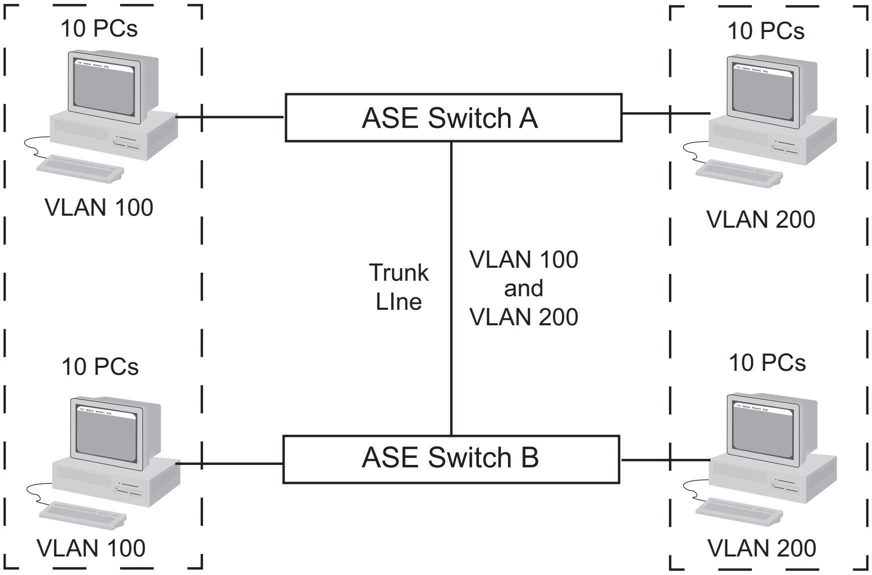


Figure 1. Basic VLAN Topology

ASE devices support several types of VLAN configurations, including basic data VLANs and shared learning VLANs.

Data VLANs

Data VLANs are used by the ASE device to separate network traffic across ports and their associated VLANs. When the ASE device is first powered on, all ports on the device are part of the active default VLAN (VLAN 1). This default VLAN is always in active mode, and cannot be modified or deleted. Each additional VLAN can be created, configured, and assigned to ports on the ASE device to logically separate traffic on the network. When creating a new VLAN, ports are configured according to port mode, VLAN ID, port type, ingress traffic filtering behavior, ingress traffic acceptance behavior, and egress traffic tagging behavior. These behaviors are applied to all ports associated with the newly created VLAN.

Shared VLANs

Shared VLAN learning on the ASE device allows frames that are initially classified to a particular VLAN (based on port VLAN ID or VLAN tag information) to be bridged on a shared VLAN. A shared VLAN is where two or more VLANs are grouped to share common source address information in the MAC address table based on an address filter ID (FID). Shared VLAN learning is beneficial in complex network configurations that utilize asymmetrical cross-VLAN traffic patterns, for example, E-TREE.

Mirroring

Mirroring is a method of monitoring transmitted and received network traffic transversing one, or several, ports on the ASE switch. Mirroring functions by replicating, or mirroring, network traffic from one port or VLAN on another, and provides the collected traffic for network administrators to analyze, diagnose, or troubleshoot network issues using a network analyzer.

The mirroring feature on the ASE device uses three types of mirroring: local mirroring, where the source and destination ports are on the same local switch, source remote mirroring (RMirror), where the port on a local

ASE switch is a source for a separate destination, and destination RMirror, where a port on the local ASE switch is a destination for traffic monitored on a separate source.

Configuring port mirroring depends on configuring a source port, from where the traffic is copied, and a destination port, where the copied traffic is captured. Ports can be configured to capture transmitted traffic only, received traffic only, or both, and can be configured on the local device only (local mirroring) or with a source or destination on a separate device (RMirror).

In local mirroring, multiple source ports can be configured, but only a single destination port is supported. In RMirror, conversely, multiple destination ports are supported (to extend the destination port to another switch), but only a single source port is supported. In addition, RMirror supports the configuration of an internal interface called a reflector port; this interface is configured when using the RMirror feature to redirect traffic to a VLAN created specifically for RMirror traffic. The reflector port does not function as a normal traffic port, but rather only as the RMirror source port.

In addition to local and RMirror port mirroring, ASE devices support VLAN-based mirroring. In VLAN-based mirroring, a VLAN is selected for the mirroring source (rather than a port) and the traffic is mirrored on a configured destination port. VLAN and port mirroring are mutually exclusive; only one mirroring option can be configured at a time.

GARP VLAN Registration Protocol (GVRP)

Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) is a Layer 2 protocol, defined in the IEEE 802.1Q-2005 standard, that is used to dynamically manage VLANs across multiple devices. When GVRP is enabled on network devices, VLAN information, such as VLAN IDs, are communicated between these devices through GVRP protocol data units (PDUs). These PDUs send VLAN registration and deregistration information to GVRP-enabled devices, allowing them to automatically compare the VLAN information in the PDU with the VLAN information currently on the device and dynamically make updates. When new VLANs are detected, GVRP can automatically create a new VLAN, matching the information contained in the PDU. When new ports are added to an existing VLAN, GVRP can automatically add the port to the VLAN configuration as indicated in the PDU. These dynamically created GVRP VLANs and GVRP ports remain active in the device configuration as long as GVRP continues to receive PDUs that contain that VLAN’s ID. When there are no longer any relevant PDUs for the VLAN, or the VLAN has no active links, GVRP deletes the VLAN from the switch.

GVRP operates using timers, which dictate how often GVRP-enabled devices send declarations regarding VLAN attributes, or how long before registered VLAN attributes are deregistered. The timers used by GVRP are actually GARP timers (defined in the IEEE 802.1D 2004 standard), and they must be configured identically across all GVRP-enabled devices in the network.

GVRP configuration on the ASE device includes enabling GVRP globally on the switch, enabling GVRP on a per-port basis, and optionally configuring the timers used by GVRP.

Spanning Tree Protocol

Spanning Tree Protocol (STP) is a Layer 2 protocol, defined by the IEEE 802.1D standard, that is used to provide a single active path between two devices in a local area network (LAN) and prevent loops from forming in the network by identifying and blocking redundant paths. ASE switches support three versions of STP: STP, Rapid STP (RSTP), and Multiple STP (MSTP). A brief overview of the three STP versions used by ASE is included in the following sections.

STP

The original Spanning Tree Protocol (STP) network protocol functions by creating a spanning tree within a switched network. This “tree” consists of multiple connected Layer 2 bridges within the network that operate together to produce a single active path between two network devices. Any links in the network that are not part of the spanning tree are disabled, so that a single, active, non-looped path exists across the network. If the single path is disrupted, previously disabled links are automatically reactivated to restore network connectivity. STP uses an algorithm to catalog each detected link within the network, determine the best loop-free path for network traffic, and automatically deactivate or reactivate redundant links as necessary to maintain the best single path between network devices.

Basic STP functionality is executed by determining a root bridge, identifying a root port, and identifying a designated port. The root bridge is a switch that has all ports actively forwarding information, serves as the center of the network, and is typically chosen automatically by STP based on bridge priority and ID. The root bridge constantly communicates with other switches in the network using Bridge Protocol Data Units (BPDUs). In addition, the STP root bridge determines the preferred and non-preferred network links to be used for network traffic by comparing the cost of each path based on bandwidth. Links with the lowest cost (highest bandwidth) are chosen by STP as the preferred link, and all other possible non-preferred links are disabled by designating the ports that connect to the preferred path as root ports.

Root ports are also specified by network connected switches on all non-root bridges within the network. These root ports are ports that connect these bridges to the root bridge, or ports that use the STP calculated preferred path. This is achieved by configuring switches that do not communicate directly with the root bridge using BDPUs to communicate with each other regarding path costs (adding up all paths and their costs from switch to switch) to determine the path with the lowest overall cost that eventually communicates with the root bridge. The port that uses that path is designated the root port on the non-root bridge.

Designated ports are ports selected from among all the ports on all the bridges on a single LAN segment to send traffic from that segment to the root bridge. When the root bridge, root port, and designated port are all identified, all other ports are blocked. In the event that a primary link fails, ports are reactivated as needed to restore network connectivity.

STP Operation

In STP operation, each switch port with STP enabled is placed in one of five states: blocking, listening, learning, forwarding, or disabled. As STP operates throughout the network segment, each port is initialized, and then placed in these states as it receives BPDU messages indicating the network topology. When STP is enabled, ports are quickly initialized, placed into the listening state, moved to the learning state, and then settled into either the forwarding or blocking state, depending on the network topology and STP configuration.

The following are the characteristics of ports in each STP state:

- **Blocking**: Ports in a blocking state are inactive for the purposes of sending or receiving user network traffic. If these ports were active, they would create a loop, so STP places them in a blocked state to maintain the single, active, non-looped network path. Ports in this state do continue to receive BPDU messages, and can be activated by STP in a failover situation.
- **Listening**: Ports in a listening state are ports that have been activated by STP, and they are listening for information from BDPU messages that may cause them to return to a blocked state. Ports in this state do not forward traffic and do not have addresses in the MAC address table.
- **Learning**: Ports in a learning state populate the MAC address table with learned source addresses but do not yet forward traffic.
- **Forwarding**: Ports in a forwarding state operate in a normal mode, sending and receiving network traffic. BDPUs are used by a port in this state to determine if they are required to return to a blocking state to prevent a looped path.
- **Disabled**: Ports in the disabled state do not pass traffic.

As devices are added to the network, they transition through these port states based on STP timers and forwarding delays, network topology information delivered by BPDUs from the root bridge, and STP determination of lowest cost paths through the network. BPDUs used to communicate STP parameters to network devices include configuration BPDUs, which are used in determining proper STP configurations, and topology change notification (TCN) BPDUs, which disseminate network topology changes to devices in the network.

RSTP

Rapid Spanning Tree Protocol (RSTP), an updated version of STP defined in the IEEE 802.1w standard, is designed to function in the same manner as traditional STP, with the seminal difference that network topology changes are communicated much faster, resulting in faster recovery from switch failures. In addition, RSTP uses fewer port states than STP; when RSTP is enabled and the port is initialized, it moves through three states instead of five. Two of the port states are the same as in STP (the learning and forwarding states), while the third, discarding, functions like the blocking state in STP, in that no network traffic is passed through the port.

In addition, RSTP includes two more port designations than STP. Whereas STP only uses root or designated port roles, RSTP adds the alternate and backup port roles. Alternate ports in RSTP configuration are used to create an alternate path to the root bridge, and backup ports in RSTP configuration are used to create a redundant path to a network segment.

Like STP, ports configured with RSTP enabled move through the varying port states based on BPDU information sent from the root bridge, and change states based on BPDU information continually sent throughout the network.

In addition to the faster communication regarding network topology changes, there are several other differences between STP and RSTP. Unlike STP, RSTP allows for ports to be configured as edge ports if they do not attach to any other bridges, and these edge ports can be detected automatically. In addition, RSTP configuration allows for the separation of point-to-point links between switches (using ports in full-duplex mode), while also supporting the shared links typically used by STP (ports in half-duplex mode).

MSTP

Multiple Spanning Tree Protocol (MSTP), a scalable type of STP/RSTP defined in the IEEE 802.1Q standard, is a protocol that allows for the creation, configuration, and management of multiple spanning tree instances within a network. The main benefit to MSTP is that it provides a method for using spanning tree in networks with multiple VLANs, by creating multiple spanning tree instances (MSTIs) to which individual VLANs, or groups of VLANs, can be statically associated. This type of configuration allows a single network topology to be applied to a configured set of VLANs, rather than limiting the network to a single STP/RSTP instance in which all VLANs on the network are contained.

To achieve the organization of MSTIs, when MSTP is configured, MSTP regions are created. These regions are composed of sets of configured VLANs and their associated MSTIs, are individually named, use the same revision number, and contain a mapping table of which VLANs are associated with which MSTIs.

When MSTP is configured on the switched network, a common internal spanning tree (CIST) instance is created by default, containing its own root bridge that manages and monitors all MSTP regions and their MSTIs. When VLANs are added to the MSTP configuration, they are placed in the CIST by default, until they are manually specified as part of a selected MSTI.

MSTP Operation

Like STP and RSTP, MSTP operates using root bridge instances, port roles, and BPDU messages to maintain at least one data route between two any endpoints on a VLAN. Root bridge instances in MSTP differ from those in STP and RSTP in that they are used to allocate and verify VLAN IDs assigned to bridges in each MSTP region, and to ensure that MSTP configuration identifiers and spanning tree information are transmitted and received in the correct regions. Configuration identifiers used by MSTP include the configuration name for the MSTP region, the revision number, and the mapping of VLANs to MSTIs.

Port roles assigned in MSTP are assigned individually to ports within the CIST and the various individual MSTIs. Both the CIST and MSTI use the root, designated, and backup port roles. MSTIs also use a master port roles. The characteristics of each role are detailed below:

- **CIST Root Port**: A port with the lowest cost path from the MSTP regional root to the CIST root bridge.
- **CIST Designated Port**: A port with the lowest cost path from the LAN segment, through the MSTI, to the CIST root bridge.
- **CIST Backup Port**: A port that provides backup connectivity to the CIST root bridge in failover situations.
- **MSTI Root Port**: A port with the lowest cost path from the MSTI to the MSTP regional root.
- **MSTI Designated Port**: A port with the lowest cost path the LAN segment, through the MSTI, to the MSTP regional root.
- **MSTI Master Port**: A port specifically used to connect all the MSTIs in the MSTP region to a CIST root bridge that lies outside the MSTP region.
- **MSTI Backup Port**: A port that provides backup connectivity for the MSTI in failover situations.

BPDU messages are used by MSTP in the same manner that they are in STP/RSTP, in that they select root bridges (in this case for the CIST and each MSTI), they communicate network topology changes, and they communicate other spanning tree configuration information. However, unlike in STP/RSTP, there is only one type of BPDU message that conveys all spanning tree information in a single message. This characteristic drastically reduces the number of BPDUs sent between LAN segments, VLANs, MSTIs, and the CIST.

2. Hardware and Software Requirements and Limitations

The Layer 2 services and protocols described in this guide are supported on the ASE platforms running ASE firmware 4.4-42 or later as outlined in the *NetVanta ASE Switch Feature Matrix*, available online at https://supportcommunity.adtran.com.

Guidelines for Layer 2 Services Configuration

The following sections include specific information related to the configuration of the Layer 2 services and protocols described in this guide.

LAG and LACP

LAG and LACP forwarding modes can be configured to use source or destination MAC addresses, IP addresses, or TCP and UDP port numbers. By default, source MAC addresses are used. These forwarding modes are applied at a Global level, and are mutually exclusive. LACP groups will use the default form of aggregation for all members in the group.

The maximum number of supported LAG and LACP groups on the ASE device is equal to the total number of ports on the device divided by two. Therefore, the maximum number of supported groups varies depending on the number of ports on the particular ASE device.

The number of members allowed in an LACP group can be restricted by setting the maximum bundle to a number less than the number of group members. Additional members of the group become standby ports and do not forward any frames, unless an active member of the group becomes disabled, in which case the standby member of the highest priority becomes active and takes over frame transmission.

Priority of LACP group members is determined by a setting configured on a per-port basis. The lower the number given to the port in the group, the higher the priority.

VLANs

When the ASE device is first powered on, all ports on the device are part of the active default VLAN (VLAN 1). This default VLAN is always in active mode, and cannot be modified or deleted.

Mirroring

Up to 5 mirroring sessions are available on the ASE device.

The ASE device supports local mirroring (source and destination on the same local device), source RMirror (local device is source, remote device is destination), and destination RMirror (local device is destination, and remote device is source).

VLAN-based mirroring is also supported, where the VLAN is the mirror source and a port is the mirror destination.

RMirror can be configured to use a VLAN ID to specify a VLAN for the mirrored traffic. This option is only available in RMirror. In addition, RMirror utilizes a special reflector port interface. This port redirects traffic to the RMirror VLAN. Configuration of a reflector port is only available if the port is an RMirror source port. STP must be disabled on the reflector port and the port must be added to the VLAN used for RMirror traffic.

When RMirror is configured with a local source but a separate destination device, any devices between the source and the destination (including the destination) must have MAC address learning disabled on the VLAN used for RMirror traffic.

For the mirroring feature to work effectively, a monitoring device must be connected to the destination port, whether local mirroring or RMirror is being used. This monitoring device runs packet monitoring or analyzing software to recover traffic sent by the switch for troubleshooting purposes.

GVRP

To utilize GVRP for dynamic VLAN management, GVRP must be enabled on all devices in the network. In addition, the timers used by GVRP must be configured to the same settings on all GVRP-enabled devices.

GVRP dynamically creates VLANs and ports associated with those VLANs; dynamic ports or VLANs created by GVRP cannot be deleted or modified manually. In addition, you cannot manually remove dynamically added ports from a statically created VLAN. Conversely, any statically created VLANs cannot be deleted by GVRP.

Each VLAN configured on a port with GVRP enabled uses a GVRP resource. By default, **20** GVRP resources are assigned to a port. If a port is configured as part of all VLANs (**1** to **4095**), and it has GVRP enabled, it will require **4096** GVRP resources, and the maximum number of allowed VLANs for GVRP must be reconfigured to **4096**.

Spanning Tree

Before configuring spanning tree on the ASE device, make sure you understand the network topology. Configuration will depend upon the locations of root bridges, network segments, edge ports, MSTP regions, VLAN configuration and use, and the paths used to communicate between those network components. Incorrect configuration of spanning tree protocols for your network topology could result in network connectivity issues.

3. Configuring LAG and LACP Using the GUI

LAG and LACP are configured in similar manners; both LAG and LACP configuration includes creating a LAG/LACP group, assigning ports to the group, and specifying the group aggregation mode. LACP, because it operates dynamically, also includes configuration for port and link priority, link timeouts, and specifies whether revertive behavior is used on the LACP group or not. Once the LAG and LACP groups are created, populated, and defined, the forwarding mode used by both LAG and LACP is defined for the switch.

To configure these settings, connect to the ASE GUI and complete the following tasks:

- *Configuring LAG Groups Using the GUI on page 12*
- *Configuring LACP Using the GUI on page 13*
- *Configuring LAG and LACP Traffic Forwarding Mode Using the GUI on page 15*

These actions serve to create, populate, and define LAG and LACP groups and their behavior on the ASE device.

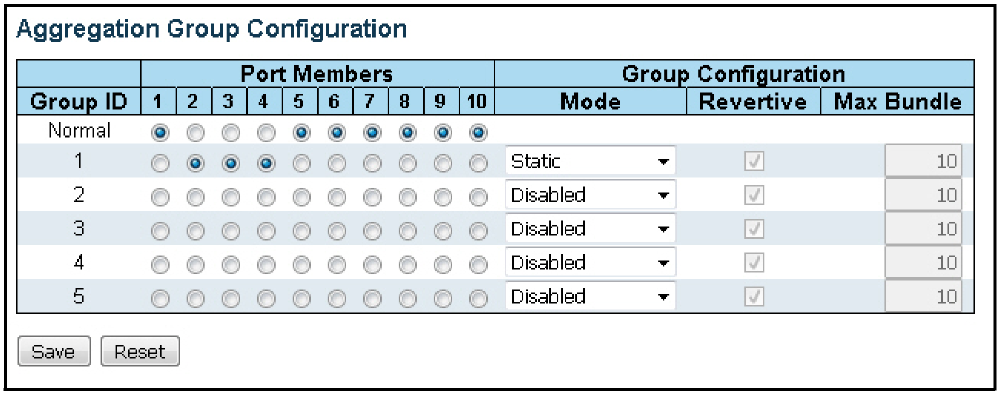
NOTE

All configurations and instructions included in this section are completed on a device returned to the factory default settings.

Configuring LAG Groups Using the GUI

By using LAG, multiple Ethernet ports can be bundled to form a single logical channel, which increases the link speed beyond the limits of a single port and increases redundancy on the switch. Configuration of the LAG feature on the ASE device includes creating a LAG group, specifying the ports to add to the group, and then defining the aggregation mode for both LAG and LACP groups

To access the LAG configuration menu, connect to the GUI and navigate to the **Configuration** tab, then select **Aggregation** > **Groups**. In the **Aggregation Group Configuration** menu, you can configure the LAG group.



Aggregation Group Configuration

	Port Members										Group Configuration		
Group ID	1	2	3	4	5	6	7	8	9	10	Mode	Revertive	Max Bundle
Normal	●	○	○	○	●	●	●	●	●	●			
1	○	●	●	●	○	○	○	○	○	○	Static	☑	10
2	○	○	○	○	○	○	○	○	○	○	Disabled	☑	10
3	○	○	○	○	○	○	○	○	○	○	Disabled	☑	10
4	○	○	○	○	○	○	○	○	○	○	Disabled	☑	10
5	○	○	○	○	○	○	○	○	○	○	Disabled	☑	10

From this menu, you can configure the LAG group settings for the switch by completing these tasks:

1. In the **Port Members** column, specify which ports are members of the appropriate LAG group (from the **Group ID** column) by selecting the appropriate port number check box. In the previous image, ports **2**, **3**, and **4** are selected to be part of LAG group **1**.
2. In the **Mode** column, enable the LAG group by selecting **Static** from the drop-down menu. By default, the LAG group mode is set to **Disabled**, indicating link aggregation is disabled. The **Static** setting specifies that LAG is always on, and that all configurations for the LAG components are applied at once. **Static** also indicates the group is a LAG only group, and that LACP is not used.

NOTE

*The other options from the **Mode** drop-down menu, **LACP (Active)** and **LACP (Passive)**, apply to LACP groups only. In addition, the **Revertive** and **Max Bundle** configurations apply only to LACP groups as well. These configuration options are discussed in more detail in Configuring the LACP Group Using the GUI on page 13.*

3. Once the ports have been assigned to a LAG group, and the LAG group has been enabled using the **Static** mode setting, select **Save** at the bottom of the menu to save the settings.

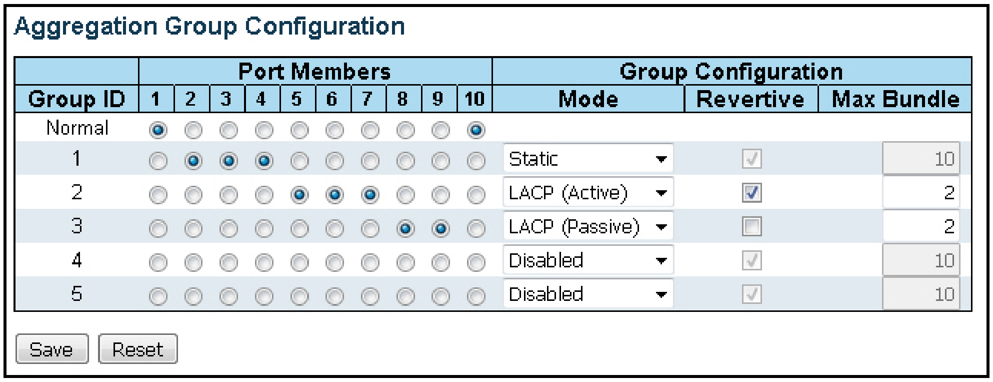
Once the LAG group settings have been saved, the LAG group is configured and its forwarding mode must be set as described in *Configuring LAG and LACP Traffic Forwarding Mode Using the GUI on page 15*.

Configuring LACP Using the GUI

LACP is configured on the ASE switch in a manner similar to LAG configuration, in that it requires a group configuration, with specified ports and mode settings. In addition, LACP configuration also includes the specification of revertive behavior, the maximum bundles allowed on the switch, and the link priority and timeout settings. Once these settings have been specified, the forwarding mode for both the LAG and LACP groups must be defined.

Configuring the LACP Group Using the GUI

The first step of configuring LACP is to configure the LACP group. To begin configuring the LACP group, connect to the GUI and navigate to the **Configuration** tab, then select **Aggregation** > **Groups**. In the **Aggregation Group Configuration** menu, you can configure the LACP group.



Aggregation Group Configuration

	Port Members										Group Configuration		
Group ID	1	2	3	4	5	6	7	8	9	10	Mode	Revertive	Max Bundle
Normal	●	○	○	○	○	○	○	○	○	●			
1	○	●	●	●	○	○	○	○	○	○	Static	☑	10
2	○	○	○	○	●	●	●	○	○	○	LACP (Active)	☑	2
3	○	○	○	○	○	○	○	●	●	○	LACP (Passive)	□	2
4	○	○	○	○	○	○	○	○	○	○	Disabled	☑	10
5	○	○	○	○	○	○	○	○	○	○	Disabled	☑	10

From this menu, you can configure the LACP group settings for the switch by completing these tasks:

1. In the **Port Members** column, specify which ports are members of the appropriate LACP group (from the **Group ID** column) by selecting the appropriate port number check box. In the previous image, ports **5**, **6**, and **7** are selected to be part of LACP group **2**, and ports **8** and **9** are selected to be part of LACP group **3**.
2. In the **Mode** column, enable the LACP group by selecting either **LACP (Active)** or **LACP (Passive)** from the drop-down menu. The **LACP (Active)** option specifies that the LACP group is in active mode, which indicates ports transmit LACP frames to connected devices no matter the mode of the connected group. The **LACP (Passive)** option specifies that the LACP group is in passive mode, which indicates ports transmit LACP frames to connected devices only when they receive LACP frames first. By default, the group mode is set to **Disabled**, indicating link aggregation is disabled.

> **NOTE**
>
> *Because LACP is a dynamic version of LAG, when the **Static** setting is chosen for the group mode (indicating that link aggregation is always on), LACP is not used. Choosing **Static** as the group mode creates a LAG group, rather than an LACP group. When creating a LAG to an AOS based switch, ensure **Static** is configured on both the AES and AOS switches for supported functionality.*

3. Next, specify whether the group operates in revertive mode or not by selecting (or deselecting) the **Revertive** check box. When the **Revertive** check box is selected, it indicates the LACP group operates in revertive mode, and therefore when LACP is used between linked devices, if a better, or higher priority link becomes available, the link communication switches to the higher priority link. This is the default setting for LACP groups and can be beneficial because it allows connected devices to utilize the best link for communication and allows for redundancy when links become inactive or go into standby mode. When LACP is configured to be non-revertive, by deselecting the **Revertive** check box, the ability to switch back to a higher priority link is disabled. Non-revertive behavior can be beneficial when traffic disruption must be avoided. Link priority is configured separately (as described in *Specifying LACP Priority and Timeout Settings Using the GUI on page 14*), but those priorities determine which links are used when the LACP group operates in revertive mode.
4. Next, specify the maximum number of bundles supported in the LACP group by entering a value in the **Max Bundle** field. The number of members allowed in an LACP group can be restricted by setting the maximum bundle to a number less than the number of group members. Additional members of the group become standby ports and do not forward any frames, unless an active member of the group becomes disabled, in which case the standby member of the highest priority becomes active and takes over frame transmission. For example, in the previous screenshot, the **Max Bundle** value for both LACP groups is set to **2**.

NOTE

*You can achieve one to one active and standby behavior on a LACP group by creating a single group with two associated ports, then specifying the **Max Bundle** value as **1**. In this case, the LACP group port with the higher priority actively forwards traffic, while the lower priority port is in standby mode. If the active port goes down for any reason, the standby port takes over and begins forwarding traffic.*

5. Once the ports have been assigned to the LACP group, and the LACP group has been enabled and configured, select **Save** at the bottom of the menu to save the group settings.

You can then specify the link priority and timeout settings for the LACP groups by following the steps described in the next section.

Specifying LACP Priority and Timeout Settings Using the GUI

Once the LACP group has been created, defined, and enabled, you must set the LACP system priority and port priorities for the ports included in the LACP group, as well as specify the port timeout settings.

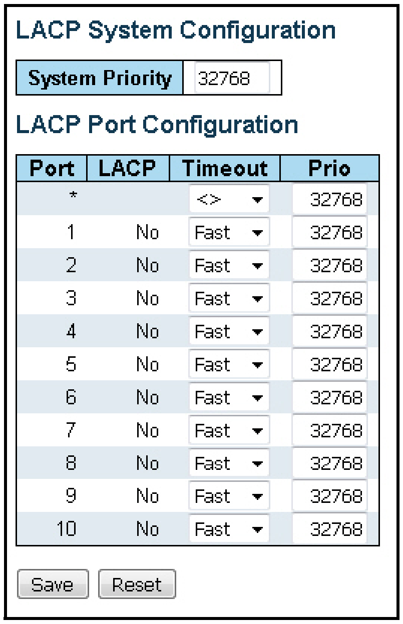
The LACP priority settings include setting the system priority, which determines the priority for the ASE device when connected to other devices using LACP. The priority settings for the ports within the LACP group determine which ports are active, and which are in standby mode. The ports with the higher priority are used as active ports, and the lower priority ports are typically in standby mode, unless they are needed for failover or backup scenarios. The lower the number assigned to the port, the higher the port priority. The same priority hierarchy principles apply to the system priority setting for the ASE device in the LACP network.

The port timeout settings control the period between LACP message transmissions. Transmissions can be configured to be sent each second, or every **30** seconds. By default, messages are sent every second.

To configure LACP priority and timeout settings, connect to the ASE GUI, navigate to the **Configuration** tab, select **Aggregation** > **LACP**, and complete the following tasks:

1. In the **LACP System Configuration** menu, specify the priority for this ASE device in the LACP network by entering a value in the **System Priority** field. This value determines the priority of the ASE device against other devices connected using LACP. The lower the number entered in this field, the higher the

priority of this system. Valid range for the system priority is **1** to **65535**. By default, this value is set to **32768**.



LACP System Configuration

System Priority	32768

LACP Port Configuration

Port	LACP	Timeout	Prio
*		<>	32768
1	No	Fast	32768
2	No	Fast	32768
3	No	Fast	32768
4	No	Fast	32768
5	No	Fast	32768
6	No	Fast	32768
7	No	Fast	32768
8	No	Fast	32768
9	No	Fast	32768
10	No	Fast	32768

2. Next, specify the time between LACP transmissions for the ports included in the LACP group by selecting either **Fast** or **Slow** from the **Timeout** drop-down menu. Selecting **Fast** indicates that LACP transmissions are sent every second, and by default, this is the timeout value for ports in LACP groups. Selecting **Slow** indicates that LACP transmissions are sent every **30** seconds. You can optionally choose to configure all ports to the same transmission setting by specifying a **Timeout** value from the * port row.
3. Lastly, specify the priority for each port in the LACP group by entering a value in the **Prio** field. Valid priority value range is **1** to **65535**, and by default, each port is set to the same priority of **32768**. The lower the value entered in this field, the higher the priority of the port. You can optionally choose to configure all the ports to the same priority setting by specifying a **Prio** value from the * port row.

Once the LACP timeout values and priorities have been configured, select **Save** at the bottom of the menu to save these settings, and complete the LACP and LAG configuration by specifying the LAG and LACP forwarding mode, as described in the following section.

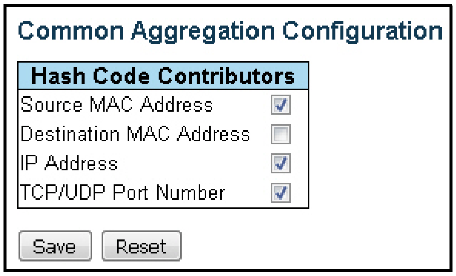
Configuring LAG and LACP Traffic Forwarding Mode Using the GUI

LAG and LACP traffic forwarding modes are set at a Global level across the ASE device, and are used to specify the methods used to determine the destination port for a traffic frame. Forwarding decisions are based on source or destination MAC addresses, IP addresses, or TCP and UDP port numbers. These modes can be combined, and by default, LAG and LACP traffic forwarding modes use the source MAC address, IP address, and TCP/UDP port numbers for determining traffic destinations. The destination MAC address is not used in the default configuration. The forwarding mode is specified once on the ASE device and applies to all configured LAG and LACP groups.

To configure the forwarding mode for LAG and LACP groups, complete the following tasks:

1. Navigate to the **Configuration** tab, and select **Aggregation > Common**.

2. In the **Common Aggregation Configuration** menu, select the methods to use for calculating traffic forwarding practices in LAG and LACP operation by selecting the check box next to the associated method. By default, **Source MAC Address**, **IP Address**, and **TCP/UDP Port Number** are selected.



Common Aggregation Configuration

Hash Code Contributors	
Source MAC Address	☑
Destination MAC Address	□
IP Address	☑
TCP/UDP Port Number	☑

3. Select **Save** at the bottom of the menu to save these settings.

NOTE

Any change in the LAG/LACP traffic forwarding mode stops all traffic forwarding until the mode is fully specified and saved.

Once the LAG and LACP forwarding mode has been defined, the LAG and LACP configuration is complete. You can view LAG and LACP statistics on the ASE device by using the instructions detailed in *Troubleshooting on page 82*.

4. MAC Address Table Configuration Using the GUI

The MAC address table keeps entries of the source and destination MAC addresses used for communication between devices connected to the ASE switch. The addresses can be learned dynamically by the ASE device, or entered manually when needed. Configuration of the MAC address table in the ASE device includes configuring the aging time used for table entries, manually adding static MAC addresses to the table when necessary, and optionally configuring the MAC address learning behavior. The configuration steps for these tasks are described in the following sections:

- *Configuring the MAC Address Table Entry Aging Time Using the GUI on page 16*
- *Adding Static MAC Address Entries to the MAC Address Table Using the GUI on page 17*
- *Configuring MAC Address Table Learning Behavior Using the GUI (Optional) on page 18*

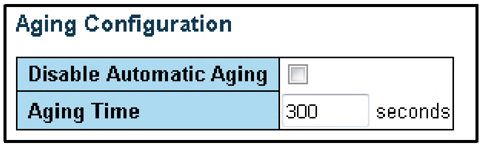
NOTE

All configurations and instructions included in this section are completed on a device returned to the factory default settings.

Configuring the MAC Address Table Entry Aging Time Using the GUI

When traffic from a specific source MAC address ceases, the MAC address table automatically removes the address entry from the table after a configurable amount of aging time. By default, dynamic entries are removed from the MAC address table after **300** seconds. To configure a different aging time, connect to the ASE GUI and complete the following steps:

1. Navigate to the **Configuration** tab, and select **MAC Table**. In the **Aging Configuration** menu of the **MAC Address Table Configuration** page, you can specify the aging time for MAC address entries.



Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

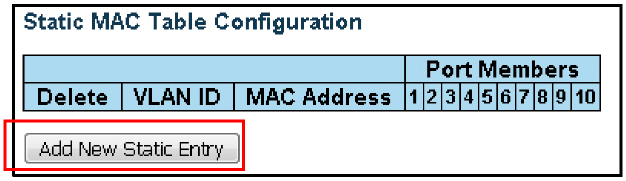
2. Optionally disable automatic entry aging by selecting the **Disable Automatic Aging** check box. By default, this feature is enabled. When disabled, entries remain in the address table until they are removed manually.
3. Enter the desired aging time in the **Aging Time** field. Valid aging time range is **10** to **1000000** seconds. By default, the entry aging time is set to **300** seconds.
4. Select **Save** at the bottom of the menu to save these settings.

Once the MAC address table entry aging time has been configured, you can add entries manually to the MAC address table and optionally configure the MAC address table learning behavior.

Adding Static MAC Address Entries to the MAC Address Table Using the GUI

MAC addresses can be manually entered into the MAC address table by creating static MAC address entries. To add a static MAC address entry to the MAC address table, complete the following steps:

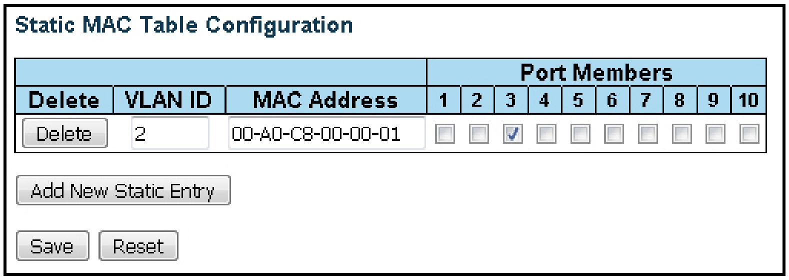
1. Navigate to the **Configuration** tab and select **MAC Table**. In the **Static MAC Table Configuration** menu of the **MAC Address Table Configuration** page, select **Add New Static Entry**.



Static MAC Table Configuration

			Port Members									
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10

2. Next, in the **Static MAC Table Configuration** menu, specify the **VLAN ID** and **MAC Address** for the entry using the appropriate fields. Select the appropriate ports to which the MAC address is associated by selecting the appropriate **Port Members** check box.



Static MAC Table Configuration

			Port Members									
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10
Delete	2	00-A0-C8-00-00-01	□	□	☑	□	□	□	□	□	□	□

3. Select **Save** at the bottom of the menu to save these settings.
4. Any created static MAC address table entries will be listed in the **Static MAC Table Configuration** menu. To delete any of these entries, select the **Delete** button next to the appropriate entry.

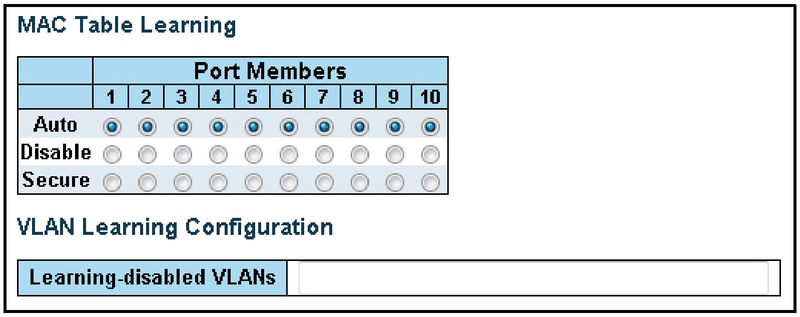
Once the static MAC address table entry has been configured, you can optionally configure the MAC address table learning behavior.

Configuring MAC Address Table Learning Behavior Using the GUI (Optional)

By default, the MAC address table learns new source MAC addresses dynamically when new address are processed by the switch. If traffic is sent from a source MAC address that does not already exist in the MAC address table, it is automatically learned and added to the table. You can optionally change this behavior by disabling MAC address learning on specific ports or VLANs, or by specifying that secure MAC addresses are also learned and added to the MAC address table. By default, secure MAC addresses are not included in the address table.

To change the MAC address table learning behavior, complete the following steps:

1. Navigate to the **Configuration** tab and select **MAC Table**. In the **MAC Address Table Configuration** page, find the **MAC Table Learning** and **VLAN Learning Configuration** menus.



MAC Table Learning

	Port Members									
	1	2	3	4	5	6	7	8	9	10
Auto	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○

VLAN Learning Configuration

Learning-disabled VLANs	

2. By default, the MAC address table is configured to automatically learn all new source MAC addresses (except for secure addresses) on all ports (**Auto** setting). To disable the automatic learning of new source MAC addresses, select the **Disable** check box for all ports on which you want to disable the feature. If you want to add secure MAC addresses to the MAC address table, select the **Secure** check box for each port with secure addresses.
3. To disable the automatic learning of MAC addresses on particular VLANs, enter the VLAN IDs in the **Learning-disabled VLANs** field of the **VLAN Learning Configuration** menu. By default, dynamic learning of MAC addresses is enabled on all configured VLANs.
4. After configuring the address learning behavior for the necessary ports and VLANs, select **Save** at the bottom of the menu to save these settings.

Once the MAC address table entries, learning behavior, and aging time have been configured, the MAC address table configuration is complete. You can view MAC address table statistics on the ASE device by using the instructions detailed in *Troubleshooting on page 82*.

5. VLAN Configuration Using the GUI

VLANs are used on the ASE device to logically divide traffic across the network. VLANs can be configured for specific types of data streams, including VoIP traffic, and can be configured so that specific ports are used by designated VLANs for specific traffic, thus making network management much easier.

When creating a new VLAN, ports are configured according to port mode, VLAN ID, port type, ingress traffic filtering behavior, ingress traffic acceptance behavior, and egress traffic tagging behavior. To configure VLANs on the ASE device, complete the following tasks:

- *Configuring VLAN Port Modes and VLAN IDs Using the GUI on page 19*
- *Configuring VLANs for Access Ports Using the GUI on page 20*
- *Configuring VLANs for Trunk and Hybrid Ports Using the GUI on page 21*
- *Configuring Shared VLAN Learning Using the GUI on page 26*
- *Configuring Shared VLAN Learning Using the GUI on page 26*

NOTE

All configurations and instructions included in this section are completed on a device returned to the factory default settings.

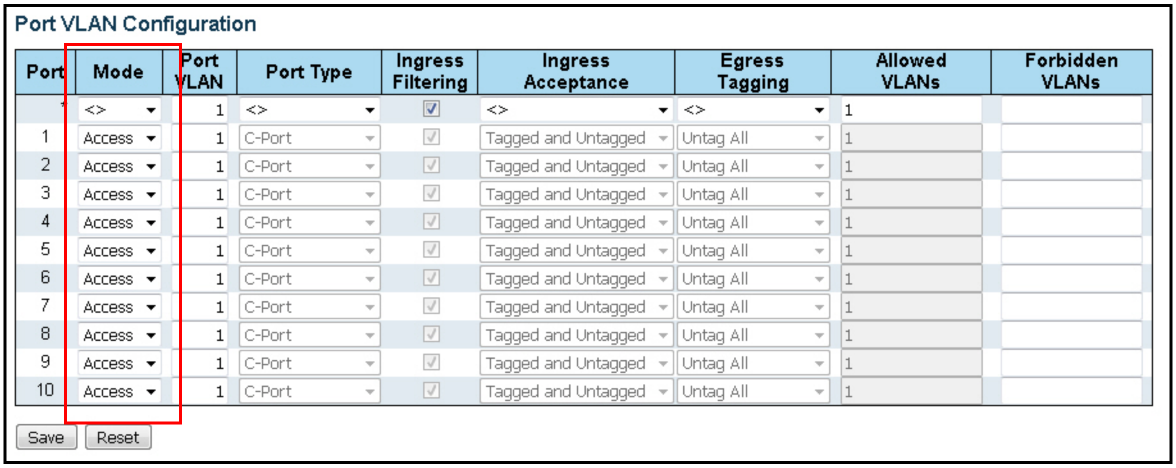
Configuring VLAN Port Modes and VLAN IDs Using the GUI

The first step in VLAN configuration is to specify the port mode for the ports to be used in the VLAN and associate the port with a VLAN ID. There are three supported types of port modes in the ASE device: access, trunk, and hybrid modes. Different port modes serve different purposes on the network and include different types of configuration. For example, access ports usually connect to end points on the network, trunk ports are used to connect to other switches in the network, and hybrid ports perform in a similar manner to trunk ports, but with additional configurations and abilities. *Table 1 on page 19* describes the characteristics of each port mode type.

Table 1. VLAN Port Mode Types and Characteristics

Port Mode	Typical Usage	Characteristics
Access	Used to connect the switch to endpoints on the network	• Default port mode • Member of exactly one VLAN (VLAN 1 by default, either Port VLAN or Access VLAN) • Accepts untagged and C-tagged frames • Transmits untagged egress frames
Trunk	Used to connect the switch to other switches on the network	• Member of all existing VLANs by default • Can transmit traffic on multiple VLANs simultaneously • All frames are tagged on egress by default, except for those classified to the Port VLAN or Native VLAN • Egress tagging can be enabled for all frames, however that means only tagged frames are accepted upon ingress
Hybrid	Used to connect the switch to other switches on the network, and operate similarly to trunk ports	• Includes all characteristics of trunk ports • Can be configured to be VLAN tag unaware • Can be configured to be C-tag, S-tag, or S-Custom-tag aware • Ingress filtering can be configured and controlled • Frame ingress acceptance and egress frame tagging can be configured independently

To specify the port mode for VLAN configuration, connect to the ASE GUI, navigate to the **Configuration** tab, and select **VLANs** > **Configuration**. In the **Port VLAN Configuration** menu, select the appropriate port mode (**Access**, **Trunk**, or **Hybrid**) from the **Mode** drop-down menu.



Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Once you have specified the port mode for the VLAN, specify the VLAN ID associated with the port by entering the VLAN ID in the **Port VLAN** field of the **Port VLAN Configuration** menu (as shown in *Figure* on page 20). By default, all ports are associated with the default VLAN **1**. Valid VLAN ID range is **1** to **4095**.

After configuring the port mode type and associating a VLAN ID with the port, continue VLAN configuration by following the steps outlined in *Configuring VLANs for Access Ports Using the GUI on page 20* for access ports, and *Configuring VLANs for Trunk and Hybrid Ports Using the GUI on page 21* for trunk or hybrid ports.

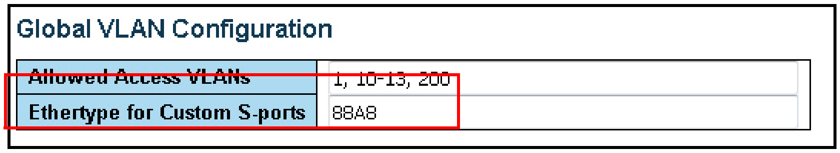
Configuring VLANs for Access Ports Using the GUI

If the port mode type for the VLAN was specified as **Access**, the remainder of the VLAN configuration is based on creating data connections to the endpoints in the network. The **Access** port mode is the default setting for all ports, in the default VLAN, and therefore only a few additional configuration steps are necessary to complete VLAN configuration for access ports.

By default, access ports have ingress filtering enabled, which indicates that incoming traffic for a VLAN of which the port is not a member is discarded. In addition, access ports are configured as a C-port, so that on ingress, frames with a VLAN tag with a tag protocol ID (TPID) of 0x8100 are associated with the VLAN ID embedded in the tag. If the frame is untagged, or priority tagged, the frame is associated with the VLAN ID configured on the port. If frames must be tagged on egress, they are tagged with a C-tag. These settings cannot be changed on an access port.

The only additional configurations for VLAN access ports is to specify VLANs allowed or forbidden by the access ports. To configure the allowed and forbidden VLANs for the access ports, follow these steps:

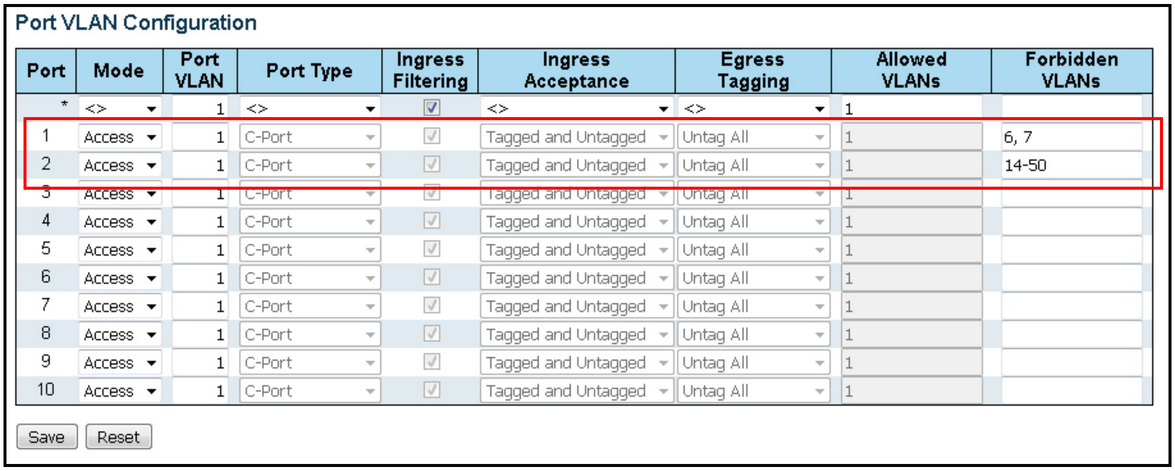
1. Navigate to the **Configuration** tab, and select **VLANs** > **Configuration**. In the **Global VLAN Configuration** menu, specify the VLANs allowed by the access ports in the **Allowed Access VLANs** field as shown below. You can enter a specific VLAN, a range of VLANs separated by a hyphen or comma, or a combination of both. Valid VLAN range is **1** to **4095**. These allowed VLANs apply to all ports in **Access** mode.



Global VLAN Configuration

Allowed Access VLANs	1, 10-13, 200
Ethertype for Custom S-ports	88A8

2. After specifying the allowed VLANs for the access ports, you can specify any forbidden VLANs for the port in the **Port VLAN Configuration** menu (**Configuration** tab, **VLANs** > **Configuration**). Enter any forbidden VLANs in the **Forbidden VLANs** field for the appropriate port(s) as shown below. The VLANs entered in this field are VLANS of which these ports are never allowed to become a member. This setting can be useful when dynamic VLAN protocols, such as Multiple VLAN Registration Protocol (MVRP) or GVRP must be prevented from dynamically adding these ports to VLANs. By default, this field is blank. You can enter a specific VLAN, a range of VLANs separated by a hyphen or comma, or a combination of both. Valid VLAN range is **1** to **4095**.



Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	6, 7
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	14-50
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

3. After configuring any allowed or forbidden VLANs for the ports in access modes, select **Save** at the bottom of the menu to save these settings.

Once you have configured the allowed or forbidden VLANs for the access ports, the VLANs associated with those ports have been configured. You can choose to configure VLANs for ports in trunk or hybrid mode, or view details of the VLAN configuration statistics on the ASE device by using the instructions detailed in *Troubleshooting on page 82*.

Configuring VLANs for Trunk and Hybrid Ports Using the GUI

If the port mode type for the VLAN was specified as **Trunk** or **Hybrid**, there are several additional configurations available for connecting these ports, and their associated VLANs, to other switches on the network. Both trunk and hybrid port modes have configurable port types, ingress acceptance criteria, egress traffic tagging preferences, and allowed and forbidden VLANs. In addition, hybrid ports can be configured with ingress filtering disabled.

To configure these settings, connect to the ASE GUI and complete the following tasks:

- *Configuring VLAN Port Types Using the GUI (Hybrid Ports Only) on page 22*
- *Configuring VLAN Ingress Filtering Using the GUI (Hybrid Ports Only) on page 23*
- *Configuring VLAN Ingress Acceptance Criteria for Ports Using the GUI (Hybrid Ports Only) on page 23*
- *Configuring Egress Traffic Tagging for Trunk and Hybrid Ports Using the GUI on page 24*
- *Specifying Allowed and Forbidden VLANs for Trunk and Hybrid Ports Using the GUI on page 25*

These actions serve to create, configure, and specify VLAN behavior for trunk and hybrid ports on the ASE device.

Configuring VLAN Port Types Using the GUI (Hybrid Ports Only)

For VLAN ports configured in **Hybrid** mode, you can specify whether the VLAN tag of ingress traffic is used to classify the incoming frames to a particular VLAN by configuring the port type associated with the VLAN port. Four port types are supported: **Unaware**, **C-Port**, **S-Port**, and **S-Custom-Port**. These port types are associated with specific TPIDs, and when configured, use the TPID to classify ingress traffic to the VLAN associated with the port.

When the port type is set to **Unaware**, all ingress frames (whether carrying a VLAN tag or not) are classified to the VLAN associated with the port.

When the port type is set to **C-Port**, all ingress frames with a VLAN tag TPID of 0x8100 are classified to the VLAN ID embedded in the tag. If a frame is untagged, or has a priority tag, the frame is classified to the VLAN associated with the port. With this setting, any egress frames that must be tagged are tagged with a C-tag.

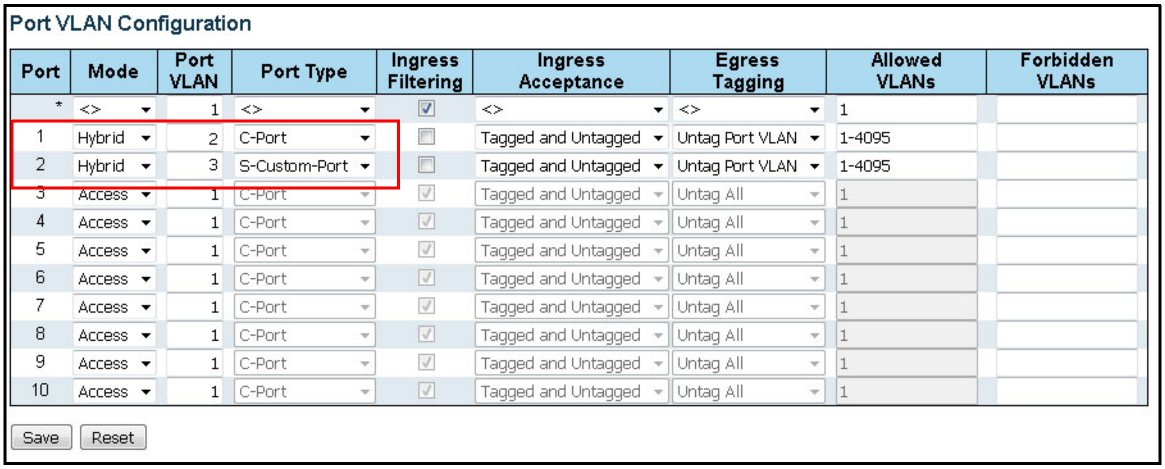
When the port type is set to **S-Port**, all ingress frames with a VLAN tag TPID of 0x8100 or 0x88A8 are classified to the VLAN ID embedded in the tag. If a frame is untagged, or has a priority tag, the frame is classified to the VLAN associated with the port. With this setting, any egress frames that must be tagged are tagged with an S-tag.

When the port type is set to **S-Custom-Port**, all ingress frames with a VLAN tag TPID of 0x8100, or a value equal to the Ethertype configured for S-Custom-Ports, are classified to the VLAN ID embedded in the tag. If a frame is untagged, or has a priority tag, the frame is classified to the VLAN associated with the port. With this setting, any egress frames that must be tagged are tagged with the custom S-tag.

> **NOTE**
>
> *By default, all ports in **Trunk** or **Access** mode are set to **C-Port**. This setting cannot be changed for ports in these modes.*

To configure a port type for VLAN ports in **Hybrid** mode, follow these steps:

1. Navigate to the **Configuration** tab, and select **VLANs** > **Configuration**. In the **Port VLAN Configuration** menu, select the appropriate port type from the **Port Type** drop-down menu for the **Hybrid** mode ports as shown below. Available port types include **Unaware**, **C-Port**, **S-Port**, and **S-Custom-Port**.

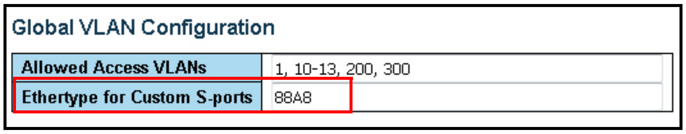


Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Hybrid	2	C-Port	☐	Tagged and Untagged	Untag Port VLAN	1-4095	
2	Hybrid	3	S-Custom-Port	☐	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

2. If the port type selected is **S-Custom-Port**, you must specify the Ethertype (TPID) for the custom setting. Navigate to the **Global VLAN Configuration** menu (**Configuration** tab, **VLANs** > **Configuration**), and

enter the hexadecimal value for tagged frames to be used for classification purposes on the port in the **Ethertype for Custom S-ports** field. By default, this value is set to **88A8**.



Global VLAN Configuration

Allowed Access VLANs	1, 10-13, 200, 300
Ethertype for Custom S-ports	88A8

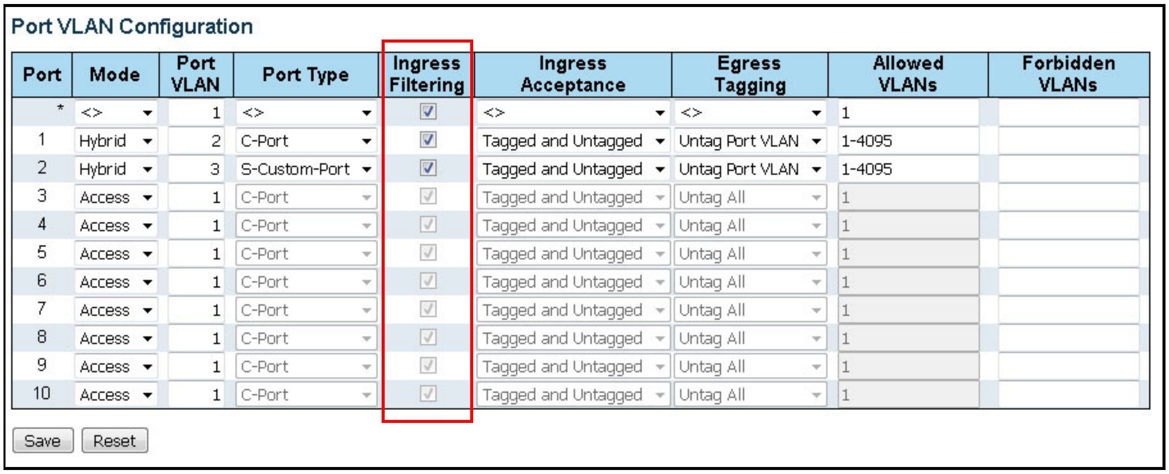
3. After specifying the port type for the VLAN port, and specifying the custom S-port TPID if necessary, select **Save** at the bottom of the menu to save these selections.

After configuring the port type for the ports in **Hybrid** mode, you can continue port VLAN configuration by specifying the VLAN ingress filtering parameters as described in the next section.

Configuring VLAN Ingress Filtering Using the GUI (Hybrid Ports Only)

By default, ports configured in **Hybrid** mode have ingress filtering disabled. All other port types (**Access** and **Trunk**) have ingress filtering enabled by default, and that setting cannot be changed. Enabling ingress filtering on a hybrid port indicates that incoming traffic for a VLAN of which the port is not a member is discarded.

To enable ingress filtering on a hybrid port, navigate to the **Port VLAN Configuration** menu (**Configuration** tab, **VLANs** > **Configuration**) and select the **Ingress Filtering** check box for the port.



Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Hybrid	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
2	Hybrid	3	S-Custom-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

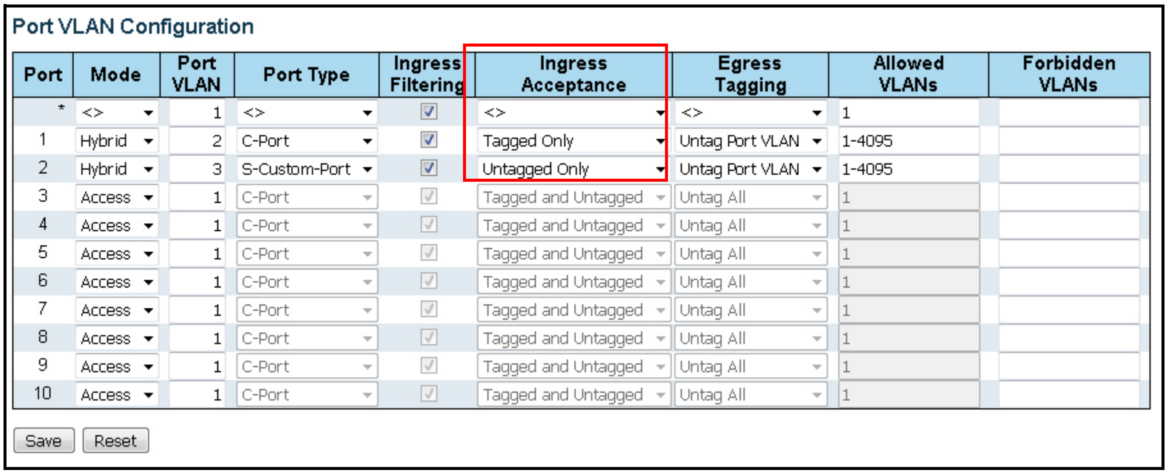
Once **Ingress Filtering** has been enabled, select **Save** at the bottom of the menu to save these settings. You can then continue to configure hybrid VLAN ports by specifying their ingress traffic acceptance criteria as described in the next section.

Configuring VLAN Ingress Acceptance Criteria for Ports Using the GUI (Hybrid Ports Only)

After specifying the port type and ingress filtering behavior for ports in **Hybrid** mode, you can begin configuring the ingress acceptance criteria for these ports. Only ports in **Hybrid** mode can be configured to specify the type of frames that are accepted on ingress. By default, ports in either **Access** or **Trunk** modes accept either tagged or untagged frames, and this setting cannot be changed. Options available for ports in **Hybrid** mode include **Tagged and Untagged**, **Tagged Only**, and **Untagged Only**.

When the accepted frame types for the port is specified as **Tagged and Untagged**, both types of frames are accepted. When the accepted frame type is specified as **Tagged Only**, only tagged ingress frames are accepted and all others are discarded. When the accepted frame type is specified as **Untagged Only**, only untagged ingress frames are accepted and all others are discarded.

To specify the accepted ingress frame type for the hybrid port, navigate to the **Port VLAN Configuration** menu (**Configuration** tab, **VLANs** > **Configuration**) and select the appropriate option from the **Ingress Acceptance** drop-down menu. By default, ports are configured to accept both tagged and untagged frames.



Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Hybrid	2	C-Port	☑	Tagged Only	Untag Port VLAN	1-4095	
2	Hybrid	3	S-Custom-Port	☑	Untagged Only	Untag Port VLAN	1-4095	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

After specifying the ingress frame types accepted on the hybrid port, select **Save** at the bottom of the menu to save these settings. Continue the VLAN configuration by specifying the tagging preferences for egress traffic on both hybrid and trunk ports as described in the following section.

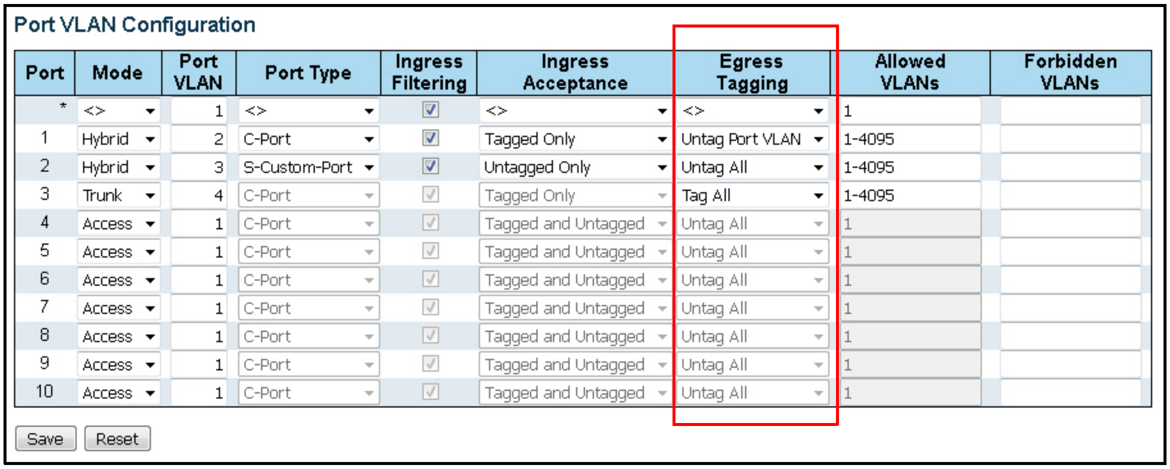
Configuring Egress Traffic Tagging for Trunk and Hybrid Ports Using the GUI

While access ports do not tag egress traffic, ports that are configured in either **Trunk** or **Hybrid** mode can be configured to control the tagging of egress traffic as needed. Egress traffic tagging actions can be specified as one of the following selections:

- **Untag Port VLAN**: This selection indicates that traffic associated with the port's VLAN is transmitted untagged at egress. Any traffic not associated with the port's VLAN is transmitted with the relevant tag. This is the default setting for both trunk and hybrid ports.
- **Tag All**: This selection indicates that all egress traffic, whether classified as part of the port's VLAN or not, is transmitted with a tag.
- **Untag All**: This selection indicates that all egress traffic, whether classified as part of the port's VLAN or not, is transmitted without a tag. This option applies to hybrid ports only.

To specify the port's tagging behavior for egress traffic, navigate to the **Port VLAN Configuration** menu (**Configuration** tab, **VLANs** > **Configuration**) and select the appropriate option from the **Ingress**

Acceptance drop-down menu. By default, both trunk and hybrid ports do not tag egress frames for traffic associated with the port's VLAN.



Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Hybrid	2	C-Port	☑	Tagged Only	Untag Port VLAN	1-4095	
2	Hybrid	3	S-Custom-Port	☑	Untagged Only	Untag All	1-4095	
3	Trunk	4	C-Port	☑	Tagged Only	Tag All	1-4095	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

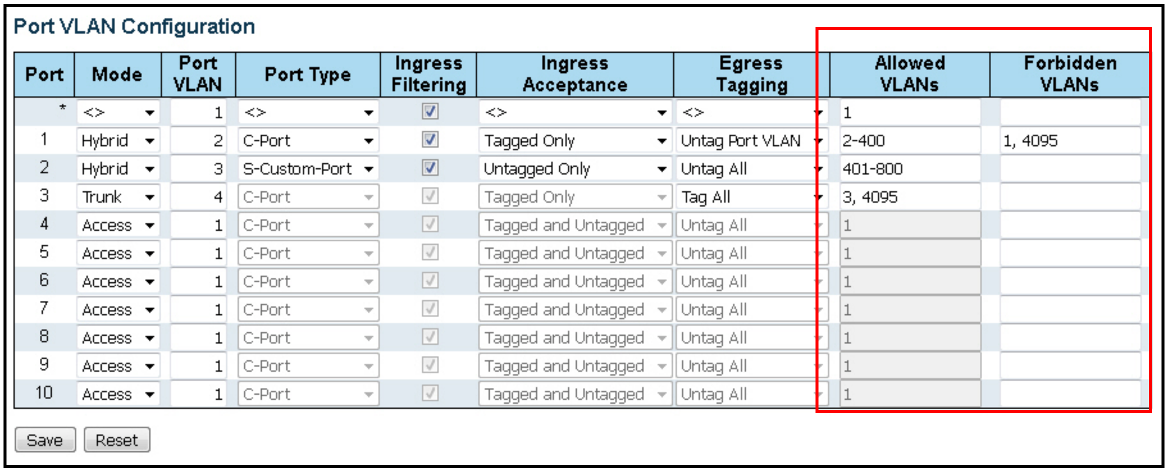
After specifying the egress frame tagging behavior on the trunk or hybrid ports, select **Save** at the bottom of the menu to save these settings. Continue the VLAN configuration by specifying the allowed or forbidden VLANs on both hybrid and trunk ports as described in the following section.

Specifying Allowed and Forbidden VLANs for Trunk and Hybrid Ports Using the GUI

For both trunk and hybrid ports, you can specify of which VLANs each port type is allowed to become members, and of which VLANs the port is forbidden to become a member. By default, all ports are allowed to become members of all available VLANs.

To specify the allowed and forbidden VLANs for trunk and hybrid ports, navigate to the **Port VLAN Configuration** menu (**Configuration** tab, **VLANs** > **Configuration**) and enter the appropriate VLAN IDs in the **Allowed VLANs** and **Forbidden VLANs** fields. You can enter a specific VLAN, a range of VLANs separated by a hyphen or comma, or a combination of both. Valid VLAN range is **1** to **4095**. By default, both trunk and hybrid ports are members of all available VLANs (**1-4095**).

By default, the **Forbidden VLANs** field is blank. Assigning forbidden VLANs can be useful when dynamic VLAN protocols, such as MVRP or GVRP must be prevented from dynamically adding these ports to VLANs.



Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Hybrid	2	C-Port	☑	Tagged Only	Untag Port VLAN	2-400	1, 4095
2	Hybrid	3	S-Custom-Port	☑	Untagged Only	Untag All	401-800	
3	Trunk	4	C-Port	☑	Tagged Only	Tag All	3, 4095	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

NOTE

*This section describes how to assign allowed and forbidden VLANs for ports set to **trunk** or **hybrid** mode. For ports in **access** mode, follow the instructions detailed in Configuring VLANs for Access Ports Using the GUI on page 20.*

After specifying the allowed and forbidden VLANs for the trunk or hybrid ports, select **Save** at the bottom of the menu to save these settings.

Once you have configured the allowed or forbidden VLANs for the trunk and hybrid ports, the VLANs associated with those ports have been configured. You can view details of the VLAN configuration statistics on the ASE device by using the instructions detailed in *Troubleshooting on page 82*.

Configuring Shared VLAN Learning Using the GUI

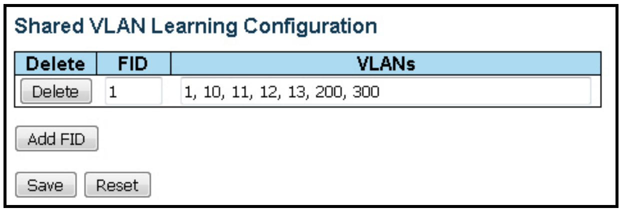
Shared VLAN learning (SVL) allows frames that are initially classed to a particular VLAN to be bridged on a shared VLAN. When enabled, SVL allows two or more VLANs to be grouped together to share common source address information in the MAC address table. SVL can be beneficial for more complex, asymmetrical cross-VLAN traffic patterns and configurations, such as E-TREE.

SVL operation depends on the filter ID (FID) associated with the MAC address in the MAC address table. Without SVL, each VLAN is associated with one FID, which in turn is associated with one MAC address. By using SVL, the specified FID can be used by multiple VLANs, which learn the FID from the MAC address table when SVL is enabled. SVL is configured by specifying which VLANs are mapped to which FIDs. A single VLAN can only be associated with one FID, so although multiple VLANs can use the same FID, one VLAN cannot use more than one FID.

To enable SVL, and specify which VLANs are associated with which FID, follow these steps:

1. Navigate to the **Configuration** tab, and select **VLANs** > **SVL**. In the **Shared VLAN Learning Configuration** menu, select the **Add FID** button to specify a VLAN to FID mapping. Enter VLAN IDs in

the **VLANs** field. Valid VLAN ID range is **1** to **4095**; each VLAN ID must be entered separated by a comma, or ranges can be specified using a hyphen. By default, a new entry uses FID **1**.


Shared VLAN Learning Configuration

Delete	FID	VLANs
Delete	1	1, 10, 11, 12, 13, 200, 300

2. After entering the necessary FID and VLAN ID entries, select **Save** at the bottom of the menu to save these settings.

Once you have specified the VLANs associated with the FIDs, the SVL configuration is complete. You can optionally choose to view VLAN or SVL configurations and statistics using methods described in *Troubleshooting on page 82*.

6. Port Mirroring Configuration Using the GUI

Port mirroring in the ASE device uses three types of mirroring: local mirroring, where the source and destination ports are on the same local switch, source remote mirroring (RMirror), where the port on a local ASE switch is a source for a separate destination, and destination RMirror, where a port on the local ASE switch is a destination for traffic monitored on a separate source. Configuring port mirroring depends on configuring a source port or VLAN, from where the traffic is copied, and a destination port, where the copied traffic is captured. Sources can be configured to capture transmitted traffic only, received traffic only, or both, and can be configured on the local device only (local mirroring) or with a source or destination on a separate device (RMirror).

To configure port mirroring, connect to the ASE GUI and complete the following tasks:

- *Configuring the Mirroring Session Using the GUI on page 27*
- *Configuring the Mirror Source Using the GUI on page 29*
- *Configuring the Mirror Destination Using the GUI on page 30*
- *Mirroring Configuration Examples Using the GUI on page 31*

NOTE

All configurations and instructions included in this section are completed on a device returned to the factory default settings.

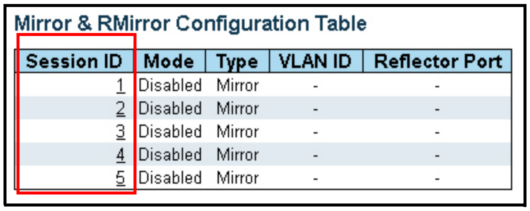
Configuring the Mirroring Session Using the GUI

The first step in configuring port mirroring on the ASE device is to configure the mirroring session. Up to five simultaneous mirroring sessions are supported. Configuring the mirroring session includes providing a session ID, enabling the mirroring feature, specifying the type of mirroring (local, RMirror source, or RMirror destination), and specifying the RMirror VLAN and reflector port.

To configure the mirroring session, follow these steps:

1. Navigate to the **Configuration** tab, and select **Mirroring**. In the **Mirror & RMirror Configuration Table**, select the session ID that you would like to configure from the **Session ID** list. All available mirroring

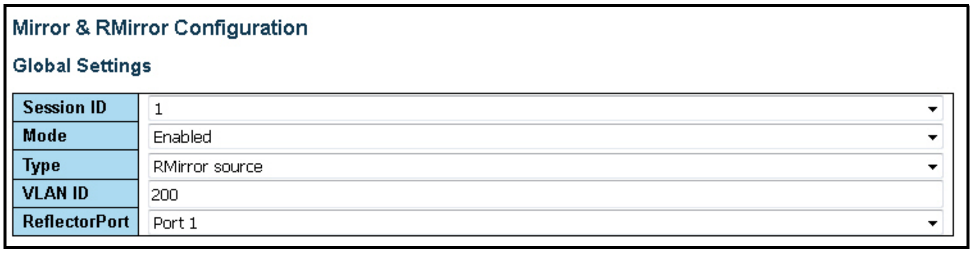
sessions and their configuration are listed in the **Mirror & RMirror Configuration Table**. The session ID number is a hyperlink that opens a configuration menu.



Mirror & RMirror Configuration Table

Session ID	Mode	Type	VLAN ID	Reflector Port
1	Disabled	Mirror	-	-
2	Disabled	Mirror	-	-
3	Disabled	Mirror	-	-
4	Disabled	Mirror	-	-
5	Disabled	Mirror	-	-

2. In the **Mirror & RMirror Configuration** menu that appears once a session ID has been selected, you can begin mirroring session configuration by specifying the global parameters for the mirroring session in the **Global Settings** menu.



Mirror & RMirror Configuration

Global Settings

Session ID	1
Mode	Enabled
Type	RMirror source
VLAN ID	200
ReflectorPort	Port 1

3. The **Session ID** field shows the session you are configuring, and is automatically populated with the ID you selected from the **Mirror & RMirror Configuration Table**.
4. Enable the mirroring feature for this session by selecting **Enabled** from the **Mode** drop-down menu. Selecting **Disabled** disables the mirroring feature for this session.
5. Specify the type of mirroring session you are configuring using the **Type** drop-down menu. Selections include **Mirror**, indicating this is a local mirroring session in which the source and destination are on the same local device, **RMirror source**, indicating this session is the source for a destination on a remote device, and **RMirror destination**, indicating this session is the destination from a source on a remote device. Either **RMirror** selection allows you to then specify the **VLAN ID** and **Reflector Port**. These options are not available for a local **Mirror** session.
6. In the **VLAN ID** field, when configuring **RMirror**, specify the ID of the VLAN used to transmit mirrored traffic. This VLAN ID should be separate from normal data VLANs. Valid ID range is **1** to **4095**; by default, the mirroring VLAN has an ID of **200**.
7. In the **Reflector Port** field, select the port you want to use as the reflector port for **RMirror source** from the drop-down list. The reflector port is an internal interface that redirects mirrored traffic to the VLAN specified for use with RMirror. The selected port will no longer function as a normal port, and will only send mirrored traffic to the VLAN. A reflector port can only be configured for RMirror source sessions; local mirroring and destination RMirror sessions do not support the reflector port.
8. After configuring the global settings for the mirroring session, select **Save** at the bottom of the menu to save these settings.

Once the global settings for the mirroring session are configured, continue mirroring configuration by specifying a source VLAN (optional), and configuring the port(s).

Configuring the Mirror Source Using the GUI

Once the mirroring session global settings have been configured, you must configure the mirroring source, whether port or VLAN, and whether local or remote. Configuring the source includes specifying the port or VLAN to be used as the source, and the type of traffic that will be mirrored.

> **NOTE**
>
> *If you are configuring an **RMirror destination** session, mirror source configuration is not available.*

> **NOTE**
>
> *To capture traffic from the switch itself, the CPU must be mirrored in addition to a source port.*

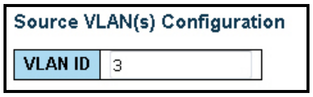
Configuring a Source VLAN Using the GUI

In ASE mirroring, you can choose to specify a source VLAN from which to mirror traffic instead of a source port. Mirrored traffic is still sent to a destination port to be analyzed, but it is traffic over the VLAN rather than the port interface. If a source VLAN is specified, for VLAN-based mirroring, a source port cannot be specified. VLAN and port mirroring are mutually exclusive, and only one can be mirrored at a time.

> **NOTE**
>
> *VLAN-based mirroring is only available for local mirroring sessions.*

To specify a source VLAN for VLAN-based mirroring, in the ASE GUI, navigate to the **Configuration** tab and select **Mirroring**. Select the **Session ID** for the mirroring session you are configuring from the **Mirror & RMirror Configuration Table**.

In the **Source VLAN(s) Configuration** menu, specify the VLAN ID for the VLAN to use a source for mirroring in the **VLAN ID** field. Valid VLAN ID range is **1** to **4095**.


Source VLAN(s) Configuration

VLAN ID: 3

Select **Save** at the bottom of the menu to save these settings.

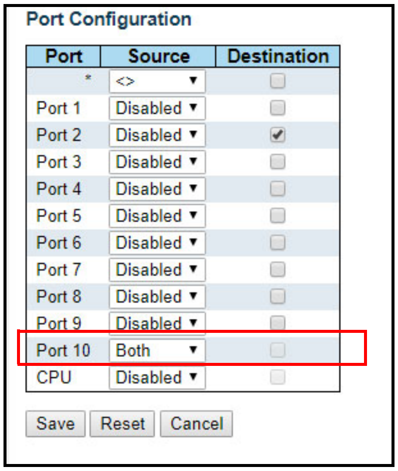
After specifying the source VLAN for VLAN-based mirroring, you can continue configuring the mirroring feature by specifying the mirroring destination, as described in *Configuring the Mirror Destination Using the GUI on page 30*.

Configuring a Source Port Using the GUI

The source port specifies the port from which traffic is copied in the mirroring feature. To configure a mirroring source port, follow these steps:

1. Navigate to the **Configuration** tab and select **Mirroring**. Select the **Session ID** for the mirroring session you are configuring from the **Mirror & RMirror Configuration Table**, as shown in *Figure 1* on page 28.
2. In the **Port Configuration** menu, select the setting for the source port from the **Source** drop-down menu next to the appropriate port. Source port settings include **Disabled**, indicating the port is not a source port;

Both, indicating both received and transmitted traffic is mirrored; **Rx only**, indicating only received traffic is mirrored; and **Tx only**, indicating only transmitted traffic is mirrored. By default, all possible source ports are disabled. In the example below, **Port 10** is configured as the mirroring source port for both transmitted and received traffic.



Port Configuration

Port	Source	Destination
*	<> ▾	□
Port 1	Disabled ▾	□
Port 2	Disabled ▾	☑
Port 3	Disabled ▾	□
Port 4	Disabled ▾	□
Port 5	Disabled ▾	□
Port 6	Disabled ▾	□
Port 7	Disabled ▾	□
Port 8	Disabled ▾	□
Port 9	Disabled ▾	□
Port 10	Both ▾	□
CPU	Disabled ▾	□

> **NOTE**
>
> *For local mirroring, multiple source ports can be specified.*

> **NOTE**
>
> *Modifying the **Description** field in the **Port Configuration** menu will also update the CLI.*

3. Once the source port(s) have been configured, select **Save** at the bottom of the menu to save these settings.

After configuring the mirror source(s), you can proceed to configuring the mirror destination.

Configuring the Mirror Destination Using the GUI

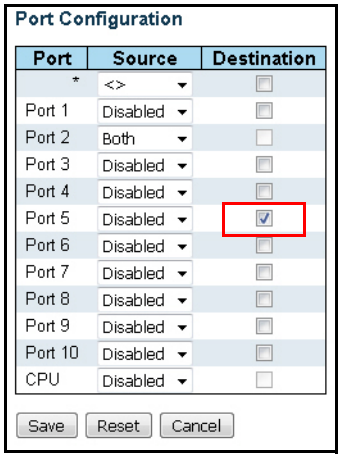
Once the mirroring session global and source settings have been configured, you can configure the mirroring destination. Configuring the destination includes specifying the port to be used as the mirroring destination.

> **NOTE**
>
> *If you are configuring an **RMirror source** session, mirror destination configuration is not available.*

The destination port specifies the port to which traffic is copied in the mirroring feature. To configure a mirroring destination port, follow these steps:

1. Navigate to the **Configuration** tab and select **Mirroring**. Select the **Session ID** for the mirroring session you are configuring from the **Mirror & RMirror Configuration Table**, as shown in *Figure 1* on page 28.

2. In the **Port Configuration** menu, select the check box next to the port you want to use as the destination port. By default, all available destination ports are disabled. In the example below, **Port 5** is configured to be the destination port.



Port Configuration

Port	Source	Destination
*	<>	□
Port 1	Disabled	□
Port 2	Both	□
Port 3	Disabled	□
Port 4	Disabled	□
Port 5	Disabled	☑
Port 6	Disabled	□
Port 7	Disabled	□
Port 8	Disabled	□
Port 9	Disabled	□
Port 10	Disabled	□
CPU	Disabled	□

NOTE

For local mirroring, only a single destination can be specified.

3. Once the destination port has been configured, select **Save** at the bottom of the menu to save these settings.

After configuring the mirror destination, the configuring of the mirroring feature is complete. To view sample configurations of the mirroring feature, refer to *Mirroring Configuration Examples Using the GUI on page 31*. To view statistics related to the mirroring configuration, refer to *Troubleshooting on page 82*.

Mirroring Configuration Examples Using the GUI

The example scenarios contained in this section are designed to enhance understanding of mirroring configurations on ASE devices. All configurations provided in this section use the GUI.

NOTE

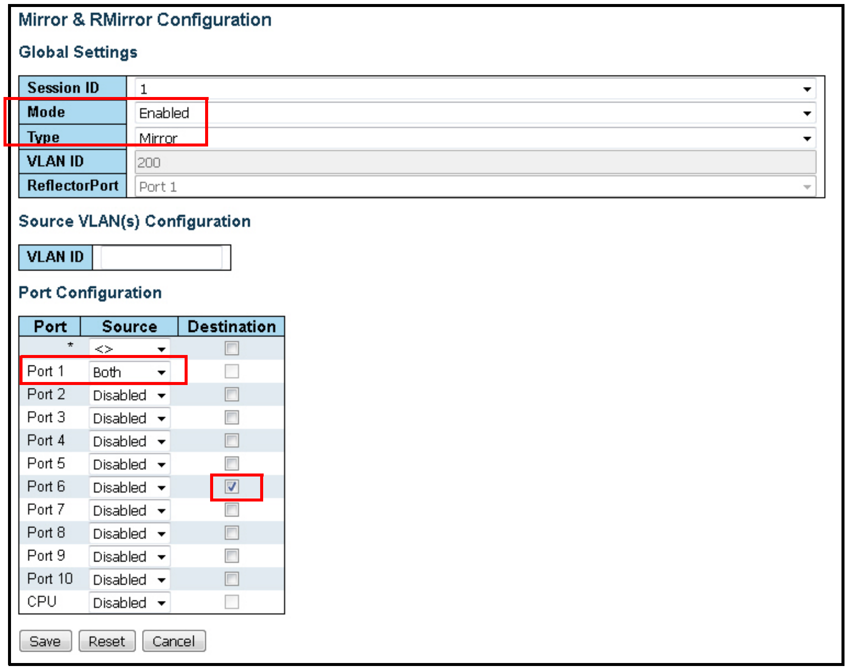
The configuration parameters entered in these examples are sample configurations only. These applications should be configured in a manner consistent with the needs of your particular network. These configurations should not be copied without first making the necessary adjustments to ensure they will function properly in your network.

Local Mirroring Configuration Example (GUI)

The following example configures local mirroring for the traffic on **Port 1**. The mirrored traffic is displayed on **Port 6**.

1. Navigate to the **Configuration** tab, select **Mirroring**, and select Session ID **1** from the **Mirror & RMirror Configuration Table** menu.
2. In the **Mirror & RMirror Configuration** menu, configure the following as shown in the example below:
   - **Mode**: Select **Enabled** from the drop-down menu

- **Type**: Select **Mirror** from the drop-down menu
- **Source**: For **Port 1**, select **Both** from the drop-down menu
- **Destination**: Select the check box for **Port 6**



Mirror & RMirror Configuration

Global Settings

Session ID	1
Mode	Enabled
Type	Mirror
VLAN ID	200
ReflectorPort	Port 1

Source VLAN(s) Configuration

VLAN ID	

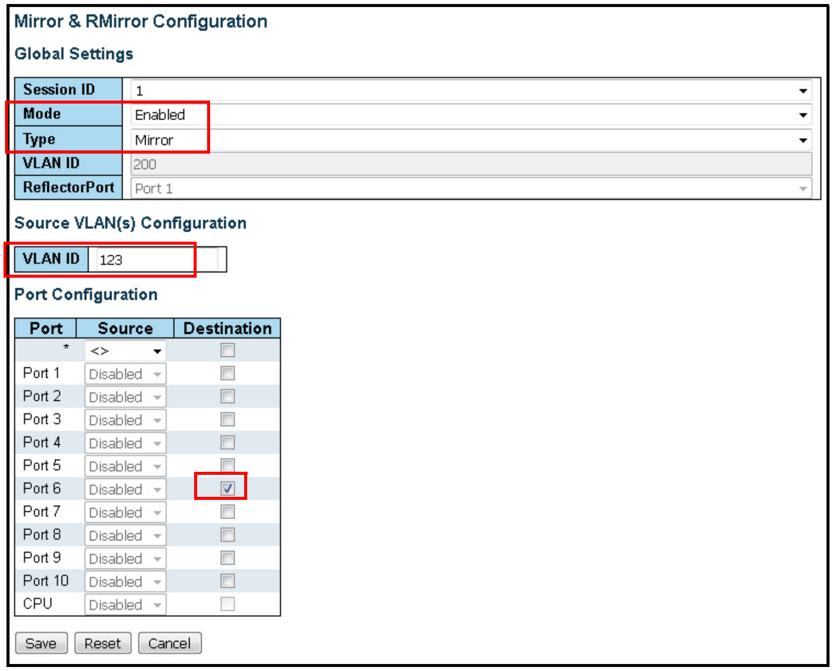
Port Configuration

Port	Source	Destination
*	<>	□
Port 1	Both	□
Port 2	Disabled	□
Port 3	Disabled	□
Port 4	Disabled	□
Port 5	Disabled	□
Port 6	Disabled	☑
Port 7	Disabled	□
Port 8	Disabled	□
Port 9	Disabled	□
Port 10	Disabled	□
CPU	Disabled	□

VLAN-Based Mirroring Example (GUI)

The following example configures VLAN-based mirroring for the traffic on **VLAN 123**. The mirrored traffic is displayed on **Port 6**.

1. Navigate to the **Configuration** tab, select **Mirroring**, and select Session ID **1** from the **Mirror & RMirror Configuration Table** menu.
2. In the **Mirror & RMirror Configuration** menu, configure the following as shown in the following example:
   - **Mode**: Select **Enabled** from the drop-down menu
   - **Type**: Select **Mirror** from the drop-down menu
   - **Source VLAN(s) Configuration**: Enter **123** in the VLAN ID field
   - **Destination**: Select check box for **Port 6**



Mirror & RMirror Configuration

Global Settings

Session ID	1
Mode	Enabled
Type	Mirror
VLAN ID	200
ReflectorPort	Port 1

Source VLAN(s) Configuration

VLAN ID	123

Port Configuration

Port	Source	Destination
*	<>	□
Port 1	Disabled	□
Port 2	Disabled	□
Port 3	Disabled	□
Port 4	Disabled	□
Port 5	Disabled	□
Port 6	Disabled	☑
Port 7	Disabled	□
Port 8	Disabled	□
Port 9	Disabled	□
Port 10	Disabled	□
CPU	Disabled	□

RMirror Configuration Example (GUI)

In the following example, remote mirroring is used to mirror a user port (**port 1**) from a PC connected to **ASE Switch 1**. The mirrored traffic is sent to the network administrator with a network analyzer connected to a port (**port 1**) on **ASE Switch 3**. The mirrored traffic is sent by the reflector port (**port 2**) to a VLAN configured for mirroring use (**VLAN 200**), which then sends the mirrored traffic through **ASE Switch 2** from using the mirror VLAN members, **port 3** and **port 4**. The network topology for this example is displayed in the following image.

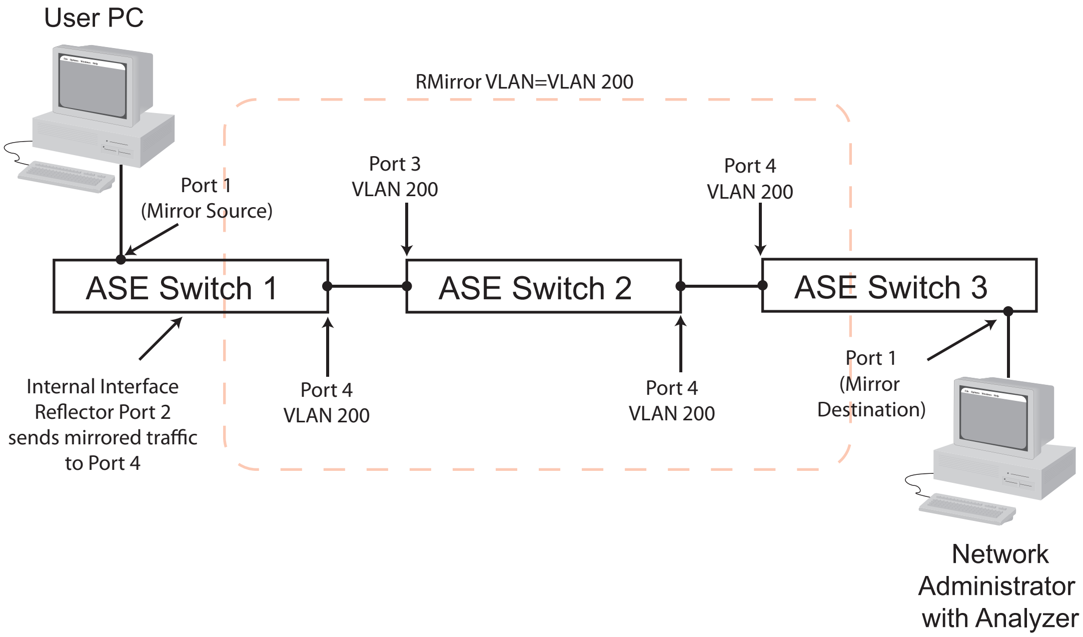


Figure 2. RMirror Network Topology

RMirror Example Configuration Considerations

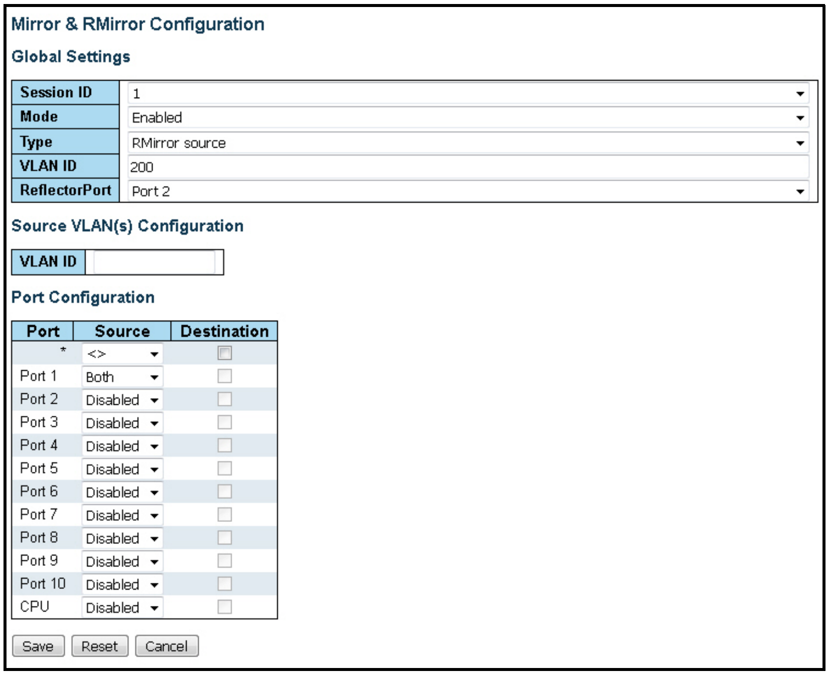
The following are configuration parameters to consider when studying this example:

- The reflective port (**port 2** on **ASE Switch 1**) must have STP disabled
- MAC address learning should be disabled for all ports using the RMirror VLAN
- In a remote mirroring configuration like this, the source and destination devices must be ASE devices. The intermediate device can be an ASE device or a non-ASE device. This example assumes the intermediate device is an ASE device.

Step 1: Configuring the Source Device

The source device for this example (**ASE Switch 1**) should be configured with the **RMirror source** session. The device should be configured with the following parameters (as shown in Figure 4, Figure 5 and Figure 6):

- Mirror type: RMirror Source
- VLAN 200: for mirrored traffic
- Reflector Port: Port 2, disable STP on this port
- Disable source MAC address learning for RMirror VLAN 200
- Configure RMirror VLAN membership: Port 4
- Source mirror port: Port 1
- Both transmitted and received frames are mirrored on source port



Mirror & RMirror Configuration

Global Settings

Session ID	1
Mode	Enabled
Type	RMirror source
VLAN ID	200
ReflectorPort	Port 2

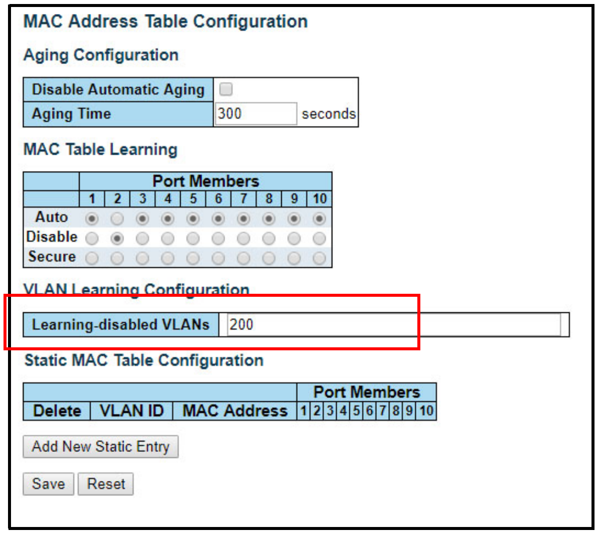
Source VLAN(s) Configuration

VLAN ID	

Port Configuration

Port	Source	Destination
*	<>	□
Port 1	Both	□
Port 2	Disabled	□
Port 3	Disabled	□
Port 4	Disabled	□
Port 5	Disabled	□
Port 6	Disabled	□
Port 7	Disabled	□
Port 8	Disabled	□
Port 9	Disabled	□
Port 10	Disabled	□
CPU	Disabled	□

Figure 3. Source Device Configuration Example



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

MAC Table Learning

	Port Members									
	1	2	3	4	5	6	7	8	9	10
Auto	●	○	●	●	●	●	●	●	●	●
Disable	○	●	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○

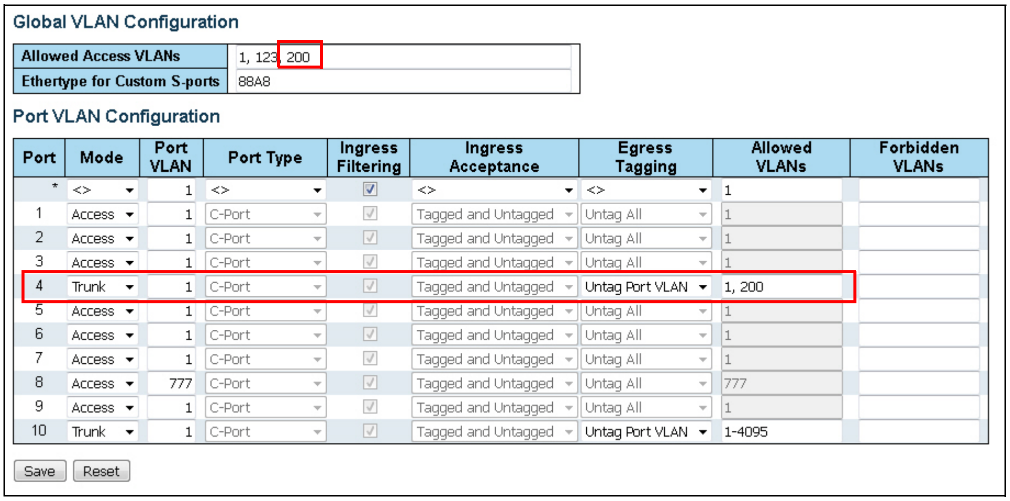
VLAN Learning Configuration

Learning-disabled VLANs	200

Static MAC Table Configuration

			Port Members									
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10

Figure 4. Disable Source MAC Address Learning for RMirror VLAN 200



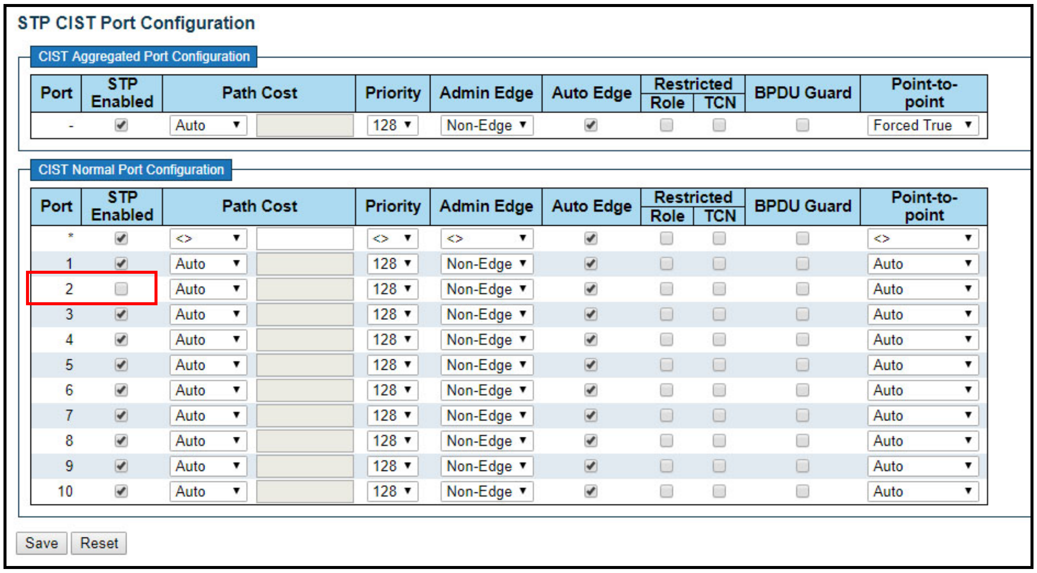
Global VLAN Configuration

Allowed Access VLANs	1, 123, 200
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1, 200	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	777	C-Port	☑	Tagged and Untagged	Untag All	777	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	

Figure 5. Add Port Mirroring VLAN to Allowed VLAN List



STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
-	☑	Auto ▼		128 ▼	Non-Edge ▼	☑	□	□	□	Forced True ▼

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
*	☑	<> ▼		<> ▼	<> ▼	☑	□	□	□	<> ▼
1	☑	Auto ▼		128 ▼	Non-Edge ▼	☑	□	□	□	Auto ▼
2	□	Auto ▼		128 ▼	Non-Edge ▼	☑	□	□	□	Auto ▼
3	☑	Auto ▼		128 ▼	Non-Edge ▼	☑	□	□	□	Auto ▼
4	☑	Auto ▼		128 ▼	Non-Edge ▼	☑	□	□	□	Auto ▼
5	☑	Auto ▼		128 ▼	Non-Edge ▼	☑	□	□	□	Auto ▼
6	☑	Auto ▼		128 ▼	Non-Edge ▼	☑	□	□	□	Auto ▼
7	☑	Auto ▼		128 ▼	Non-Edge ▼	☑	□	□	□	Auto ▼
8	☑	Auto ▼		128 ▼	Non-Edge ▼	☑	□	□	□	Auto ▼
9	☑	Auto ▼		128 ▼	Non-Edge ▼	☑	□	□	□	Auto ▼
10	☑	Auto ▼		128 ▼	Non-Edge ▼	☑	□	□	□	Auto ▼

Figure 6. Disable STP on the Reflector Port

Step Two: Configure the Intermediate Switch/Device

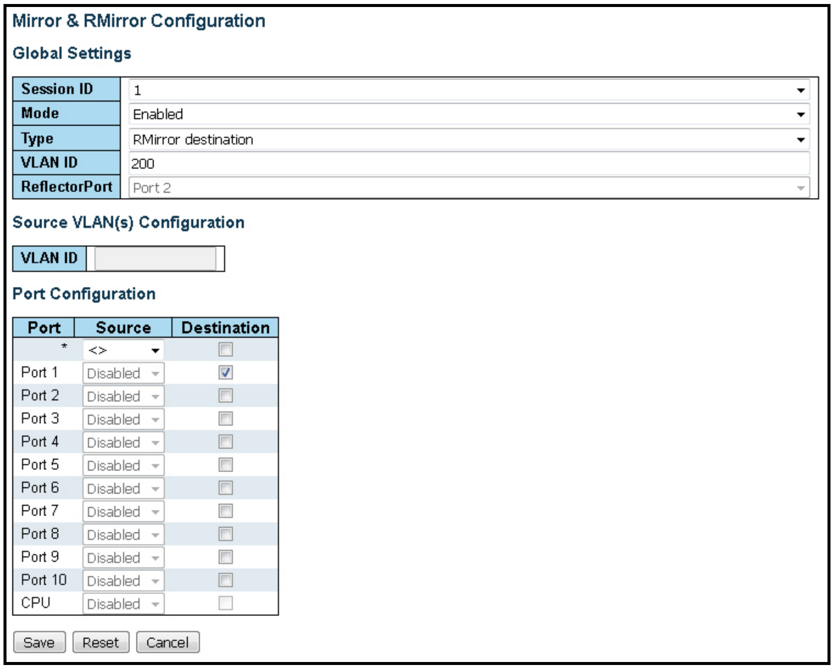
Configure the intermediate device for this example with the following parameters:

- VLAN for mirrored traffic: 200
- Disable source MAC address learning for RMirror VLAN 200

Step Three: Configure the Destination Device

The destination device for this example (**ASE Switch 3**) should be configured with the **RMirror destination** session. The device should be configured with the following parameters (as shown in Figure 7, Figure 8, and Figure 9):

- Mirror type: RMirror Destination
- VLAN 200: for mirrored traffic
- Disable source MAC address learning for RMirror VLAN 200
- Configure RMirror VLAN membership: Port 4
- Destination mirror port: Port 1



Mirror & RMirror Configuration

Global Settings

Session ID	1
Mode	Enabled
Type	RMirror destination
VLAN ID	200
ReflectorPort	Port 2

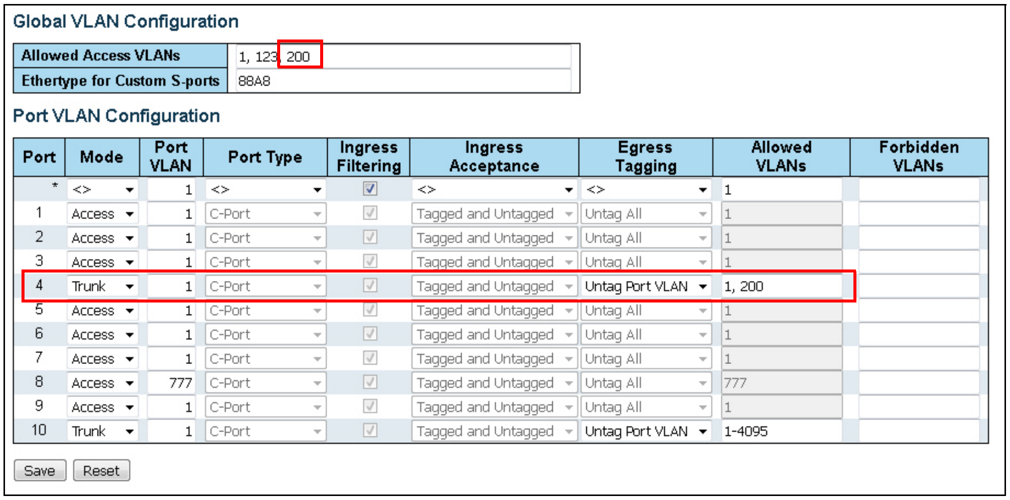
Source VLAN(s) Configuration

VLAN ID	

Port Configuration

Port	Source	Destination
*	<>	□
Port 1	Disabled	☑
Port 2	Disabled	□
Port 3	Disabled	□
Port 4	Disabled	□
Port 5	Disabled	□
Port 6	Disabled	□
Port 7	Disabled	□
Port 8	Disabled	□
Port 9	Disabled	□
Port 10	Disabled	□
CPU	Disabled	□

Figure 7. Destination Device Configuration Example



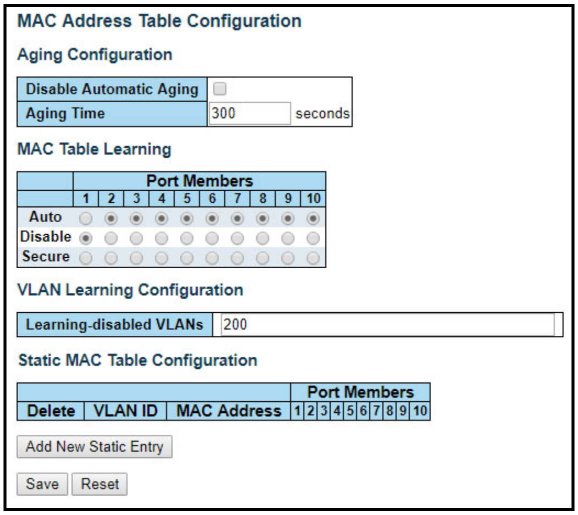
Global VLAN Configuration

Allowed Access VLANs	1, 123, 200
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1, 200	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	777	C-Port	☑	Tagged and Untagged	Untag All	777	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	

Figure 8. Add Port Mirroring VLAN to Allowed VLAN List



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

MAC Table Learning

	Port Members									
	1	2	3	4	5	6	7	8	9	10
Auto	○	●	●	●	●	●	●	●	●	●
Disable	●	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○

VLAN Learning Configuration

Learning-disabled VLANs	200

Static MAC Table Configuration

			Port Members									
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10

Figure 9. Disable Source MAC Address Learning for RMirror VLAN 200

7. GVRP Configuration Using the GUI

GVRP configuration on the ASE device includes enabling GVRP globally on the switch, enabling GVRP on a per-port basis, and optionally configuring the timers used by GVRP. To configure GVRP, connect to the ASE GUI and complete these tasks:

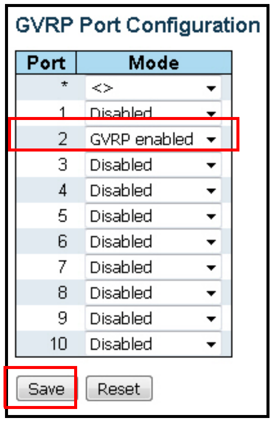
- *Enabling GVRP on a Port Using the GUI on page 38*
- *Configuring GVRP Timers and Resources Using the GUI (Optional) on page 39*
- *Enabling GVRP Globally Using the GUI on page 40*

NOTE

All configurations and instructions included in this section are completed on a device returned to the factory default settings.

Enabling GVRP on a Port Using the GUI

To enable GVRP on a port, connect to the ASE GUI and navigate to the **Configuration** tab, and select **GVRP** > **Port Config**. In the **GVRP Port Configuration** menu, select **GVRP Enabled** from the **Mode** drop-down menu associated with the port on which you want to enable GVRP. By default, GVRP is disabled on all ports. Once you have enabled GVRP on all required ports, select **Save** at the bottom of the menu to save these settings. Continue GVRP configuration by enabling GVRP globally on the ASE switch.



GVRP Port Configuration

Port	Mode
*	<>
1	Disabled
2	GVRP enabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled

NOTE

GVRP will not function without being enabled on both an interface and globally on the switch.

Configuring GVRP Timers and Resources Using the GUI (Optional)

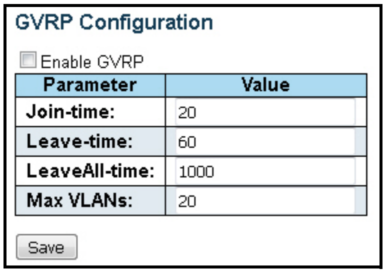
You can optionally choose to continue GVRP configuration by globally defining the GVRP timers and resources, but this additional configuration is not required. Additional GVRP configuration consists of defining the three GVRP timers (Join-time, Leave-time, and LeaveAll-time) and adjusting the maximum number of VLANs that can be simultaneously controlled by GVRP.

CAUTION!

Caution should be exercised when adjusting GVRP timers. All GVRP timers across any GVRP-enabled devices on the network must be set to the same value. In addition, any adjustments to the maximum number of VLANs simultaneously controlled by GVRP should be made before enabling GVRP on the switch.

To configure the GVRP timers and maximum VLANs supported by GVRP, follow these steps:

1. Navigate to the **Configuration** tab, and select **GVRP** > **Global Config**. In the **GVRP Configuration** menu, you can enter the new timer values and GVRP-supported VLANs.



GVRP Configuration

☐ Enable GVRP

Parameter	Value
Join-time:	20
Leave-time:	60
LeaveAll-time:	1000
Max VLANs:	20

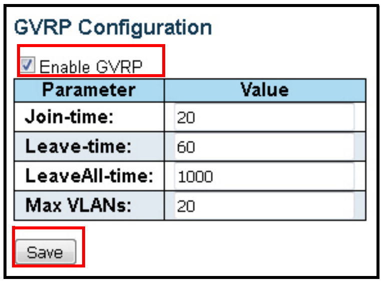
2. Specify the GVRP join-timer by entering an appropriate value in the **Join-time** field. This timer specifies the interval between declarations of new attributes in GVRP PDUs. Valid range is **1** to **20** centiseconds. By default, this value is set to **20** centiseconds.

3. Specify the GVRP leave-timer by entering an appropriate value in the **Leave-time** field. This timer specifies how long after a leave message is received before a VLAN attribute is deregistered. Valid range is **60** to **300** centiseconds. By default, this value is set to **60** centiseconds.
4. Specify the GVRP leave-all-timer by entering an appropriate value in the **LeaveAll-time** field. This timer specifies how long after a VLAN attribute has been GVRP-enabled before it sends a LeaveAll message. Once the LeaveAll message is sent, the LeaveAll timer starts again. Valid range is **1000** to **5000** centiseconds. By default, this value is set to **1000** centiseconds.
5. Specify the maximum number of VLANs that can be simultaneously controlled by GVRP by entering an appropriate value in the **Max VLANs** field. Valid range is **1** to **4094** VLANs. By default, this value is set to **20** VLANs.
6. Select **Save** at the bottom of the menu to save these settings.

Once GVRP has been enabled on the necessary port(s), and the optional settings have been configured, complete GVRP configuration by enabling GVRP globally on the switch.

Enabling GVRP Globally Using the GUI

To enable GVRP globally on the switch, connect to the ASE GUI and navigate to the **Configuration** tab, and select **GVRP** > **Global Config**. In the **GVRP Configuration** menu, select the **Enable GVRP** check box to enable GVRP. By default, GVRP is disabled on the switch. Once you have enabled GVRP, select **Save** at the bottom of the menu to save these settings.



GVRP Configuration

☑ Enable GVRP

Parameter	Value
Join-time:	20
Leave-time:	60
LeaveAll-time:	1000
Max VLANs:	20

Once GVRP has been enabled on the necessary port(s) and globally on the ASE device, GVRP configuration is complete.

8. Spanning Tree Configuration Using the GUI

Spanning tree is configured on the ASE switch by selecting which protocol type you need to configure (STP, RSTP, or MSTP), and configuring the associated priorities, timers, and ports required for the particular protocol, and then configuring spanning tree settings on a per-port basis. In addition, MSTP configurations include configuring the CIST, MSTP regions, and MSTIs.

To configure spanning tree, connect to the ASE GUI, and complete the following tasks:

- *Configuring Common Spanning Tree Settings Using the GUI on page 41*
- *Configuring Additional MSTP Settings Using the GUI on page 43*
- *Configuring Spanning Tree Ports Using the GUI on page 45*

NOTE

All configurations and instructions included in this section are completed on a device returned to the factory default settings.

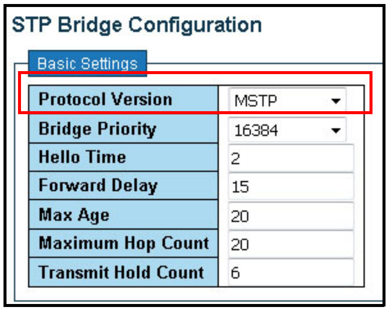
Configuring Common Spanning Tree Settings Using the GUI

STP, RSTP, and MSTP configuration in the ASE device includes configuring some global settings that are common to all versions of spanning tree, including enabling the protocol, specifying bridge priorities, configuring timers and counters, and specifying edge port settings.To configure these common settings, complete the following tasks:

- *Selecting the Spanning Tree Protocol Using the GUI on page 41*
- *Configuring the Bridge Priority Using the GUI on page 41*
- *Configuring Spanning Tree Timers and Counters Using the GUI (Optional) on page 42*
- *Configuring Global Edge Port Settings Using the GUI (Optional) on page 42*

Selecting the Spanning Tree Protocol Using the GUI

To enable any version of spanning tree on the switch, navigate to the **Configuration** tab, and select **Spanning Tree** > **Bridge Settings**. In the **STP Bridge Configuration** menu, select either **STP**, **RSTP**, or **MSTP** from the **Protocol version** field of the **Basic Settings** menu.



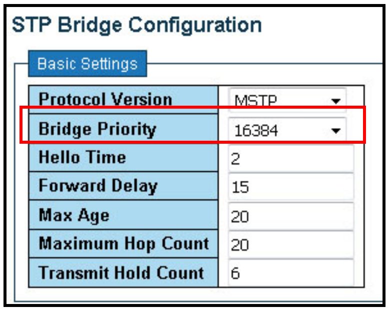
STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Bridge Priority	16384
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Configuring the Bridge Priority Using the GUI

To configure the bridge priority for the spanning tree instance, select the appropriate priority from the **Bridge Priority** drop-down menu in the **Basic Settings** menu of the **STP Bridge Configuration** menu (**Configuration** tab, **Spanning Tree** > **Bridge Settings**).



STP Bridge Configuration

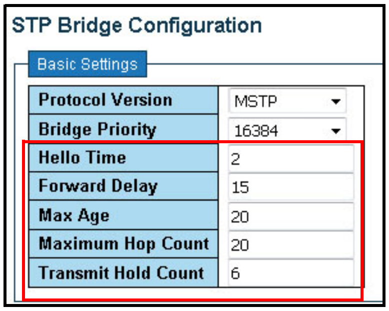
Basic Settings

Protocol Version	MSTP
Bridge Priority	16384
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

The **Bridge Priority** setting for spanning tree configurations specifies the priority of the bridge associated with the spanning tree instance on the ASE switch. This priority is used by the protocol to determine which switch is the root bridge, and the priorities of the other switches connected to the instance. Valid **Bridge Priority** range is **0** to **61440**, in multiples of **4096**. By default, the **Bridge Priority** is set to **16384**.

Configuring Spanning Tree Timers and Counters Using the GUI (Optional)

Spanning tree protocols use several timers and counters to determine when to send BPDU messages, when to change port state, and how long to retain network topology information. These timers include hello, forward delay, and maximum age timers, and counters include the maximum hop count and transmit hold count. To change the default timer and count values, navigate to the **Configuration** tab, and select **Spanning Tree** > **Bridge Settings**. In the **STP Bridge Configuration** menu, enter the new values in the **Hello Time**, **Forward Delay**, **Max Age**, **Maximum Hop Count**, and **Transmit Hold Count** fields of the **Basic Settings** menu.



STP Bridge Configuration

Basic Settings

Protocol Version	MSTP ▾
Bridge Priority	16384 ▾
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

The **Hello Time** specifies the interval between BPDU messages sent by the bridge. By default, messages are sent every **2** seconds. Valid range is **1** to **10** seconds.

The **Forward Delay** timer specifies the time that ports spend in the Listening and Learning states, before moving to the Forwarding state. By default, ports spend **15** seconds in the Listening and Learning states. Valid range is **4** to **30** seconds.

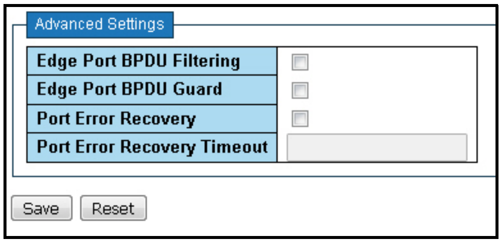
The **Max Age** timer specifies how long the ports save the configuration information delivered to them in BPDU messages. By default, ports hold on to this information for **20** seconds. Valid range is **6** to **40** seconds. The **Max Age** timer must be configured to be less than or equal to two times the forward delay. So, if the **Forward Delay** is configured to be **20** seconds, the **Max Age** timer must be set to less than or equal to **40** seconds.

The **Maximum Hop Count** specifies the number of hops a BPDU message can travel before being discarded and before the port information included in the message is no longer valid. By default, the **Maximum Hop Count** is set to **20** hops. Valid range is **6** to **40** hops.

The **Transmit Hold Count** specifies the maximum number of transmitted BPDU messages per second. By default, a maximum of **6** BPDU messages can be sent per second. Valid range is **1** to **10**.

Configuring Global Edge Port Settings Using the GUI (Optional)

Edge ports refer to ports at the edge of the network, that are not connected to other bridges within the spanning tree instance. You can specify how all edge ports within the spanning tree instance behave with regards BPDU transmissions and error recovery. To configure the edge port settings for all edge ports in the spanning tree instance, navigate to the **Configuration** tab, and select **Spanning Tree** > **Bridge Settings**. In the **STP Bridge Configuration** menu, navigate to the **Advanced Settings** menu.



Advanced Settings

Edge Port BPDU Filtering	□
Edge Port BPDU Guard	□
Port Error Recovery	□
Port Error Recovery Timeout	

To enable BPDU filtering on all edge ports within the spanning tree instance, select the **Edge Port BPDU Filtering** check box. This setting, when enabled, prevents the port from transmitting or receiving BPDU messages. This feature is disabled by default.

To enable BPDU guarding on all edge ports within the spanning tree instance, select the **Edge Port BPDU Guard** check box. This setting, when enabled, prevents the port from receiving BPDU messages. This feature is disabled by default.

To enable the ports to automatically recover from errors, select the **Port Error Recovery** check box. The port will automatically recover from being disabled by an error after an allotted timeout period, specified in the **Port Error Recovery Timeout** field. Valid timeout range is **30** to **86400** seconds. The error recovery feature is disabled by default.

Once all the spanning tree bridge settings have been configured, select **Save** at the bottom of the menu. Continue with spanning tree configuration by specifying the port and MSTI settings as outlined in *Configuring Additional MSTP Settings Using the GUI on page 43*.

Configuring Additional MSTP Settings Using the GUI

Additional MSTP configuration includes specifying MSTP region names and IDs, configuring MSTI VLAN mapping associations, and defining MSTP bridge priorities. To configure the settings specific to MSTP operation on the ASE device, complete these tasks:

- *Configuring MSTP Regions and MSTI Mapping Using the GUI on page 43*
- *Specifying MSTP Bridge Priorities Using the GUI on page 45*

Configuring MSTP Regions and MSTI Mapping Using the GUI

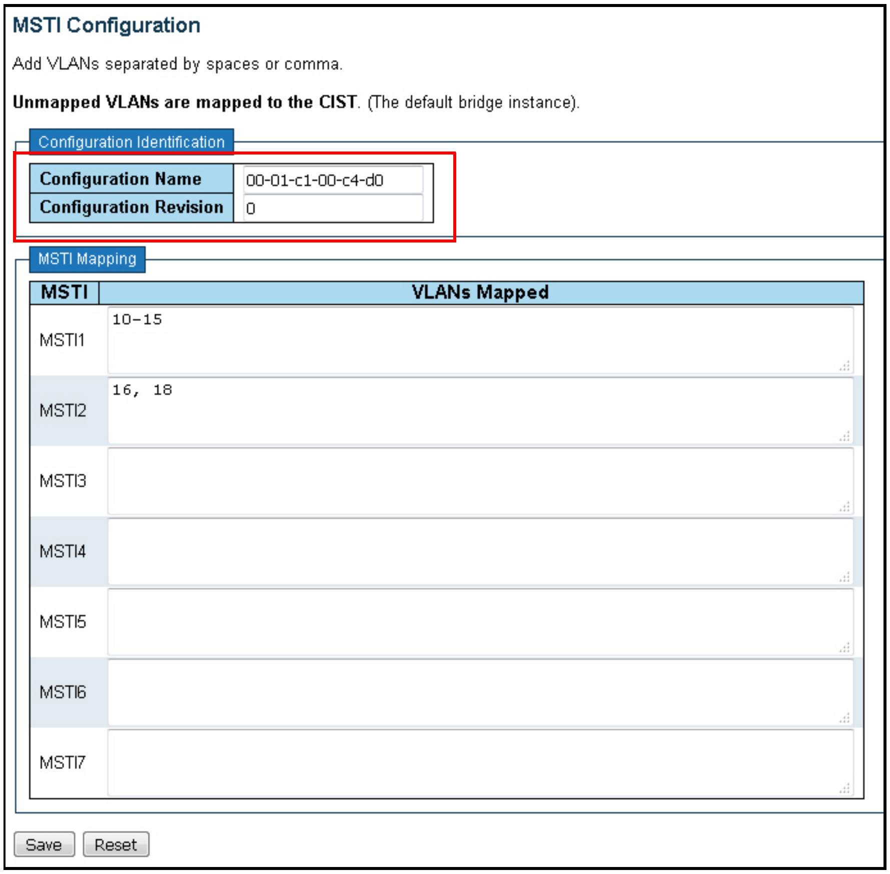
MSTP operates using MSTP regions to organize multiple spanning tree instances within the network. These regions are composed of sets of configured VLANs and their associated MSTIs, are individually named, use the same revision number, and contain a mapping table of which VLANs are associated with which MSTIs. By default, each created VLAN within the MSTP spanning tree configuration is mapped to the CIST. However, you can choose to map particular VLANs to one of seven MSTIs within the single MSTP region. Each MSTP region is configured with a name and revision, and then VLANs are associated with the particular MSTI instance within the region.

NOTE

For MSTP to function correctly, all MSTI mapping settings must be identical on all switches in the network. AOS switches do not support MSTI, as they only support RSTP. See note on page 69.

To configure the MSTP region and VLAN mapping to an MSTI instance, connect to the ASE GUI and follow these steps:

1. Navigate to the **Configuration** tab, and select **Spanning Tree** > **MSTI Mapping**.



MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	00-01-c1-00-c4-d0
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	10-15
MSTI2	16, 18
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

2. Specify the configuration name for the MSTP region in the **Configuration Identification** menu by entering the region's configuration name in **Configuration Name** field. These names are carried in BPDU messages throughout the network and must be identical on all switches within the MSTP region. Configuration names are specified as ASCII strings with a maximum length of 32 characters, and are case-sensitive. By default, the configuration name for the MSTP region is a text string in hexadecimal format based on the switch's MAC address.

3. Specify the configuration revision number for the MSTP region in the **Configuration Identification** menu by entering the region's revision number in **Configuration Revision** field. Like configuration names, revision numbers must be identical on all switches within the MSTP region. Valid range for revision numbers is **1** to **65535**; it is set to **0** by default.

4. Associate VLANs with each MSTI by entering the VLAN ID in the appropriate MSTI field in the **MSTI Mapping** menu. Seven MSTIs are available for each MSTP region, and are named **MSTI1**, **MSTI2**, **MSTI3** and so on through **MSTI7**. VLANs can be entered as a single ID, a list of IDs separated by a comma, or a range of VLAN IDs using a hyphen. For example, in the screenshot above, VLANs **10** through **15** are associated with **MSTI1**, and VLANs **16** and **18** are associated with **MSTI2**. Valid VLAN ID range is s **1** to **4095**. Remember that any VLANs not mapped to a specific MSTI are mapped by default to the CIST.

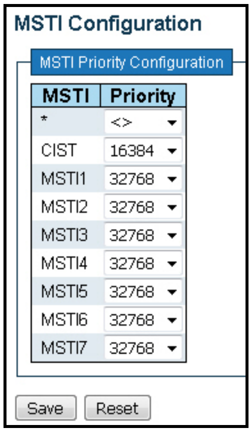
5. After specifying the MSTP region configuration identification information and mapping any VLANs to the appropriate MSTI, select **Save** at the bottom of the menu to save these settings.

Continue MSTP configuration by specifying the MSTP bridge priorities for each MSTI, including the CIST, as described in the following section.

Specifying MSTP Bridge Priorities Using the GUI

You can specify the priority of each MSTI, including the CIST, for the MSTP region to be used as part of the bridge identifier and to aid spanning tree in determining the root bridge (root bridges have the lowest bridge ID). Each bridge ID is comprised of the bridge priority number concatenated with the MAC address of the device. For example, if a bridge has a priority of **4096**, and the switch's MAC address is **00:A0:C8:00:00:01**, then the bridge ID is **4096.00.A0.C8.00.00.01**. Because a low priority number indicates a higher priority, the lower the bridge ID, the more likely the bridge is selected as the root of the spanning tree.

To configure the priority of the CIST and each MST, navigate to the **Configuration** tab, and select **Spanning Tree** > **MSTI Priorities**.



MSTI Configuration

MSTI Priority Configuration

MSTI	Priority
*	<>
CIST	16384
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

Select the desired priority for the CIST and each MSTI from the appropriate drop-down menu. Priorities for MSTIs are set to **32768** by default, and can only be configured in multiples of **4096**. The priority for the CIST is set to **16384** default, and also can only be configured in multiples of **4096**. By default, the CIST is configured with the lower number and therefore has the lower bridge ID, higher priority, and is the default root bridge for the spanning tree instance.

Once the priorities for the CIST and associated MSTIs have been specified, select **Save** at the bottom of the menu to save these settings, and continue spanning tree configuration by configuring the spanning tree port settings as described in the next sections.

Configuring Spanning Tree Ports Using the GUI

Spanning tree port settings configuration includes ensuring spanning tree is enabled, specifying port path cost and priority, and configuring port behavior with regards to BPDU transmission and port connection types. All ports using spanning tree, whether STP, RSTP, or MSTP, can be configured from a single GUI menu. These settings are specified in a CIST port GUI menu, but define port settings for all versions of spanning tree. If MSTP is being used, MSTI path cost and priority settings can also be configured on a per-port basis.

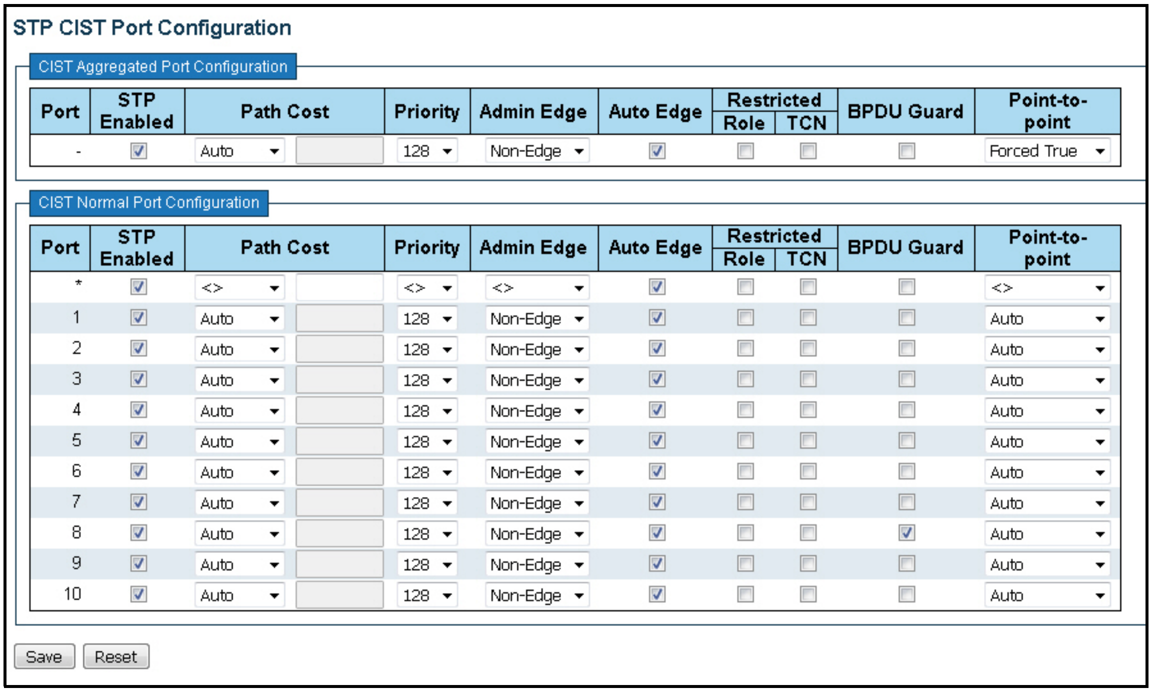
To configure the port settings for specific spanning tree operation on the ASE device, complete these tasks:

- *Configuring Spanning Tree Port Settings Using the GUI on page 45*
- *Configuring MSTP MSTI Port Path Cost and Priority Using the GUI on page 48*

Configuring Spanning Tree Port Settings Using the GUI

Spanning tree settings, on a per-port basis, are configured either by configuring all ports as a group (aggregated), or by configuring each port individually. Port configuration includes ensuring spanning tree is enabled, specifying the port's path cost and priority, defining the edge port properties of the port (if applicable), configuring the BDPU processing behavior for the port(s), and specifying the link type between ports. To configure the spanning tree settings for all ports, including those associated with the MSTP CIST, connect to the ASE GUI and complete these steps:

1. Navigate to the **Configuration** tab, and select **Spanning Tree** > **CIST Ports**. The **STP CIST Port Configuration** menu appears.



STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
-	☑	Auto		128	Non-Edge	☑	□	□	□	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
*	☑	<>		<>	<>	☑	□	□	□	<>
1	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
2	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
3	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
4	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
5	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
6	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
7	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
8	☑	Auto		128	Non-Edge	☑	□	□	☑	Auto
9	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
10	☑	Auto		128	Non-Edge	☑	□	□	□	Auto

NOTE

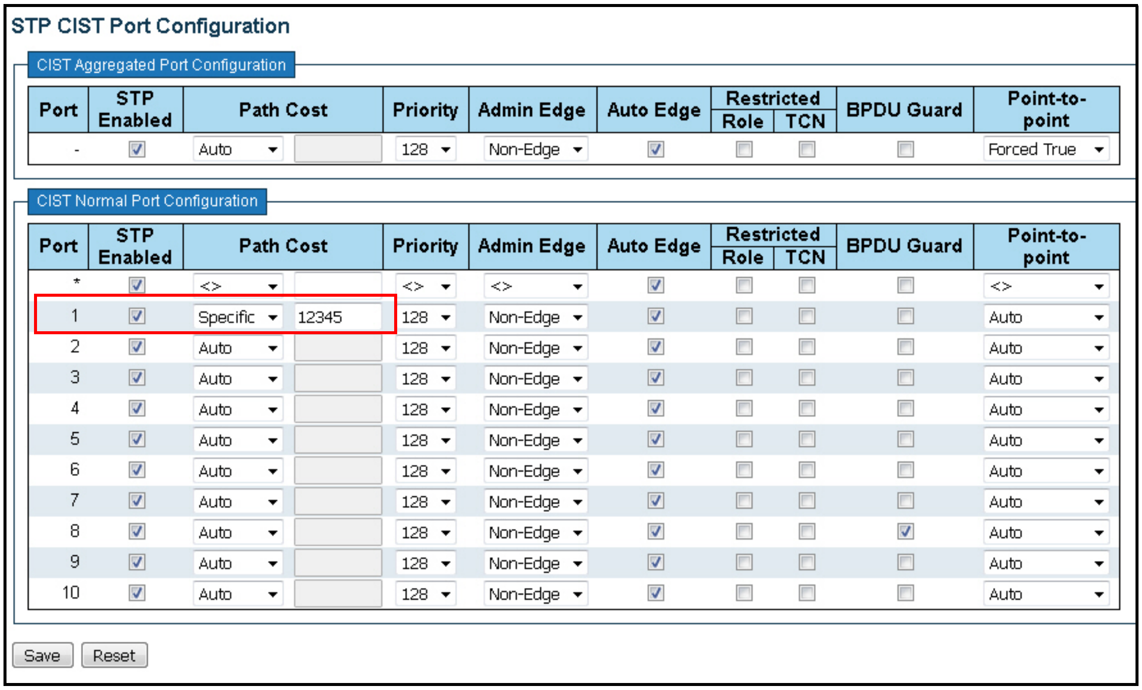
Although this menu is used to configure ports specifically associated with the default MSTI for MSTP configuration (the CIST), this menu is also used to configure specific spanning tree settings on a per-port basis for STP and RSTP configurations.

2. Using your network topology and needs, determine if you will be configuring all ports associated with the CIST as an aggregated group, or each port individually. If you are configuring the ports as an aggregated group, use the **CIST Aggregated Port Configuration** menu to configure the ports. If you are configuring each port individually, use the **CIST Normal Port Configuration** menu and make configuration selections for the appropriate port(s).

3. Ensure that spanning tree is enabled on the ports, aggregated group of ports, by selecting the **STP Enabled** check box. You can disable this setting to remove particular ports from the spanning tree instance as needed. If disabled, the port will not participate in the spanning tree protocol or transmit any associated BPDUs.

4. Next, specify the path cost associated with the port(s), or aggregated group of ports, by selecting either **Auto** or **Specific** from the **Path Cost** drop-down menu. The path cost is used by spanning tree to determine which port to put in a forwarding state should a loop occur in the network. Selecting **Auto** indicates that the spanning tree protocol will automatically determine the cost of the path from the port to the root bridge. Selecting **Specific** allows you to then enter a specific cost for the port's path in the **Path Cost** field. Valid path cost range is **1** to **200000000**. Lower costs values can be assigned interfaces that should be selected by spanning tree first, and higher costs can be assigned to interfaces that should be selected last. If all ports have the same path cost, spanning tree selects the interface with the lowest

number should a loop occur. For example, in the image below, **port 1** is configured with a specific path cost of **12345**.



STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
-	☑	Auto		128	Non-Edge	☑	☐	☐	☐	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
*	☑	<>		<>	<>	☑	☐	☐	☐	<>
1	☑	Specific	12345	128	Non-Edge	☑	☐	☐	☐	Auto
2	☑	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
3	☑	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
4	☑	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
5	☑	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
6	☑	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
7	☑	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
8	☑	Auto		128	Non-Edge	☑	☐	☐	☑	Auto
9	☑	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
10	☑	Auto		128	Non-Edge	☑	☐	☐	☐	Auto

5. After specifying the port cost, specify the port's, or aggregated port group's, priority by selecting an appropriate value from the **Priority** drop-down menu. The port's priority is also used by spanning tree to determine which port to put in a forwarding state should a loop occur in the network. Higher priority is assigned to ports with a lower numerical **Priority** value. By default, each port is assigned a priority of **128**. Valid priority range is **0** to **240**, in multiples of **16**.

6. Next, specify the edge port configurations for the port(s) or aggregated port group. The port's edge port settings are determined by the **Admin Edge** drop-down menu, and the **Auto Edge** check box. By default, the **Auto Edge** feature is enabled on the port, indicating that spanning tree determines if it is an edge port based on whether or not BPDU messages are received on that port. If the port is determined to be an edge port, then spanning tree controls the port's state. When **Auto Edge** is disabled, you can manually specify whether or not the port is an edge port by selecting **Edge** from the **Admin Edge** drop-down menu.

7. If the port's role should be restricted, select the **Restricted Role** check box. By default, this feature is disabled. When enabled, it specifies that the port is not selected as the root port for the CIST (or any MSTI), even if it has the lowest cost or higher priority, although it does not keep the port from being selected as an alternative once the root port has been determined. Enabling this feature can be beneficial by preventing external bridges from influencing the active topology of the spanning tree instance; however, when enabled this feature can also cause a lack of spanning tree connectivity.

8. You can also choose to restrict TCN BPDU messages on the port, or aggregated port group, by selecting the **Restricted TCN** check box. By default, this feature is disabled. When enabled, the port does not propagate TCNs to other ports in the spanning tree instance. Enabling this feature can prevent a device outside the core region of the network from causing address flushing in the core region; however, when enabled it can also cause temporary loss of connectivity if any modifications to the network topology result in perpetuating incorrect topology information from the port.

9. To enable BPDU guarding on an edge ports within the CIST, select the **BPDU Guard** check box. This setting, when enabled, prevents the port from receiving BPDU messages, and causes the port to shut down if it does receive valid BPDU messages. This feature is disabled by default.

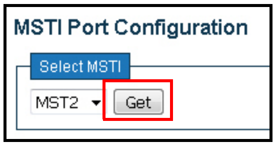
10. Lastly, specify the link type used on the port by selecting **Forced True**, **Forced False**, or **Auto** from the **Point-to-point** drop-down menu. The link type determines how quickly the spanning tree protocol will be able to disseminate network topology information between ports. By default, the switch automatically determines the link type based on the port's duplex mode (full-duplex ports are treated as point-to-point connected ports, and half-duplex ports are treated as shared connection ports); this is the **Auto** setting. To override the default (**Auto**) setting for the port, select either **Forced True** (specifying a point-to-point connection), or **Forced False** (specifying a shared connection) from the **Point-to-point** drop-down menu.
11. Once the spanning tree configuration for aggregated or individual port(s) associated with the CIST have been specified, select **Save** at the bottom of the menu to save these settings.

After configuring the spanning tree port settings, configuration for STP or RSTP is complete. To view STP or RSTP configurations and statistics, refer to *Troubleshooting on page 82*. If you are configuring MSTP, you can continue MSTP configuration by specifying port path cost and priority for each MSTI, as described in the next section.

Configuring MSTP MSTI Port Path Cost and Priority Using the GUI

With MSTP, you can specify the path cost and priority for each port, or an aggregated port group, associated with a particular MSTI. By default, these values are determined automatically by the spanning tree protocol, but they can be overridden per-MSTI on an aggregated group or per-port basis. To configure the path cost and priority for ports associated with a particular MSTI, connect to the ASE GUI and complete the following steps:

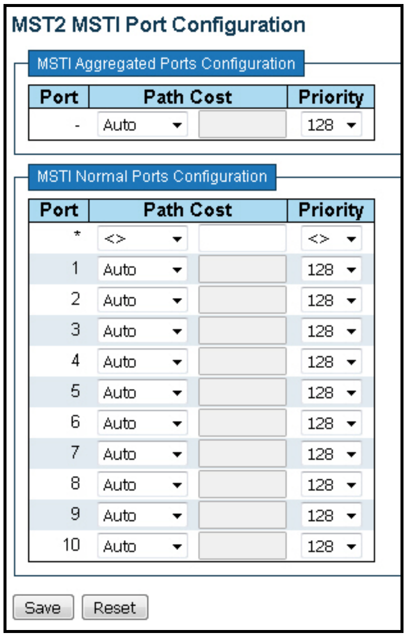
1. Navigate to the **Configuration** tab, and select **Spanning Tree** > **MSTI Ports**. In the **MSTI Port Configuration** menu, select the appropriate MSTI (MSTI1 through MSTI7) from the **Select MSTI** drop-down menu and select **Get**. The **MSTI Port Configuration** menu opens for the selected MSTI.



MSTI Port Configuration

Select MSTI

MST2



MST2 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost		Priority
-	Auto		128

MSTI Normal Ports Configuration

Port	Path Cost		Priority
*	<>		<>
1	Auto		128
2	Auto		128
3	Auto		128
4	Auto		128
5	Auto		128
6	Auto		128
7	Auto		128
8	Auto		128
9	Auto		128
10	Auto		128

2. Using your network topology and needs, determine if you will be configuring all ports associated with the particular MSTI as an aggregated group, or each port individually. If you are configuring the ports as an aggregated group, use the **MSTI Aggregated Ports Configuration** menu to configure the ports. If you are configuring each port individually, use the **MSTI Normal Ports Configuration** menu and make configuration selections for the appropriate port(s).
3. Specify the path cost for either the aggregated port group, or the specific port(s) by selecting either **Auto** or **Specific** from the **Path Cost** drop-down menu. The path cost is used by MSTP to determine which port on the MSTI to put in a forwarding state should a loop occur in the network. Selecting **Auto** indicates that the spanning tree protocol will automatically determine the cost of the path from the port to the root bridge. Selecting **Specific** allows you to then enter a specific cost for the port's path in the **Path Cost** field. Valid path cost range is **1** to **200000000**. Lower costs values can be assigned to interfaces that should be selected by MSTP first, and higher costs can be assigned to interfaces that should be selected last. If all ports have the same path cost, spanning tree selects the interface with the lowest number should a loop occur.
4. After specifying the port cost, then specify the port's priority by selecting an appropriate value from the **Priority** drop-down menu. The port's priority is also used by MSTP to determine which port to put in a forwarding state should a loop occur in the network. Higher priority is assigned to ports with a lower numerical **Priority** value. By default, each port is assigned a priority of **128**. Valid priority range is **0** to **240**, in multiples of **16**.
5. Once the path cost and priority for the aggregated port group, or specific port(s) on the MSTI, select **Save** at the bottom of the menu to save these settings.

After completing the additional MSTP configurations, the spanning tree configuration is complete. To view statistics associated with spanning tree configuration and operation, refer to *Troubleshooting on page 82*.

9. LAG and LACP Configuration Using the CLI

LAG and LACP are configured in similar manners; both LAG and LACP configuration includes creating a LAG/LACP group, assigning ports to the group, and specifying the group aggregation mode. LACP, because it operates dynamically, also includes configuration for port and link priority, link timeouts, and specifies whether revertive behavior is used on the LACP group or not. Once the LAG and LACP groups are created, populated, and defined, the forwarding mode used by both LAG and LACP is defined for the switch.

To configure these settings, connect to the ASE CLI and complete the following tasks:

- *Configuring LAG Groups Using the CLI on page 49*
- *Configuring LACP Using the CLI on page 50*
- *Configuring LAG and LACP Traffic Forwarding Mode Using the CLI on page 53*

These actions serve to create, populate, and define LAG and LACP groups and their behavior on the ASE device.

> **NOTE**
>
> *All configurations and instructions included in this section are completed on a device returned to the factory default settings.*

Configuring LAG Groups Using the CLI

By using LAG, multiple Ethernet ports can be bundled to form a single logical channel, which increases the link speed beyond the limits of a single port and increases redundancy on the switch. Configuration of the LAG feature on the ASE device when using the CLI includes creating a LAG group on the necessary ports and enabling LAG aggregation.

Enter the **`interface`** *`<interface>`* command from the Global Configuration mode prompt to enter the interface's configuration mode for the ports on which you want to create the LAG group. The *`<interface>`* parameter is specified in the format **`interface type`** *`<slot/port>`*; available interfaces differ by ASE switch model. Enter **`interface ?`** for a list of available interfaces. Ports can be specified as a single value, or as a range. For example, to create a LAG group for the **GigabitEthernet 1** interface using both ports **1** and **2** as group members, enter the command as follows:

```
#config terminal
(config)#interface GigabitEthernet 1/1-2
(config-if)#
```

Once in the interface's configuration mode, enter the **`[no] aggregation group`** *`<group id>`* **`mode on`** command to create the LAG group. Valid *`<group id>`* range depends on the ASE switch model. For an 8-port ASE switch, the range is **1** to **5**. The **`mode on`** parameters specify that this is a LAG group, using static mode and thus always on, and that LACP is not employed. Use the **`no`** form of this command to remove the LAG group from the ASE device configuration. For example, to create a LAG group with an ID of **3**, on the **GigabitEthernet 1** interface with both ports **1** and **2** as group members, enter the commands as follows:

```
#config terminal
(config)#interface GigabitEthernet 1/1-2
(config-if)#aggregation group 3 mode on
```

Once the LAG group has been created on the necessary ports, and the aggregation mode has been specified, the LAG configuration is complete except for specifying the forwarding mode used by both LAG and LACP groups, as described in *Configuring LAG and LACP Traffic Forwarding Mode Using the CLI on page 53*.

NOTE

*Because LACP is a dynamic version of LAG, when the **Static** setting is chosen for the group mode (indicating that link aggregation is always on), LACP is not used. Choosing **Static** as the group mode creates a LAG group, rather than an LACP group. When creating a LAG to an AOS based switch, ensure **Static** is configured on both the AES and AOS switches for supported functionality.*

Configuring LACP Using the CLI

LACP is configured on the ASE switch in a manner similar to LAG configuration in that it also requires a group configuration, with specified ports and mode settings. In addition, LACP configuration also includes the specification of revertive behavior, the maximum bundles allowed on the switch, and the link priority and timeout settings. Once these settings have been specified, the forwarding mode for both the LAG and LACP groups must be defined.

Configuring the LACP Group Using the CLI

The first step of configuring LACP is to configure the LACP group. LACP groups are configured in a similar manner to LAG groups, using the same commands in the CLI. To configure the LACP group, first create an LACP group on the necessary ports and specify the LACP aggregation mode.

Enter the **`interface`** *`<interface>`* command from the Global Configuration mode prompt to enter the interface's configuration mode for the ports on which you want to create the LACP group. The *`<interface>`* parameter is specified in the format **`interface type`** *`<slot/port>`*; available interfaces differ by ASE switch model. Enter **`interface ?`** for a list of available interfaces. Ports can be specified as a single value, or as a range. For example, to create an LACP group for the **GigabitEthernet 1** interface using both ports **1** and **2** as group members, enter the command as follows:

```
#config terminal
(config)#interface GigabitEthernet 1/1-2
(config-if)#
```

Once in the interface's configuration mode, enter the **`[no] aggregation group`** *`<group id>`* **`mode [active | passive]`** command to create the LACP group. Valid *`<group id>`* range depends on the ASE switch model. For an 8-port ASE switch, the range is **1** to **5**. The **`active`** parameter specifies that the LACP group is in active mode, indicating ports transmit LACP frames to connected devices no matter the mode of the connected group. The **`passive`** parameter specifies that the LACP group is in passive mode, indicating ports transmit LACP frames to connected devices only when they receive LACP frames first. Use the **`no`** form of this command to remove the LACP group from the ASE device configuration. To create an LACP group with an ID of **5**, on the **GigabitEthernet 1** interface with both ports **1** and **2** as group members, functioning in **active** mode, enter the commands as follows:

```
#config terminal
(config)#interface GigabitEthernet 1/1-2
(config-if)#aggregation group 5 mode active
```

After creating the LACP group and specifying its LACP operation mode, continue LACP configuration by defining whether the group operates in revertive mode and specifying the maximum number of members allowed in the group,,as described in the next section.

NOTE

*If any problems arise while swapping between **Active** and **Static**, try making the changes within the GUI. See Configuring the LACP Group Using the GUI on page 13 for details.*

Specifying LACP Revertive Behavior and Maximum Group Members Using the CLI

Once the LACP group has been created, and its operation mode specified, you must specify whether revertive behavior is used by the group and the maximum number of members supported in the group.

To begin these LACP configurations, you must first enter the local link aggregation (LLAG) interface configuration mode using the **`interface llag`** *`<group id>`* command from the Global Configuration mode prompt. The *`<group id>`* specifies the LACP group that you will be configuring. Enter the command as follows:

```
(config)#interface llag 3
(config-llag)#
```

Next, specify whether the group operates in revertive mode or not by entering the **`[no] lacp failover [non-revertive | revertive]`** command from the LLAG interface configuration mode prompt. Entering the **`revertive`** parameter indicates the LACP group operates in revertive mode, and therefore when LACP is used between linked devices, if a better, or higher priority, link becomes available, the link communication switches to the higher priority link. This is the default setting for LACP groups and can be beneficial because it allows connected devices to utilize the best link for communication and allows for redundancy when links become inactive or go into standby mode. Entering the **`non-revertive`** parameter disables the ability for the group to switch between higher priority links. Non-revertive behavior can be beneficial when traffic disruption must be avoided. Link priority is configured separately (as described in *Specifying LACP Priority and Timeout Settings Using the CLI on page 52*), but those priorities determine which links are used when the LACP group operates in revertive mode. Using the **`no`** form of this command returns the LACP group to the default revertive behavior. To disable the revertive behavior for the LACP group, enter the command as follows:

```
(config)#interface llag 3
(config-llag)#lacp failover non-revertive
```

Lastly, specify the maximum number of bundles supported in the LACP group by entering the **[no] lacp max-bundle** *<value>* command from the LLAG interface configuration mode prompt. The valid *<value>* range is determined by the number of LACP groups available on the ASE device. For example, if **5** LACP groups are available, the maximum bundle is **10**. The number of members allowed in an LACP group can be restricted by setting the maximum bundle to a number less than the number of group members. Additional members of the group become standby ports and do not forward any frames, unless an active member of the group becomes disabled, in which case the standby member of the highest priority becomes active and takes over frame transmission. Using the **no** form of this command returns the maximum bundle value to the default setting. To configure the maximum number of members allowed to **3**, in the 3rd LACP group, enter the command as follows:

```
(config)#interface llag 3
(config-llag)#lacp max-bundle 3
```

NOTE

You can achieve one to one active and standby behavior on a LACP group by creating a single group with two associated ports, and specifying the **max-bundle** *value as* ***1****. In this case, the LACP group port with the higher priority actively forwards traffic, while the lower priority port is in standby mode. If the active port goes down for any reason, the standby port takes over and begins forwarding traffic.*

Once the revertive behavior and maximum bundle settings have been configured for the LACP group, you can then specify the link priority and timeout settings for the LACP groups by following the steps described in the next section.

Specifying LACP Priority and Timeout Settings Using the CLI

Once the LACP group has been created, defined, and enabled, you must set the LACP system priority and port priorities for the ports included in the LACP group, as well as specify the port timeout settings.

The LACP priority settings include setting the system priority, which determines the priority for the ASE device when connected to other devices using LACP. The priority settings for the ports within the LACP group determine which ports are active, and which are in standby mode. The ports with the higher priority are used as active ports, and the lower priority ports are typically in standby mode, unless needed for failover or backup scenarios. The lower the number assigned to the port, the higher the port priority. The same priority hierarchy principles apply to the system priority setting for the ASE device in the LACP network.

The port timeout settings control the period between LACP message transmission. Transmissions can be configured to be sent each second, or every 30 seconds. By default, messages are sent every second.

To configure LACP system priority settings, enter the **[no] lacp system-priority** *<value>* command from the Global Configuration mode prompt. This command sets the priority for the ASE device in the LACP connected network. Valid *<value>* range is **1** to **65535**, with a default value of **32768**; it is important to remember that the lower the entered value, the higher the priority. Using the **no** form of this command returns the LACP system priority to the default setting. To change the system's LACP priority, enter the command as follows:

```
(config)#lacp system-priority 1500
```

To configure the LACP group port priority settings, enter the **[no] lacp port-priority** *<value>* command from the interface's configuration mode. This command sets the priority for the port within the LACP group. Valid *<value>* range is **1** to **65535**, with a default value of **32768**; it is important to remember that the lower the entered value, the higher the priority. Using the **no** form of this command returns the LACP port priority to the default setting. To change the port's LACP priority, enter the command as follows:

```
(config)#interface GigabitEthernet 1/1-2
```

```
    (config-if)#lacp port-priority 1500
```

To configure the period between LACP message transmission on the port, enter the **[no] lacp timeout [fast | slow]** command from the interface's configuration mode. Entering the **fast** parameter specifies that LACP messages are sent every second. Entering the **slow** parameter specifies that LACP messages are sent every **30** seconds. By default, LACP messages are sent every second (**fast**). Using the **no** form of this command returns the timeout value to the default setting. To change the LACP message timeout value, enter the command as follows:

```
    (config)#interface GigabitEthernet 1/1-2
    (config-if)#lacp timeout slow
```

Once the LACP timeout values and priorities have been configured, you can complete the LACP and LAG configuration by specifying the LAG and LACP forwarding mode, as described in the following section.

Configuring LAG and LACP Traffic Forwarding Mode Using the CLI

LAG and LACP traffic forwarding modes are set at a Global level across the ASE device, and are used to specify the methods used to determine the destination port for a traffic frame. Forwarding decisions are based on source or destination MAC addresses, IP addresses, or TCP and UDP port numbers. These modes can be combined, and by default, LAG and LACP traffic forwarding modes use the source MAC address, IP address, and TCP/UDP port numbers for determining traffic destinations. The destination MAC address is not used in the default configuration. The forwarding mode is specified once on the ASE device and applies to all configured LAG and LACP groups.

To configure the LAG and LACP forwarding modes, enter the **[no] aggregation mode [dmac | ip | port | smac]** command from the Global Configuration mode prompt. The **dmac** parameter specifies that destination MAC addresses are used by link aggregation in calculating traffic destinations. The **ip** parameter specifies that IP addresses are used. The **port** parameter specifies that TCP and UDP port numbers are used in calculating traffic destinations, and the **smac** parameter specifies that source MAC addresses are used. By default, destinations are determined by using **ip**, **port**, and **smac** parameters. All of these parameters can be used, and can be entered in any order. Using the **no** form of this command returns the traffic forwarding calculations to the default settings. To change the methods used to calculate traffic destination for LACP forwarded traffic, enter the command as follows:

```
    (config)#aggregation mode dmac port
```

NOTE

Any change in the LAG/LACP forwarding mode stops all traffic forwarding until the mode is fully specified.

Once the LAG and LACP forwarding mode has been defined, the LAG and LACP configuration is complete. You can view LAG and LACP statistics on the ASE device by using the instructions detailed in *Troubleshooting on page 82*.

10. MAC Address Table Configuration Using the CLI

The MAC address table keeps entries of the source and destination MAC addresses used for communication between devices connected to the ASE switch. The addresses can be learned dynamically by the ASE device, or entered manually when needed. Configuration of the MAC address table in the ASE device includes configuring the aging time used for table entries, manually adding static MAC addresses to the table when necessary, and optionally configuring the MAC address learning behavior. The configuration steps for these tasks are described in the following sections:

- *Configuring the MAC Address Table Entry Aging Time Using the CLI on page 54*

- *Adding Static MAC Address Entries to the MAC Address Table Using the CLI on page 54*
- *Configuring MAC Address Table Learning Behavior Using the CLI (Optional) on page 54*

NOTE

All configurations and instructions included in this section are completed on a device returned to the factory default settings.

Configuring the MAC Address Table Entry Aging Time Using the CLI

When traffic from a specific source MAC address ceases, the MAC address table automatically removes the address entry from the table after being inactive for a configurable amount of time (aging time).

To configure the MAC address table entry aging time, enter the **[no] mac address-table aging-time** *<value>* command from the Global Configuration mode prompt. The *<value>* parameter defines the time, in seconds, before an inactive entry is removed from the table. Valid *<value>* range is **10** to **1000000** seconds, with a default value of **300** seconds. Entering **0** as the value disables the automatic aging feature, and all entries remain in the table unless manually deleted. Using the **no** form of this command returns the aging time to the default value.

To change the MAC address table aging time, enter the command as follows:

```
(config)#mac address-table aging-time 500
```

Adding Static MAC Address Entries to the MAC Address Table Using the CLI

MAC addresses can be manually entered into the MAC address table by creating static MAC address entries.

To add a static MAC address entry to the MAC address table, enter the **[no] mac address-table static** *<mac address>* **vlan** *<vlan id>* **[interface** *<interface>***]** command from the Global Configuration mode prompt. The *<mac address>* parameter is the MAC address you are adding to the MAC address table. MAC addresses should be expressed in the following format **xx:xx:xx:xx:xx:xx** (for example, **00:A0:C8:00:00:01**). The *<vlan id>* parameter is the VLAN to which you are associating the MAC address. Valid *<vlan id>* range is **1** to **4095**. The optional **interface** *<interface>* parameter specifies the port to which you are associating the MAC address. The *<interface>* parameter is specified in the format **interface type** *<slot/port>*; available interfaces differ by ASE switch model. Enter **interface ?** for a list of available interfaces. Using the **no** form of this command removes the specified MAC address from the MAC address table.

To add a static MAC address to the MAC address table, enter the command as follows:

```
(config)#mac address-table static 00:A0:C8:00:00:01 vlan 2 interface
GigabitEthernet 1/1
```

Configuring MAC Address Table Learning Behavior Using the CLI (Optional)

By default, the MAC address table learns new source MAC addresses dynamically when new address are processed by the switch. If traffic is sent from a source MAC address that does not already exist in the MAC address table, it is automatically learned and added to the table. You can optionally change this behavior by disabling MAC address learning on specific ports or VLANs, or by specifying that secure MAC addresses are also learned and added to the MAC address table. By default, secure MAC addresses are not included in the address table. Configuring MAC address table learning behavior using the CLI includes configuring VLAN learning behavior from the Global Configuration mode, and configuring port learning behavior from the interface configuration mode.

To configure MAC address learning behavior on the port, enter the **[no] mac address-table learning [secure]** command from the interface's configuration mode. This command enables or disables the automatic learning of source MAC addresses for the port. By default, this feature is enabled. The optional **secure** parameter specifies that secure MAC addresses are learned by the switch and added to the MAC address table. By default, secure MAC addresses are not included in the address table. Using the **no** form of this command disables dynamic learning of source MAC addresses on the port. To enable the dynamic addition of secure MAC addresses on the port, if it has been disabled, enter the command as follows:

```
(config)#interface GigabitEthernet 1/1
(config-if)#mac address-table learning secure
```

To configure MAC address learning behavior for VLANs, enter the **[no] mac address-table learning vlan** *<vlan ids>* command from the Global Configuration mode prompt. By default, this feature is enabled on all VLANs. The *<vlan ids>* parameter specifies a single VLAN ID, or a range of VLAN IDs separated by a hyphen or comma, on which to enable (or disable) this feature. Valid *<vlan ids>* range is **1** to **4095**. Using the **no** form of this command disables the ability for the VLAN to automatically learn and add source MAC addresses to the MAC address table. To disable this feature for VLANs **2** to **6**, enter the command as follows:

```
(config)#no mac address-table learning vlan 2-6
```

Once the MAC address table entries, learning behavior, and aging time have been configured, the MAC address table configuration is complete. You can view MAC address table statistics on the ASE device as described in *Troubleshooting on page 82*.

11. VLAN Configuration Using the CLI

VLANs are used on the ASE device to logically divide traffic across the network. VLANs can be configured for specific types of data streams, including VoIP traffic, and can be configured so that specific ports are used by designated VLANs for specific traffic, thus making network management much easier.

When creating a new VLAN, ports are configured according to port mode, VLAN ID, port type, ingress traffic filtering behavior, ingress traffic acceptance behavior, and egress traffic tagging behavior. To configure VLANs on the ASE device, complete the following tasks:

- *Configuring VLAN Port Modes and VLAN IDs Using the CLI on page 55*
- *Configuring VLANs for Access Ports Using the CLI on page 56*
- *Configuring VLANs for Trunk and Hybrid Ports Using the CLI on page 57*
- *Configuring Shared VLAN Learning Using the CLI on page 60*

NOTE

All configurations and instructions included in this section are completed on a device returned to the factory default settings.

Configuring VLAN Port Modes and VLAN IDs Using the CLI

The first step in VLAN configuration is to specify the port mode for the ports to be used in the VLAN and associate the port with a VLAN ID. There are three supported types of port modes in the ASE device: **access**, **trunk**, and **hybrid** modes. Different port modes serve different purposes on the network and include different types of configuration. For example, **access** ports usually connect to end points on the network, **trunk** ports are used to connect to other switches in the network, and **hybrid** ports perform in a similar manner to trunk ports, but with additional configurations and abilities. *Table 2 on page 56* describes the characteristics of each port mode type.

Table 2. VLAN Port Mode Types and Characteristics

Port Mode	Typical Usage	Characteristics
Access	Used to connect the switch to endpoints on the network	• Default port mode • Member of exactly one VLAN (VLAN 1 by default, either Port VLAN or Access VLAN) • Accepts untagged and C-tagged frames • Transmits untagged egress frames
Trunk	Used to connect the switch to other switches on the network	• Member of all existing VLANs by default • Can transmit traffic on multiple VLANs simultaneously • All frames are tagged on egress by default, except for those classified to the Port VLAN or Native VLAN • Egress tagging can be enabled for all frames, however that means only tagged frames are accepted upon ingress
Hybrid	Used to connect the switch to other switches on the network, and operate similarly to trunk ports	• Includes all characteristics of trunk ports • Can be configured to be VLAN tag unaware • Can be configured to be C-tag, S-tag, or S-Custom-tag aware • Ingress filtering can be configured and controlled • Frame ingress acceptance and egress frame tagging can be configured independently

To specify the port's mode for VLAN configuration, enter the **[no] switchport mode [access | hybrid | trunk]** command from the interface's configuration mode. Entering the **access** parameter specifies the port as an access port, entering the **hybrid** parameter specifies the port as a hybrid port, and entering the **trunk** parameter specifies the port is a trunk port. By default, ports are in **access** mode. Using the **no** form of this command returns the port to the default setting. Enter the command as follows:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport mode trunk
```

Once the port mode has been configured, associate the port with a VLAN using one of the following commands from the interface's configuration mode: **[no] switchport access vlan** *<id>*, **[no] switchport hybrid native vlan** *<id>*, or **[no] switchport trunk native vlan** *<id>*. The **switchport access** command defines the VLAN ID for an access port, the **switchport hybrid** command defines the VLAN ID for a hybrid port, and the **switchport trunk** command defines the VLAN ID for a trunk port. Valid *<id>* range is **1** to **4095**; by default, each port is associated with the default VLAN (**VLAN 1**). Using the **no** form of this command returns the port to the default setting. For example, to configure a trunk port associated with VLAN 3, enter the command as follows:

```
(config-if)#switchport trunk native vlan 3
```

After configuring the port mode type and associating a VLAN ID with the port, continue VLAN configuration by following the steps outlined in *Configuring VLANs for Access Ports Using the CLI on page 56* for access ports, and *Configuring VLANs for Trunk and Hybrid Ports Using the CLI on page 57* for trunk or hybrid ports.

Configuring VLANs for Access Ports Using the CLI

If the port mode type for the VLAN was specified as **access**, the remainder of the VLAN configuration is based on creating data connections to the endpoints in the network. The **access** port mode is the default setting for all ports, in the default VLAN, and therefore only a few additional configuration steps are necessary to complete VLAN configuration for access ports.

By default, access ports have ingress filtering enabled, which indicates that incoming traffic for a VLAN of which the port is not a member is discarded. In addition, access ports are configured as a C-port, so that on ingress, frames with a VLAN tag with a tag protocol ID (TPID) of 0x8100 are associated with the VLAN ID embedded in the tag. If the frame is untagged, or priority tagged, the frame is associated with the VLAN ID configured on the port. If frames must be tagged on egress, they are tagged with a C-tag. These settings cannot be changed on an access port.

The only additional configurations for VLAN access ports is to specify the VLANs forbidden by the access ports. Defining forbidden VLANs occurs at the interface level, by entering the **switchport forbidden vlan [add** *<vlan ids>* **| remove** *<vlan ids>***]** command from the interface's configuration mode. Entering the **add** *<vlan ids>* parameter adds VLANs to the list of forbidden VLANs for the port, and entering the **remove** *<vlan ids>* parameter removes VLANs from the list of forbidden VLANs for the port. The *<vlan ids>* parameter specifies a list of VLANs in which the port is forbidden to transmit traffic. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid *<vlan ids>* range is **1** to **4095**. For example, to add VLANs 3, 5, and 100 to the forbidden VLAN list for an access port, enter the command as follows:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport forbidden vlan add 3,5,100
```

Configuring VLANs for Trunk and Hybrid Ports Using the CLI

If the port mode type for the VLAN was specified as **trunk** or **hybrid**, there are several additional configurations available for connecting these ports, and their associated VLANs, to other switches on the network. Both **trunk** and **hybrid** port modes have configurable port types, ingress acceptance criteria, egress traffic tagging preferences, and allowed and forbidden VLANs. In addition, hybrid ports can be configured with ingress filtering disabled.

To configure these settings, connect to the ASE CLI and complete the following tasks:

- *Configuring VLAN Port Types Using the CLI (Hybrid Ports Only) on page 57*
- *Configuring VLAN Ingress Filtering Using the CLI (Hybrid Ports Only) on page 58*
- *Configuring VLAN Ingress Acceptance Criteria for Ports Using the CLI (Hybrid Ports Only) on page 59*
- *Configuring Egress Traffic Tagging for Trunk and Hybrid Ports Using the CLI on page 59*
- *Specifying Allowed and Forbidden VLANs for Trunk and Hybrid Ports Using the CLI on page 60*

These actions serve to create, configure, and specify VLAN behavior for trunk and hybrid ports on the ASE device.

Configuring VLAN Port Types Using the CLI (Hybrid Ports Only)

For VLAN ports configured in **hybrid** mode, you can specify whether the VLAN tag of ingress traffic is used to classify the incoming frames to a particular VLAN by configuring the port type associated with the VLAN port. Four port types are supported: Unaware, C-Port, S-Port, and S-Custom-Port. These port types are associated with specific TPIDs, and when configured, use the TPID to classify ingress traffic to the VLAN associated with the port. Port types are configured for hybrid ports by entering the **[no] switchport hybrid port-type [c-port | s-custom-port | s-port | unaware]** command from the interface's configuration mode. Using the **no** form of this command returns the port to the default setting (**unaware**).

When the port type is set to **`c-port`**, all ingress frames with a VLAN tag TPID of 0x8100 are classified to the VLAN ID embedded in the tag. If a frame is untagged, or has a priority tag, the frame is classified to the VLAN associated with the port. With this setting, any egress frames that must be tagged are tagged with a C-tag.

> **NOTE**
>
> *By default, all ports in* **`trunk`** *or* **`access`** *mode are set to* **`c-port`**. *This setting cannot be changed for ports in these modes.*

When the port type is set to **`s-custom-port`**, all ingress frames with a VLAN tag TPID of 0x8100, or a value equal to the Ethertype configured for S-Custom-Ports (using the **`vlan ethertype s-custom-port`** command), are classified to the VLAN ID embedded in the tag. If a frame is untagged, or has a priority tag, the frame is classified to the VLAN associated with the port. With this setting, any egress frames that must be tagged are tagged with the custom S-tag.

When the port type is set to **`s-port`**, all ingress frames with a VLAN tag TPID of 0x8100 or 0x88A8 are classified to the VLAN ID embedded in the tag. If a frame is untagged, or has a priority tag, the frame is classified to the VLAN associated with the port. With this setting, any egress frames that must be tagged are tagged with an S-tag.

When the port type is set to **`unaware`**, all ingress frames (whether carrying a VLAN tag or not) are classified to the VLAN associated with the port. This is the default setting for hybrid ports.

To configure a port type for VLAN ports in hybrid mode, enter the command from the interface’s configuration mode as follows:

```
(config-if)#switchport hybrid port-type c-port
```

If the hybrid port type is configured to **`s-custom-port`**, you must also specify the custom port setting using the **`[no] vlan ethertype s-custom-port`** *`<type>`* command from the Global Configuration mode prompt. The *`<type>`* parameter is the Ethertype used by port to classify incoming VLAN traffic. Valid range is **0x0600** to **0xffff**, and is set to **0x88A8** by default. Using the **`no`** form of this command returns the custom Ethertype to the default value. Enter the command as follows:

```
(config)#vlan ethertype s-custom-port 0x0600
```

After configuring the port type for hybrid ports, you can continue port VLAN configuration by specifying the VLAN ingress filtering parameters as described in the next section.

Configuring VLAN Ingress Filtering Using the CLI (Hybrid Ports Only)

By default, ports configured in **`hybrid`** mode have ingress filtering disabled. All other port types (**`access`** and **`trunk`**) have ingress filtering enabled by default, and that setting cannot be changed. Enabling ingress filtering on a hybrid port indicates that incoming traffic for a VLAN of which the port is not a member is discarded.

To enable ingress filtering on a hybrid port, enter the **`[no] switchport hybrid ingress-filtering`** command from the interface’s configuration mode. Using the **`no`** form of this command disables ingress filtering. Enter the command as follows:

```
(config-if)#switchport hybrid ingress-filtering
```

Once ingress filtering has been enabled for the hybrid port, you can continue VLAN configuration for hybrid ports by specifying their ingress traffic acceptance criteria as described in the next section.

Configuring VLAN Ingress Acceptance Criteria for Ports Using the CLI (Hybrid Ports Only)

After specifying the port type and ingress filtering behavior for ports in **hybrid** mode, you can begin configuring the ingress acceptance criteria for these ports. Only ports in **hybrid** mode can be configured to specify the type of frames that are accepted on ingress. By default, ports in either **access** or **trunk** modes accept either tagged or untagged frames, and this setting cannot be changed. Options available for ports in **hybrid** mode include **all**, **tagged**, and **untagged**.

When the accepted frame types for the port is specified as **all**, both types of frames are accepted. When the accepted frame type is specified as **tagged**, only tagged ingress frames are accepted and all others are discarded. When the accepted frame type is specified as **untagged**, only untagged ingress frames are accepted and all others are discarded.

To specify the accepted ingress frame type for the hybrid port, enter the **[no] switchport hybrid acceptable-frame-type [all | tagged | untagged]** command from the interface's configuration mode. By default, hybrid ports accept **all** frame types. Using the **no** form of this command returns the accepted frame type to the default setting. Enter the command as follows:

```
    (config-if)#switchport hybrid acceptable-frame-type untagged
```

After specifying the ingress frame types accepted on the hybrid port, continue VLAN configuration by specifying the tagging preferences for egress traffic on both hybrid and trunk ports as described in the following section.

Configuring Egress Traffic Tagging for Trunk and Hybrid Ports Using the CLI

While **access** ports do not tag egress traffic, ports that are configured in either **trunk** or **hybrid** mode can be configured to control the tagging of egress traffic as needed. By default, egress traffic tagging behavior for both port types is that traffic associated with the port's VLAN is transmitted untagged at egress, and any traffic not associated with the port's VLAN is transmitted with its relevant tag.

To change the egress tagging behavior of hybrid ports, enter the **[no] switchport hybrid egress-tag [all | none]** command from the interface's configuration mode. Entering the **all** parameter specifies that all egress traffic is transmitted with a tag, whether it is classified as part of the port's VLAN or not. Entering the **none** parameter specifies that all egress traffic is transmitted without a tag, whether it is classified as part of the port's VLAN or not. Using the **no** form of this command returns the hybrid port to the default tagging behavior (only traffic not associated with the port VLAN is tagged). Enter the command as follows:

```
    (config-if)#switchport hybrid egress-tag none
```

To change the egress tagging behavior of trunk ports, enter the **[no] switchport trunk vlan tag native** command from the interface's configuration mode. This command specifies that traffic classified as part of the port's VLAN is tagged upon egress, in addition to the traffic that is already tagged because it is not part of the port's VLAN. In effect, all traffic is tagged upon egress when this command is issued. Using the **no** form of this command returns the port to the default tagging behavior (only traffic not associated with the port VLAN is tagged).

Enter the command as follows:

```
    (config-if)#switchport trunk vlan tag native
```

After specifying the egress frame tagging behavior on the trunk or hybrid ports, continue VLAN configuration by specifying the allowed or forbidden VLANs on both hybrid and trunk ports as described in the following section.

Specifying Allowed and Forbidden VLANs for Trunk and Hybrid Ports Using the CLI

For both trunk and hybrid ports, you can specify of which VLANs each port type is allowed to become a member, and of which VLANs the port is forbidden to become a member. By default, all ports are allowed to become members of all available VLANs.

To specify of which VLANs the hybrid or trunk port is allowed to become a member, enter the **[no] switchport [hybrid | trunk] allowed vlan [***<vlan ids>* **| add** *<vlan ids>* **| all | except** *<vlan ids>***| none | remove** *<vlan ids>***]** command from the interface's configuration mode. The **hybrid** and **trunk** parameters specify whether you are configuring allowed VLANs for a hybrid or trunk port. The *<vlan ids>* parameter specifies a list of VLANs in which the port is allowed to transmit traffic. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid *<vlan ids>* range is **1** to **4095**. The **add** *<vlan ids>* parameter specifies VLAN IDs to add to the allowed VLAN list. The **all** parameter specifies that all configured VLANs are allowed. The **except** *<vlan ids>* parameter specifies that all configured VLANs are allowed except for the specified VLANs. The **none** parameter specifies that no VLANs are allowed for the port. The **remove** *<vlan ids>* parameter specifies that the listed VLANs are removed from the allowed VLAN list. Using the **no** form of this command returns the allowed VLAN list to the default setting (all ports are allowed to become members of all available VLANs). To configure the allowed VLANs list for a previously configured trunk port, enter the command as follows:

```
(config-if)#switchport trunk allowed vlan 3, 5, 100
```

To specify VLANs forbidden by the trunk or hybrid ports, enter the **switchport forbidden vlan [add** *<vlan ids>* **| remove** *<vlan ids>***]** command from the interface's configuration mode. Entering the **add** *<vlan ids>* parameter adds VLANs to the list of forbidden VLANs for the port, and entering the **remove** *<vlan ids>* parameter removes VLANs from the list of forbidden VLANs for the port. The *<vlan ids>* parameter specifies a list of VLANs in which the port is forbidden to transmit traffic. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid *<vlan ids>* range is **1** to **4095**. For example, to add VLANs **7**, **15**, and **200** to the forbidden VLAN list for a previously configured trunk port enter the command as follows:

```
(config-if)#switchport mode trunk
(config-if)#switchport forbidden vlan add 7,15,200
```

Once you have configured the allowed or forbidden VLANs for the trunk or hybrid ports, and the VLANs associated with those ports have been configured, the VLAN configuration is complete. You can view details of the VLAN configuration and statistics on the ASE device as described in *Troubleshooting on page 82*.

Configuring Shared VLAN Learning Using the CLI

Shared VLAN learning (SVL) allows frames that are initially classed to a particular VLAN to be bridged on a shared VLAN. When enabled, SVL allows two or more VLANs to be grouped together to share common source address information in the MAC address table. SVL can be beneficial for more complex, asymmetrical cross-VLAN traffic patterns and configurations, such as E-TREE.

SVL operation depends on the filter ID (FID) associated with the MAC address in the MAC address table. Without SVL, each VLAN is associated with one FID, which in turn is associated with one MAC address. By using SVL, the specified FID can be used by multiple VLANs, which learn the FID from the MAC address table when SVL is enabled. SVL is configured by specifying which VLANs are mapped to which FIDs. A single VLAN can only be associated with one FID, so although multiple VLANs can use the same FID, one VLAN cannot use more than one FID.

To enable SVL, and specify which VLANs are associated with which FID, enter the **[no] svl fid** *<fid>* **vlan** *<vlan ids>* command from the Global Configuration mode prompt. The *<fid>* parameter specifies the FID to which the VLANs will be associated. Valid *<fid>* range is **1** to **4095**. The *<vlan ids>* parameter specifies a list of VLANs to associate with the FID. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid *<vlan ids>* range is **1** to **4095**. Using the **no** form of this command disables SVL on the ASE device. Enter the command as follows:

```
(config)#svl fid 1 vlan 3-75
```

Once the SVL settings have been configured, you can view VLAN configuration and statistics on the ASE device as described in *Troubleshooting on page 82*.

12. Port Mirroring Configuration Using the CLI

Port mirroring in the ASE device uses three types of mirroring: local mirroring, where the source and destination ports are on the same local switch, source remote mirroring (RMirror), where the port on a local ASE switch is a source for a separate destination, and destination RMirror, where a port on the local ASE switch is a destination for traffic monitored on a separate source. Configuring port mirroring depends on configuring a source port or VLAN, from where the traffic is copied, and a destination port, where the copied traffic is captured. Sources can be configured to capture transmitted traffic only, received traffic only, or both, and can be configured on the local device only (local mirroring) or with a source or destination on a separate device (RMirror).

To configure port mirroring, connect to the ASE CLI and complete the following tasks:

- *Configuring the Mirroring Session Using the CLI on page 61*
- *Configuring the Mirror Source Using the CLI on page 62*
- *Configuring the Mirror Destination Using the CLI on page 63*
- *Mirroring Configuration Examples Using the CLI on page 64*

NOTE

All configurations and instructions included in this section are completed on a device returned to the factory default settings.

Configuring the Mirroring Session Using the CLI

The first step in configuring port mirroring on the ASE device when using the CLI is to configure the mirroring session. Up to five simultaneous mirroring sessions are supported. Configuring the mirroring session includes providing a session ID and enabling the mirroring feature.

To enable the mirroring feature and specify a session ID, enter the **[no] monitor session** *<session id>* command from the Global Configuration mode prompt. By default, the mirroring feature is disabled and no sessions are configured. Valid *<session id>* range depends on the ASE switch model. For an 8-port ASE switch, the range is **1** to **5**. Using the **no** form of this command disables the mirroring feature.

Enter the command as follows:

```
(config)#monitor session 1
(config)#
```

Configuring the Mirror Source Using the CLI

Once the mirroring feature has been enabled, you can begin configuring the mirroring source, whether port or VLAN, and whether local or remote. Configuring the source includes specifying the port or VLAN to be used as the source, and the type of traffic that will be mirrored.

NOTE

To capture traffic from the switch itself, the CPU must be mirrored in addition to a source port.

Configuring a Local Mirroring Source Port Using the CLI

To configure a port as the local mirroring source, enter the **`[no] monitor session`** *`<session id>`* **`source interface`** *`<interface>`* **`[both | rx | tx]`** command from the Global Configuration mode prompt. The *`<session id>`* parameter specifies the monitoring session that you are configuring. Valid *`<session id>`* range depends on the ASE switch model. For an 8-port ASE switch, the range is **1** to **5**. The **`interface`** *`<interface>`* parameter specifies the port from which to mirror traffic. The *`<interface>`* parameter is specified in the format **`interface type`** *`<slot/port>`*; available interfaces differ by ASE switch model. Enter **`interface ?`** for a list of available interfaces. Specify the type of traffic using the **`both`**, **`rx`**, and **`tx`** keywords. The **`rx`** keyword specifies that traffic received on the port is mirrored, **`tx`** indicates that traffic transmitted on the port is mirrored, and **`both`** indicates both received and transmitted traffic is mirrored. By default, no mirroring sessions are configured. Using the **`no`** form of this command removes the mirroring session configuration. Enter the command as follows to specify the GigabitEthernet 1/1 interface as a source port for a local mirroring session monitoring transmitted traffic:

```
(config)#monitor session 1 source interface GigabitEthernet 1/1 tx
```

Configuring a Local Mirroring Source VLAN Using the CLI

In ASE mirroring, you can choose to specify a source VLAN from which to mirror traffic, instead of a source port. Mirrored traffic is still sent to a destination port to be analyzed, but it is traffic over the VLAN rather than the port interface. If a source VLAN is specified, for VLAN-based mirroring, a source port cannot be specified. VLAN and port mirroring are mutually exclusive, and only one can be mirrored at a time.

NOTE

VLAN-based mirroring is only available for local mirroring sessions.

To specify a source VLAN for VLAN-based mirroring, enter the **`[no] monitor session`** *`<session id>`* **`source vlan`** *`<vlan id>`* command from the Global Configuration mode prompt. The *`<session id>`* parameter specifies the monitoring session that you are configuring. Valid *`<session id>`* range depends on the ASE switch model. For an 8-port ASE switch, the range is **1** to **5**. The **`vlan`** *`<vlan id>`* parameter specifies the VLAN from which to mirror traffic. Valid *`<vlan id>`* range is **1** to **4095**. Using the **`no`** form of this command removes the mirroring session configuration.

NOTE

Because using a VLAN and a port as sources for local mirroring are mutually exclusive, you should clear the mirroring session configuration from local source interfaces before specifying the VLAN as the mirroring source. Clear the mirroring session using the **`no monitor session`** *`<session id>`* **`interface *`** *command to clear all source interfaces from the session.*

Enter the command as follows to specify that traffic for VLAN 3 is mirrored:

```
(config)#no monitor session 1 source interface *
(config)#monitor session 1 source vlan 3
```

Configuring a Source Remote Mirror VLAN Using the CLI

When configuring remote mirroring, you can specify a VLAN used specifically for source remote mirroring traffic by entering the **[no] monitor session** *<session id>* **source remote vlan** *<vlan id>* command from the Global Configuration mode prompt. The *<session id>* parameter specifies the monitoring session that you are configuring. Valid *<session id>* range depends on the ASE switch model. For an 8-port ASE switch, the range is **1** to **5**. The **remote vlan** *<vlan id>* parameter specifies the VLAN to use for sending remote mirror traffic. Valid *<vlan id>* range is **1** to **4095**; by default the remote mirroring VLAN is set to **200**. Using the **no** form of this command removes the mirroring session configuration. Enter the command as follows to specify that VLAN 350 is used for mirrored traffic:

```
(config)#monitor session 1 source remote vlan 350
```

Configuring the Mirror Destination Using the CLI

Once the mirroring session global and source settings have been configured, you can configure the mirroring destination. Configuring the destination includes specifying the port to be used as the mirroring destination, and creating the remote mirroring VLAN and reflector port to be used for sending remote mirroring traffic.

Configuring a Mirroring Destination Port Using the CLI

To configure a port as the mirroring destination, enter the **[no] monitor session** *<session id>* **destination interface** *<interface>* command from the Global Configuration mode prompt. The *<session id>* parameter specifies the monitoring session that you are configuring. Valid *<session id>* range depends on the ASE switch model. For an 8-port ASE switch, the range is **1** to **5**. The **interface** *<interface>* parameter specifies the port to which to send mirror traffic. The *<interface>* parameter is specified in the format **interface type** *<slot/port>*; available interfaces differ by ASE switch model. Enter **interface ?** for a list of available interfaces. By default, no mirroring sessions are configured. Using the **no** form of this command removes the mirroring session configuration. Enter the command as follows to specify the GigabitEthernet 1/1 interface as a destination port for mirroring session 1:

```
(config)#monitor session 1 destination interface GigabitEthernet 1/1
```

Configuring a Destination Remote Mirror VLAN and Reflector Port Using the CLI

When configuring remote mirroring, you can specify a VLAN used specifically for transmitting remote mirroring traffic, and a reflector port used to send that traffic, by entering the **[no] monitor session** *<session id>* **destination remote vlan** *<vlan id>* **reflector-port** *<interface>* command from the Global Configuration mode prompt. The *<session id>* parameter specifies the monitoring session that you are configuring. Valid *<session id>* range depends on the ASE switch model. For an 8-port ASE switch, the range is **1** to **5**. The **remote vlan** *<vlan id>* parameter specifies the VLAN to use for sending remote mirror traffic. Valid *<vlan id>* range is **1** to **4095**; by default the remote mirroring VLAN is set to **200**. The **reflector-port** *<interface>* parameter creates the reflector port for remote mirroring. The reflector port directs the mirrored traffic to the mirroring VLAN. The *<interface>* parameter is specified in the format **interface type** *<slot/port>*; available interfaces differ by ASE switch model. Enter **interface ?** for a list of available interfaces. Using the **no** form of this command removes the mirroring session configuration. Enter the command as follows to specify that VLAN 350 is used for mirrored traffic, and the reflector port is GigabitEthernet 1/2:

```
(config)#monitor session 1 destination remote vlan 350 reflector-port
GigabitEthernet 1/2
```

After configuring the mirror destination, the configuring of the mirroring feature is complete. To view sample configurations of the mirroring feature, refer to *Mirroring Configuration Examples Using the CLI on page 64*. To view statistics related to the mirroring configuration, refer to *Troubleshooting on page 82*.

Mirroring Configuration Examples Using the CLI

The example scenarios contained in this section are designed to enhance understanding of mirroring configurations on ASE devices. All configurations provided in this section use the CLI.

NOTE

The configuration parameters entered in these examples are sample configurations only. These applications should be configured in a manner consistent with the needs of your particular network. CLI prompts have been removed from the configuration examples to provide a method of copying and pasting configurations directly from this configuration guide into the CLI. These configurations should not be copied without first making the necessary adjustments to ensure they will function properly in your network.

Local Mirroring Configuration Example (CLI)

The following example configures local mirroring for the traffic on **Port 1**. The mirrored traffic is displayed on **Port 6**.

```
monitor session 1
monitor session 1 source interface GigabitEthernet 1/1 both
monitor session 1 destination interface GigabitEthernet 1/6
```

VLAN-Based Mirroring Example (CLI)

The following example configures VLAN-based mirroring for the traffic on **VLAN 123**. The mirrored traffic is displayed on **Port 6**.

```
monitor session 1
no monitor session 1 source interface *
monitor session 1 source vlan 123
monitor session 1 destination interface GigabitEthernet 1/6
```

RMirror Configuration Example (CLI)

In the following example, remote mirroring is used to mirror a user port (**port 1**) from a PC connected to **ASE Switch 1**. The mirrored traffic is sent to the network administrator with a network analyzer connected to a port (**port 1**) on **ASE Switch 3**. The mirrored traffic is sent by the reflector port (**port 2**) to a VLAN configured for mirroring use (**VLAN 200**), which then sends the mirrored traffic through **ASE Switch 2** from using the mirror VLAN members, **port 3** and **port 4**. The network topology for this example is displayed in *Figure 10* on page 65.

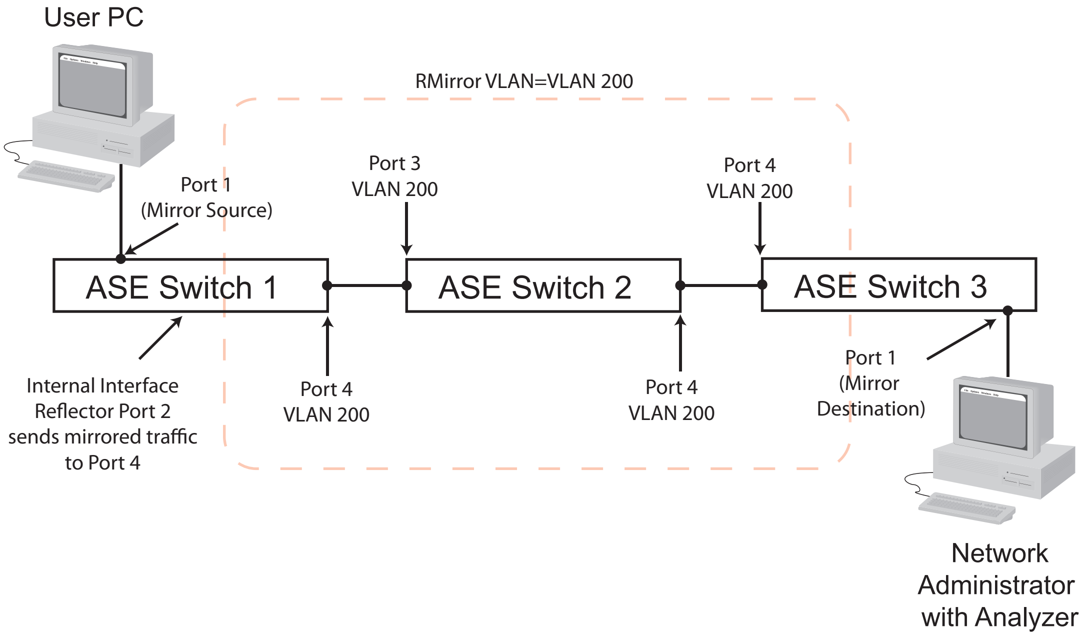


Figure 10. RMirror Network Topology

RMirror Example Configuration Considerations

The following are configuration parameters to consider when studying this example:

- The reflective port (**port 2** on **ASE Switch 1**) must have STP disabled.
- MAC address learning should be disabled for all ports using the RMirror VLAN.
- In a remote mirroring configuration like this, the source and destination devices must be ASE devices. The intermediate device can be an ASE device or a non-ASE device. This example assumes the intermediate device is an ASE device.

Step 1: Configuring the Source Device

The source device for this example (**ASE Switch 1**) should be configured with the following parameters:

```
monitor session 1
vlan 200
!
no mac address-table learning vlan 200
monitor session 1 destination remote vlan 200 reflector-port GigabitEthernet 1/2
monitor session 1 source interface GigabitEthernet 1/1 both
!
interface GigabitEthernet 1/2
  no spanning-tree
!
interface GigabitEthernet 1/4
  switchport mode trunk
  switchport trunk allowed vlan 1,200
!
```

Step Two: Configure the Intermediate Switch/Device

Configure the intermediate device for this example with the following parameters:

- VLAN 200: for mirrored traffic
- Disable source MAC address learning for RMirror VLAN 200

Step Three: Configure the Destination Device

The destination device for this example (**ASE Switch 3**) should be configured with the following parameters:

```
monitor session 1
vlan 200
!
no mac address-table learning vlan 200
monitor session 1 source remote vlan 200
monitor session 1 destination interface GigabitEthernet 1/1
interface GigabitEthernet 1/4
  switchport mode trunk
  switchport trunk allowed vlan 1,200
!
```

13. GVRP Configuration Using the CLI

GVRP configuration on the ASE device includes enabling GVRP globally on the switch, enabling GVRP on a per-port basis, and optionally configuring the timers used by GVRP. To configure GVRP, connect to the ASE CLI and complete these tasks:

- *Enabling GVRP on a Port Using the CLI on page 66*
- *Configuring GVRP Timers and Resources Using the CLI (Optional) on page 67*
- *Enabling GVRP Globally Using the CLI on page 68*

NOTE

All configurations and instructions included in this section are completed on a device returned to the factory default settings.

Enabling GVRP on a Port Using the CLI

To enable GVRP on a port, enter the **[no] gvrp** command from the interface's configuration mode. By default, GVRP is disabled on all ports. Once enabled, use the **no** version of this command to disable GVRP on the port. Enter the command as follows:

```
(config)#interface GigabitEthernet 1/1
(config-if)#gvrp
```

After enabling GVRP on the port, you can optionally choose to configure additional GVRP settings, or continue GVRP configuration by enabling GVRP globally on the ASE switch.

NOTE

GVRP will not function without being enabled on both an interface and globally on the switch.

Configuring GVRP Timers and Resources Using the CLI (Optional)

You can optionally choose to continue GVRP configuration by globally defining the GVRP timers and resources, but this additional configuration is not required. Additional GVRP configuration consists of defining the three GVRP timers (Join-time, Leave-time, and LeaveAll-time) and adjusting the maximum number of VLANs that can be simultaneously controlled by GVRP.

> ⚠ **CAUTION!**
>
> *Caution should be exercised when adjusting GVRP timers. All GVRP timers across any GVRP-enabled devices on the network must be set to the same value. In addition, any adjustments to the maximum number of VLANs simultaneously controlled by GVRP should be made before enabling GVRP on the switch.*

To configure the GVRP timers, enter the **`[no] gvrp time [join-time`** *`<value>`* **`| leave-all-time`** *`<value>`* **`| leave-time`** *`<value>`***`]`** command from the Global Configuration mode prompt. The **`join-time`** *`<value>`* parameter configures the GVRP join-timer, which specifies the interval between declarations of new attributes in GVRP PDUs. Valid *`<value>`* range is
1 to **20** centiseconds. By default, the join-timer is set to **20** centiseconds. The **`leave-all-time`** *`<value>`* parameter configures the GVRP LeaveAll timer, which specifies how long after a VLAN attribute has been GVRP-enabled before it sends a LeaveAll message. Once the LeaveAll message is sent, the LeaveAll timer starts again. Valid *`<value>`* range is **1000** to **5000** centiseconds. By default, the LeaveAll timer is set to **1000** centiseconds. The **`leave-time`** *`<value>`* parameter specifies how long after a leave message is received before a VLAN attribute is deregistered. Valid *`<value>`* range is **60** to **300** centiseconds. By default, the leave timer is set to **60** centiseconds. Using the **`no`** version of this command returns the timers to their default values. To configure GVRP timers, enter the command as follows:

```
(config)#gvrp time join-time 15
```

> **NOTE**
>
> *You can enter the timer parameters in any order using this command. You can also configure all timers with a single command by entering the command as follows:* **`gvrp time join-time 14 leave-all-time 1500 leave-time 70`***.*

To configure the maximum number of VLANs that can be simultaneously supported by GVRP, enter the **`[no] gvrp max-vlans`** *`<number>`* command from the Global Configuration mode prompt. The *`<number>`* parameter is the number of supported VLANs. Valid range is **1** to **4094**, with a default value of **20**. Using the **`no`** form of this command returns the supported number of VLANs to the default value. Enter the command as follows:

```
(config)#gvrp max-vlans 100
```

> **NOTE**
>
> *The maximum number of VLANs should only be adjusted when GVRP is disabled. Disable GVRP globally before changing this value.*

Once GVRP has been enabled on the necessary port(s), and the optional settings have been configured, complete GVRP configuration by enabling GVRP globally on the switch.

Enabling GVRP Globally Using the CLI

To enable GVRP globally on the switch, enter the **[no] gvrp** command from the Global Configuration mode prompt. By default, GVRP is disabled on the switch. Once GVRP has been enabled, using the **no** form of this command disables GVRP. Enter the command as follows:

```
(config)#gvrp
```

Once GVRP has been enabled on the necessary port(s) and globally on the ASE device, GVRP configuration is complete.

14. Spanning Tree Configuration Using the CLI

Spanning tree is configured on the ASE switch by selecting which protocol type you need to configure (STP, RSTP, or MSTP), and configuring the associated priorities, timers, and ports required for the particular protocol, and configuring spanning tree settings on a per-port basis. In addition, MSTP configurations include configuring the CIST, MSTP regions, and MSTIs. To configure spanning tree, connect to the ASE CLI, and complete the following tasks:

- *Configuring Common Spanning Tree Settings Using the CLI on page 68*
- *Configuring Additional MSTP Settings Using the CLI on page 70*
- *Configuring Spanning Tree Ports Using the CLI on page 72*

> **NOTE**
>
> *All configurations and instructions included in this section are completed on a device returned to the factory default settings.*

Configuring Common Spanning Tree Settings Using the CLI

STP, RSTP, and MSTP configuration in the ASE device includes configuring some settings that are common to all versions of spanning tree, including enabling the protocol, specifying bridge priorities, configuring timers and counters, and specifying edge port settings.To configure these common settings, complete the following tasks:

- *Selecting the Spanning Tree Protocol Using the CLI on page 68*
- *Configuring the Bridge Priority Using the CLI on page 69*
- *Configuring Spanning Tree Timers and Counters Using the CLI (Optional) on page 69*
- *Configuring Global Edge Port Settings Using the CLI (Optional) on page 70*

Selecting the Spanning Tree Protocol Using the CLI

To enable and specify the type of spanning tree protocol to use on the ASE device, enter the **[no] spanning-tree mode [mstp | rstp | stp]** command from the Global Configuration mode. Enter the **mstp** parameter to specify that MSTP is being used, the **rstp** parameter to specify that RSTP is being used, or the **stp** parameter to specify that STP is being used. Using the **no** form of this command disables spanning tree on the switch. Enter the command as follows to enable the spanning tree protocol on the switch:

```
(config)#spanning-tree mode mstp
```

NOTE

*If you are using ADTRAN Operating System (AOS) switches in the same network, select **RSTP protocol** to connect into one tree. Further network design is required to integrate MSTP with RSTP.*

Configuring the Bridge Priority Using the CLI

To configure the bridge priority for the spanning tree instance, enter the **[no] spanning-tree mst** *<instance>* **priority** *<priority>* command from the Global Configuration mode prompt. The *<instance>* parameter specifies the bridge instance for which you are configuring priority. Valid *<instance>* range is **0** to **7**, with **0** being the CIST instance, and **1** through **7** being **MSTI1** through **MSTI7**, respectively. The *<priority>* parameter specifies the priority for the bridge instance. This priority is used by the protocol to determine which switch is the root bridge, and the priorities of the other switches connected to the instance. Valid *<priority>* range is **0** to **61440**, in multiples of **4096**. By default, the *<priority>* is set to **16384**. Using the **no** form of this command returns the specified bridge instance to the default value. Enter the command as follows to configure the priority of the CIST (default MSTI for MSTP configurations):

```
(config)#spanning-tree mst 0 priority 4096
```

Configuring Spanning Tree Timers and Counters Using the CLI (Optional)

Spanning tree protocols use several timers and counters to determine when to send BPDU messages, when to change port state, and how long to retain network topology information. These timers include hello, forward delay, and maximum age timers, as well as the maximum hop count and transmit hold count. Enter the commands described below from the Global Configuration mode prompt to configure spanning tree timers and counters.

Enter the **[no] spanning-tree mst forward-time** *<value>* command to specify the time that ports spend in the Listening and Learning states, before moving to the Forwarding state. By default, ports spend **15** seconds in the Listening and Learning states. Valid *<value>* range is **4** to **30** seconds. Using the **no** form of this command returns the forward delay timer to the default setting. To change the forward delay timer value, enter the command as follows:

```
(config)#spanning-tree mst forward-time 20
```

Enter the **[no] spanning-tree mst hello-time** *<value>* command to specify the interval between BPDU messages sent by the bridge. By default, messages are sent every **2** seconds. Valid *<value>* range is **1** to **10** seconds. Using the **no** form of this command returns the hello timer to the default setting. To change the hello timer value, enter the command as follows:

```
(config)#spanning-tree mst hello-time 5
```

Enter the **[no] spanning-tree mst max-age** *<value>* command to specify how long a port saves the configuration information delivered to it in BPDU messages. By default, ports hold onto this information for **20** seconds. Valid *<value>* range is **6** to **40** seconds. The maximum age timer must be configured to be less than or equal to two times the forward delay timer. Using the **no** form of this command returns the maximum age timer to the default value. To change the maximum age timer value, enter the command as follows:

```
(config)#spanning-tree mst max-age 30
```

Enter the **[no] spanning-tree mst max-hops** *<number>* command to specify the number of hops a BPDU message can travel before being discarded and before the port information included in the message is no longer valid. By default, the maximum hop count is set to **20** hops. Valid *<number>* range is **6** to **40** hops. Using the **no** form of this command returns the maximum hop count to the default setting. To change the maximum hop count, enter the command as follows:

```
(config)#spanning-tree mst max-hops 30
```

Enter the **[no] spanning-tree transmit hold-count** *<number>* command to specify the maximum number of transmitted BPDU messages sent by the bridge per second. By default, a maximum of **6** BPDU messages can be sent per second. Valid *<number>* range is **1** to **10**. Using the **no** form of this command returns the maximum number of BPDUs transmitted to the default setting. To change the maximum transmitted number of BPDUs per second, enter the command as follows:

```
(config)#spanning-tree transmit hold-count 3
```

Configuring Global Edge Port Settings Using the CLI (Optional)

Edge ports refer to ports at the edge of the network, that are not connected to other bridges within the spanning tree instance. You can specify how all edge ports within the spanning tree instance behave with regards BPDU transmissions and error recovery by entering the commands described in the following section.

To enable BPDU filtering on all edge ports within the spanning tree instance, enter the **[no] spanning-tree edge bpdu-filter** command from the Global Configuration mode prompt. This setting, when enabled, prevents the port from transmitting or receiving BPDU messages. This feature is disabled by default. Using the **no** form of this command disables BPDU filtering if it has been enabled. To enable BPDU filtering on all edge ports, enter the command as follows:

```
(config)#spanning-tree edge bpdu-filter
```

To enable BPDU guarding on all edge ports within the spanning tree instance, enter the **[no] spanning-tree edge bpdu-guard** command from the Global Configuration mode prompt. This setting, when enabled, prevents the port from receiving BPDU messages. This feature is disabled by default. Using the **no** form of this command disables BPDU guarding if it has been enabled. To enable BPDU guarding on all edge ports, enter the command as follows:

```
(config)#spanning-tree edge bpdu-guard
```

To enable the ports to automatically recover from errors, enter the **[no] spanning-tree recovery interval** *<time>* command from the Global Configuration mode prompt. When enabled, the port will automatically recover from being disabled by an error after an allotted timeout period, specified by the *<time>* parameter. Valid *<time>* range is **30** to **86400** seconds. The error recovery feature is disabled by default. Using the **no** form of this command disables the port's automatic recovery ability if this feature has been enabled. To enable automatic error recovery on all ports within the spanning tree instance, enter the command as follows:

```
(config)#spanning-tree recovery interval 150
```

Once all the spanning tree bridge settings have been configured, continue with spanning tree configuration by specifying the port and MSTI settings as outlined in *Configuring Additional MSTP Settings Using the CLI on page 70*.

Configuring Additional MSTP Settings Using the CLI

Additional MSTP configuration includes specifying MSTP region names and IDs, configuring MSTI VLAN mapping associations, and defining MSTP bridge priorities. To configure the settings specific to MSTP operation on the ASE device, complete these tasks:

- *Configuring MSTP Regions and MSTI Mapping Using the CLI on page 70*
- *Specifying MSTP Bridge Priorities Using the CLI on page 71*

Configuring MSTP Regions and MSTI Mapping Using the CLI

MSTP operates using MSTP regions to organize multiple spanning tree instances within the network. These regions are composed of sets of configured VLANs and their associated MSTIs, are individually named, use the same revision number, and contain a mapping table of which VLANs are associated with which MSTIs. By default, each created VLAN within the MSTP spanning tree configuration is mapped to the CIST. However, you can choose to map particular VLANs to one of seven MSTIs within the single MSTP region. Each MSTP region is configured with a name and revision, and then VLANs are associated with the particular MSTI instance within the region.

NOTE

For MSTP to function correctly, all MSTI mapping settings must be identical on all switches in the network. AOS switches do not support MSTI, as they only support RSTP. See note on page 69.

To configure the MSTP region name and revision number, enter the **[no] spanning-tree mst name** *<name>* **revision** *<number>* command from the Global Configuration mode prompt. MSTP region names and revision numbers are carried in BPDU messages throughout the network and must be identical on all switches within the MSTP region. Configuration names (*<name>* parameter) are specified as ASCII strings with a maximum length of 32 characters, and are case-sensitive. By default, the configuration name for the MSTP region is a text string in hexadecimal format based on the switch's MAC address. Valid *<number>* range for revision numbers is **1** to **65535**, and is set to **0** by default. Using the **no** form of this command returns the MSTP region to the default configuration.

To specify an MSTP region name and revision number, enter the command as follows:

```
(config)#spanning-tree mst name REGION1 revision 10
```

To map VLANs to an MSTI instance, enter the **[no] spanning-tree mst** *<instance>* **vlan** *<vlan ids>* command from the Global Configuration mode prompt. The *<instance>* parameter specifies to which instance you are mapping the VLAN. Valid *<instance>* range is **0** to **7**, with **0** being the CIST instance, and **1** through **7** being **MSTI1** through **MSTI7**, respectively. By default, VLANs are mapped to the CIST. The **vlan** *<vlan ids>* parameter specifies the VLANs you are mapping to the specified instance. The *<vlan ids>* parameter specifies a single VLAN ID, or a range of VLAN IDs separated by a hyphen or comma; valid *<vlan ids>* range is **1** to **4095**. Using the **no** form of this command removes the VLAN from the specified MSTI.

To map a VLAN to an MSTI, enter the command as follows:

```
(config)#spanning-tree mst 1 vlan 3
```

Continue MSTP configuration by specifying the MSTP bridge priorities for each MSTI, including the CIST, as described in the following section.

Specifying MSTP Bridge Priorities Using the CLI

You can specify the priority of each MSTI, including the CIST, for the MSTP region to be used as part of the bridge identifier and to aid spanning tree in determining the root bridge (root bridges have the lowest bridge ID). Each bridge ID is comprised of the bridge priority number concatenated with the MAC address of the device. For example, if a bridge has a priority of **4096**, and the switch's MAC address is **00:A0:C8:00:00:01**, then the bridge ID is **4096.00.A0.C8.00.00.01**. Because a low priority number indicates a higher priority, the lower the bridge ID, the more likely the bridge is selected as the root of the spanning tree.

To configure the bridge priority for the spanning tree instance, enter the **[no] spanning-tree mst** *<instance>* **priority** *<priority>* command from the Global Configuration mode prompt. The *<instance>* parameter specifies the bridge instance for which you are configuring priority. Valid *<instance>* range is **0** to **7**, with **0** being the CIST instance, and **1** through **7** being **MSTI1** through **MSTI7**, respectively. The *<priority>* parameter specifies the priority for the bridge instance. This priority is used by the protocol to determine which switch is the root bridge, and the priorities of the other switches connected to the instance. Valid *<priority>* range is **0** to **61440**, in multiples of **4096**. By default, the *<priority>* is set to **16384**. Using the **no** form of this command returns the specified bridge instance to the default value.

Enter the command as follows to configure the priority of the CIST (default MSTI for MSTP configurations):

```
(config)#spanning-tree mst 0 priority 4096
```

Configuring Spanning Tree Ports Using the CLI

Spanning tree settings, on a per-port basis, are configured either by configuring all ports as a group (aggregated), or by configuring each port individually. Port configuration includes ensuring spanning tree is enabled, specifying the port's path cost and priority, defining the edge port properties of the port (if applicable), configuring the BDPU processing behavior for the port(s), and specifying the link type between ports. To configure the port settings for specific spanning tree operation on the ASE device, complete these tasks:

- *Configuring Ports as an Aggregated Group or Individually on page 72*
- *Configuring Ports for Spanning Tree Using the CLI on page 72*

Configuring Ports as an Aggregated Group or Individually

Using your network topology and needs, determine if you will be configuring all ports associated with the spanning tree as an aggregated group, or each port individually. The commands used for spanning tree port configuration are the same, but they are entered from two different command modes.

If you are configuring the ports as an aggregated group, enter the **[no] spanning-tree aggregation** command from the Global Configuration mode prompt. Using this command enters the STP Aggregated Group configuration mode, which contains the same spanning tree configuration commands as an individual port interface. Using the **no** form of this command removes the aggregated group from the STP configuration. Enter the command as follows to enter the STP Aggregated Group configuration mode:

```
(config)#spanning-tree aggregation
(config-stp-aggr)#
```

If you are configuring each port individually, enter the **interface** *<interface>* command from the Global Configuration mode prompt to enter the interface's configuration mode. The *<interface>* parameter is specified in the format **interface type** *<slot/port>*; available interfaces differ by ASE switch model. Enter **interface ?** for a list of available interfaces. Enter the command as follows:

```
(config)#interface GigabitEthernet 1/1
(config-if)#
```

Configuring Ports for Spanning Tree Using the CLI

The following commands describe the available spanning tree configuration commands for an individual port or an aggregated group of ports.

Enable spanning tree on the port, or aggregated group, by entering the **[no] spanning-tree** command from the appropriate configuration mode. Using the **no** form of this command disables spanning tree on the interface or aggregated group. Enter the command as follows:

```
(config-if)#spanning-tree
```

To specify the path cost associated with the port(s) or aggregated group of ports, enter the **[no] spanning-tree mst** *<instance>* **cost [***<number>* **| auto]** command from the appropriate configuration mode. The path cost is used by MSTP to determine which port to put in a forwarding state should a loop occur in the network. Lower costs values can be assigned interfaces that should be selected by spanning tree first, and higher costs can be assigned to interfaces that should be selected last. If all ports have the same path cost, spanning tree selects the interface with the lowest number should a loop occur. The *<instance>* parameter specifies the spanning tree instance for which you are configuring the port path cost. Valid *<instance>* range is **0** to **7**, with **0** being the CIST instance, and **1** through **7** being **MSTI1** through **MSTI7**, respectively. The *<number>* parameter allows you to enter a specific cost for the port's path. Valid path cost range is **1** to **200000000**. The **auto** parameter specifies that the spanning tree protocol automatically determines the cost of the path from the port to the root bridge; this is the default setting. Using the **no** form of this command returns the path cost to the default setting. Enter the command as follows:

```
(config-if)#spanning-tree mst 2 cost 3500
```

To specify the priority for the port(s) or aggregated group of ports, enter the **[no] spanning-tree mst** *<instance>* **port-priority** *<number>* command from the appropriate configuration mode. The port's priority is also used by spanning tree to determine which port to put in a forwarding state should a loop occur in the network. Higher priority is assigned to ports with a lower numerical priority value. Valid priority *<number>* range is **0** to **240**, in multiples of **16**; with a default value of **128**. Using the **no** form of this command returns the priority to the default setting. Enter the command as follows:

```
(config-if)#spanning tree mst 2 port-priority 32
```

To specify whether spanning tree automatically determines if the port(s), or aggregated group of ports, are edge ports, enter the **[no] spanning-tree auto-edge** command from the appropriate configuration mode. By default, this feature is enabled. Using the **no** form of this command disables the feature. To disable automatic edge port detection, enter the command as follows:

```
(config-if)#no spanning-tree auto-edge
```

To specify whether the port(s), or aggregated group of ports, are edge ports, regardless of any spanning tree detection, enter the **[no] spanning-tree edge** command from the appropriate configuration mode. This feature is disabled by default. By default, all ports are configured to let spanning tree automatically determine if they are edge ports. Using the **no** form of this command returns edge port detection to the default setting. To specify that the port is always an edge port, enter the command as follows:

```
(config-if)#spanning-tree edge
```

To specify that the port's, or aggregated port group's, role should be restricted, enter the **[no] spanning-tree restricted-role** command from the appropriate configuration mode. By default, this feature is disabled. When enabled, it specifies that the port is not selected as the root port for the CIST (or any MSTI), even if it has the lowest cost or higher priority, although it does not keep the port from being selected as an alternative once the root port has been determined. Enabling this feature can be beneficial by preventing external bridges from influencing the active topology of the spanning tree instance; however, when enabled this feature can also cause a lack of spanning tree connectivity. Using the **no** form of this command disables this feature if it has been enabled. To enable restricted mode for the port, enter the command as follows:

```
(config-if)#spanning-tree restricted-role
```

To restrict TCN BPDU messages on the port, or aggregated group of ports, enter the **[no] spanning-tree restricted-tcn** command from the appropriate configuration mode. By default, this feature is disabled. When enabled, the port does not propagate TCNs to other ports in the spanning tree instance. Enabling this feature can prevent a device outside the core region of the network from causing address flushing in the core region; however, when enabled it can also cause temporary loss of connectivity if any modifications to the network topology result in perpetuating incorrect topology information from the port. Using the **no** form of this command disables the feature. To restrict TCN broadcasts on the port, enter the command as follows:

```
(config-if)#spanning-tree restricted-tcn
```

To enable BPDU guarding on the port(s), or aggregated group of ports, enter the **[no] spanning-tree bpdu-guard** command from the appropriate configuration mode. This setting, when enabled, prevents the port from receiving BPDU messages, and causes the port to shut down if it does receive valid BPDU messages. This feature is disabled by default. Using the **no** form of this command disables this feature if it has been enabled. To enable BPDU guarding on the port, enter the command as follows:

```
(config-if)#spanning-tree bpdu-guard
```

To specify the link type used on the port(s), or aggregated group of ports, enter the **[no] spanning-tree link-type [auto | point-to-point | shared]** command from the appropriate configuration mode. The link type determines how quickly the spanning tree protocol will be able to disseminate network topology information between ports. By default, the switch automatically determines the link type based on the port's duplex mode (full-duplex ports are treated as point-to-point connected ports, and half-duplex ports are treated as shared connection ports); this is the **auto** parameter setting. To override the default (**auto**) setting for the port, enter either **point-to-point** (specifying a point-to-point connection), or **shared** (specifying a shared connection). Using the **no** form of this command returns the link type to the default setting. To change the link type of the port, enter the command as follows:

```
(config-if)#spanning-tree link-type point-to-point
```

After completing the port configurations, the spanning tree configuration is complete. To view statistics associated with spanning tree configuration and operation, refer to *Troubleshooting on page 82*.

15. Layer 2 Services Configuration Command Summary

The following tables summarize the commands used in conjunction with Layer 2 protocols and services configurations on the ASE device.

Table 3. LAG and LACP Configuration Commands

Prompt	Command	Description
(config-if)#	**[no] aggregation group** *<group id>* **mode on**	Creates the LAG group. Valid *<group>* range is **1** to **5**. Using the **no** form of the command removes the LAG group from the switch's configuration.
(config-if)#	**[no] no aggregation group** *<group id>* **mode [active | passive]**	Creates the LACP group. Valid *<group>* range is **1** to **5**. The **active** parameter specifies the group always transmits LACP frames, and the **passive** parameter specifies the group transmits LACP frames only when it receives them first. Using the **no** form of the command removes the LAG group from the switch's configuration.
(config)#	**[no] interface llag** *<group id>*	Enters the LLAG interface for LACP group configuration. Valid *<group id>* range depends on the ASE switch mode. For an 8-port ASE switch, the range is **1** to **5**. Using the **no** form of the command removes the LLAG interface from the switch's configuration.
(config-llag)#	**[no] lacp failover [non-revertive | revertive]**	Specifies whether the group is in revertive mode or not. Revertive mode indicates the group can switch links if a better link becomes available. Using the **no** form of the command returns the group's behavior to the default setting (**revertive**).
(config-llag)#	**[no] lacp max-bundle** *<value>*	Specifies the maximum number of bundles supported in the LACP group. Valid *<value>* range is determined by the number of groups available on the ASE device. Using the **no** form of the command returns the maximum number of supported bundles to the default setting.
(config)#	**[no] lacp system-priority** *<value>*	Specifies the priority of the ASE device in the LACP connected network. Valid *<value>* range is **1** to **65535**, with a default value of **32768**. Using the **no** form of the command returns the system priority to the default setting.

Table 3. LAG and LACP Configuration Commands (Continued)

Prompt	Command	Description
(config-if)#	**[no] lacp port-priority** *<value>*	Specifies the priority of the port within the LACP group. Valid *<value>* range is **1** to **65535**, with a default value of **32768**. Using the **no** form of the command returns the port priority to the default setting.
(config-if)#	**[no] lacp timeout [fast | slow]**	Specifies the interval between LACP message transmissions on the port. By default, messages are sent every second (**fast** setting). The **slow** setting sends messages every **30** seconds. Using the **no** form of the command returns the transmission interval to the default setting.
(config)#	**[no] aggregation mode [dmac | ip | port | smac]**	Specifies the forwarding mode of the LAG and LACP groups. Traffic destinations can be determined by destination MAC address (**dmac**), IP address (**ip**), TCP and UDP ports (**port**), and source MAC address (**smac**). Any combination of parameters can be used. By default, the groups use **ip**, **port**, and **smac** parameters. Using the **no** form of the command returns the forwarding mode to the default value.

Table 4. MAC Address Table Configuration Commands

Prompt	Command	Description
(config)#	**[no] mac address-table aging-time** *<value>*	Specifies how long the MAC address table keeps an address entry. Valid *<value>* range is **10** to **1000000** seconds; default aging time is **300** seconds Using the **no** form of the command returns the aging time to the default value.
(config)#	**[no] mac address-table static** *<mac address>* **vlan** *<vlan id>* **[interface** *<interface>***]**	Statically adds a MAC address to the MAC address table. The *<mac address>* parameter is the MAC address to add to the MAC address table. MAC addresses should be expressed in the following format **xx:xx:xx:xx:xx:xx** (for example, **00:A0:C8:00:00:01**). The *<vlan id>* parameter is the VLAN to which you are associating the MAC address. Valid *<vlan id>* range is **1** to **4095**. The optional **interface** *<interface>* parameter specifies the port to which you are associating the MAC address. The *<interface>* parameter is specified in the format **interface type** *<slot/port>*; available interfaces differ by ASE switch model. Enter **interface ?** for a list of available interfaces. Using the **no** form of the command removes address from the address table.
(config-if)#	**[no] mac address-table learning [secure]**	Enables the automatic learning of source MAC addresses for the port. This feature is enabled by default. The optional **secure** parameter specifies that secure MAC addresses are learned and added to the address table. Using the **no** form of the command disables dynamic learning of MAC addresses on the port.
(config)#	**[no] mac address-table learning vlan** *<vlan ids>*	Enables the automatic learning of source MAC addresses for VLANs. This feature is enabled by default. The <vlan ids> parameter specifies a single VLAN ID, or a range of VLAN IDs separated by a hyphen or comma. Valid range is **1** to **4095**. Using the **no** form of the command disables dynamic learning of MAC addresses on the VLAN.

Table 5. VLAN Configuration Commands

Prompt	Command	Description
`(config-if)#`	**`[no] switchport mode [access | hybrid | trunk]`**	Specifies whether the port is an access port (**`access`** parameter), hybrid port (**`hybrid`** parameter), or trunk port (**`trunk`** parameter). By default, all ports are in **`access`** mode. Using the **`no`** form of the command returns the port to the default setting.
`(config-if)#`	**`[no] switchport access vlan`** *`<id>`*	Associates an access port with a VLAN. Valid *`<id>`* range is **1** to **4095**; by default all ports are associated with the default VLAN (**VLAN 1**). Using the **`no`** form of the command returns the port to the default setting.
`(config-if)#`	**`[no] switchport hybrid native vlan`** *`<id>`*	Associates a hybrid port with a VLAN. Valid *`<id>`* range is **1** to **4095**; by default all ports are associated with the default VLAN (**VLAN 1**). Using the **`no`** form of the command returns the port to the default setting.
`(config-if)#`	**`[no] switchport trunk native vlan`** *`<id>`*	Associates a trunk port with a VLAN. Valid *`<id>`* range is **1** to **4095**; by default all ports are associated with the default VLAN (**VLAN 1**). Using the **`no`** form of the command returns the port to the default setting.
`(config)#`	**`[no] switchport forbidden [add`** *`<vlan ids>`* **`| remove`** *`<vlan ids>`***`]`**	Configures the forbidden VLANs for an access port. The **`add`** *`<vlan ids>`* parameter specifies the VLANs to forbid on the port; valid range is **1** to **4095**, and can be entered as a single VLAN ID, a list of VLAN IDs separated by a comma, or a range separated by a hyphen. The **`remove`** *`<vlan ids>`* parameter removes VLANs from the port's forbidden list; valid range is **1** to **4095**, and can be entered as a single VLAN ID, a list of VLAN IDs separated by a comma, or a range separated by a hyphen. Using the **`no`** form of the command removes the list of forbidden VLANs from the port's configuration.
`(config-if)#`	**`[no] switchport hybrid port-type [c-port | s-custom-port | s-port | unaware]`**	Configures a hybrid port to classify incoming frames to a particular VLAN using the VLAN tag of ingress traffic. The **`c-port`** parameter specifies frames with a VLAN tag TPID of 0x8100 are classified to the VLAN embedded in the tag. The **`s-custom-port`** parameter specifies that frames with a VALN tag TPID of 0x8100 (or a value equal to the Ethertype configured for S-Custom-Ports) are classified to the VLAN ID embedded in the tag. The **`s-port`** parameter specifies that frames with a VLAN tag TPID of 0x8100 or 0x88A8 are classified to the VLAN ID embedded in the tag. The **`unaware`** parameter specifies that all frames are classified to the VLAN associated with the port (this is the default behavior). Using the **`no`** form of the command returns the port to the default setting.
`(config)#`	**`[no] vlan ethertype s-custom-port`** *`<type>`*	Specifies the S-Custom-Port setting for hybrid ports using S-Custom-Port classification. Valid *`<type>`* range is **0x0600** to **0xffff**, and is set to **0x88A8** by default. Using the **`no`** form of this command returns the S-Custom-Port setting to the default value.
`(config-if)#`	**`[no] switchport hybrid ingress-filtering`**	Enables ingress filtering on a hybrid port. This feature is disabled by default on hybrid ports. Using the **`no`** form of this command disables ingress filtering on the port.
`(config-if)#`	**`[no] switchport hybrid acceptable-frame-type [all | tagged | untagged]`**	Specifies the accepted ingress frame type for a hybrid port, whether all frame types (**`all`**), tagged frames only (**`tagged`**), or untagged frames only (**`untagged`**). By default, the port accepts **`all`** frame types. Using the **`no`** form of this command returns the port to the default setting.

Table 5. VLAN Configuration Commands (Continued)

Prompt	Command	Description
(config-if)#	**[no] switchport hybrid egress-tag [all | none]**	Specifies the egress tagging behavior of the hybrid port. The **all** parameter specifies all egress traffic is tagged, and the **none** parameter specifies no egress traffic is tagged. Using the **no** form of this command returns the port to the default setting (only traffic that is not associated with the port VLAN is tagged).
(config-if)#	**[no] switchport trunk vlan tag native**	Specifies that a trunk port tags all egress traffic. Using the **no** form of this command returns the port to the default setting (only traffic not associated with the port VLAN is tagged).
(config-if)#	**[no] switchport [hybrid | trunk] allowed vlan [***<vlan ids>* **| add** *<vlan ids>* **| all | except** *<vlan ids>* **| none | remove** *<vlan ids>***]**	Specifies the VLANs of which a trunk (**trunk**) or hybrid (**hybrid**) port is allowed to become a member. The *<vlan ids>* parameter specifies the VLANs in which the port is allowed to transmit traffic. You can enter a single VLAN ID, several IDs separated by commas, or a range of IDs separated by a hyphen; valid range is **1** to **4095**. The **add** *<vlan ids>* parameter specifies VLAN IDs to add to the allowed VLAN list. The **all** parameter specifies that all configured VLANs are allowed. The **except** *<vlan ids>* parameter specifies that all configured VLANs are allowed except for the specified VLANs. The **none** parameter specifies that no VLANs are allowed for the port. The **remove** *<vlan ids>* parameter specifies that the listed VLANs are removed from the allowed VLAN list. Using the **no** form of this command returns the allowed VLAN list to the default setting (all ports are allowed to become members of all available VLANs).
(config-if)#	**[no] switchport forbidden [add** *<vlan ids>* **| remove** *<vlan ids>***]**	Specifies the forbidden VLANs for the port. The **add** *<vlan ids>* parameter specifies VLAN IDs to add to the forbidden VLAN list. The **remove** *<vlan ids>* parameter specifies that the listed VLANs are removed from the forbidden VLAN list. You can enter a single VLAN ID, several IDs separated by commas, or a range of IDs separated by a hyphen; valid range is **1** to **4095**.
(config)#	**[no] svl fid** *<fid>* **vlan** *<vlan ids>*	Enables SVL and associates VLANs with a specific FID. Valid *<fid>* range is **1** to **4095**. Valid *<vlan ids>* range is **1** to **4095**, and VLAN IDs can be entered individually, in a list separated by commas, or in a range separated by a hyphen. Using the **no** form of this command disables SVL.

Table 6. Mirroring Configuration Commands

Prompt	Command	Description
`(config)#`	**`[no] monitor session`** *`<session id>`*	Creates a mirroring session on the ASE device. Valid *`<session id>`* range depends on the ASE switch model. For an 8-port ASE switch, the range is **1** to **5**. By default, no mirroring sessions are configured. Using the **`no`** form of the command removes the mirroring session from the device's configuration.
`(config)#`	**`[no] monitor session`** *`<session id>`* **`source interface`** *`<interface>`* **`[both | rx | tx]`**	Configures a port as the local mirroring source. The *`<session id>`* parameter specifies the mirroring session you are configuring. Valid *`<session id>`* range depends on the ASE switch model. For an 8-port ASE switch, the range is **1** to **5**. The **`interface`** *`<interface>`* parameter specifies the interface to use as the source. The *`<interface>`* parameter is specified in the format **`interface type`** *`<slot/port>`*; available interfaces differ by ASE switch model. Enter **`interface ?`** for a list of available interfaces. You can configure the session to monitor received traffic only (**`rx`**), transmitted traffic only (**`tx`**), or all traffic (**`both`**). Using the **`no`** form of the command removes the mirroring session configuration.
`(config)#`	**`[no] monitor session`** *`<session id>`* **`vlan`** *`<vlan id>`*	Specifies a VLAN as a source for VLAN-based mirroring. The *`<session id>`* parameter specifies the mirroring session you are configuring. Valid *`<session id>`* range depends on the ASE switch model. For an 8-port ASE switch, the range is **1** to **5**. The **`vlan`** *`<vlan id>`* parameter specifies the VLAN from which to mirror traffic; valid *`<vlan id>`* range is **1** to **4095**. Using the **`no`** removes the mirroring session configuration.
`(config)#`	**`[no] monitor session`** *`<session id>`* **`source remote vlan`** *`<vlan id>`*	Configures a source remote mirror VLAN. The *`<session id>`* parameter specifies the mirroring session you are configuring. Valid *`<session id>`* range depends on the ASE switch model. For an 8-port ASE switch, the range is **1** to **5**. The **`vlan`** *`<vlan id>`* parameter specifies the VLAN from which to mirror traffic; valid *`<vlan id>`* range is **1** to **4095**. By default, the VLAN used as a source for remote mirroring traffic is **200**. Using the **`no`** form of the command removes the mirroring session configuration.
`(config)#`	**`[no] monitor session`** *`<session id>`* **`destination interface`** *`<interface>`*	Configures a port as the local mirroring destination. The *`<session id>`* parameter specifies the mirroring session you are configuring. Valid *`<session id>`* range depends on the ASE switch model. For an 8-port ASE switch, the range is **1** to **5**. The **`interface`** *`<interface>`* parameter specifies the interface to use as the destination. The *`<interface>`* parameter is specified in the format **`interface type`** *`<slot/port>`*; available interfaces differ by ASE switch model. Enter **`interface ?`** for a list of available interfaces. Using the **`no`** form of the command removes the mirroring session configuration.
`(config)#`	**`[no] monitor session`** *`<session id>`* **`destination remote vlan`** *`<vlan id>`* **`reflector-port`** *`<interface>`*	Configures a reflector port for sending mirrored traffic to the VLAN for remote mirroring configurations. The *`<session id>`* parameter specifies the mirroring session you are configuring. Valid *`<session id>`* range depends on the ASE switch model. For an 8-port ASE switch, the range is **1** to **5**. The **`vlan`** *`<vlan id>`* parameter specifies the VLAN that is used for mirrored traffic; valid *`<vlan id>`* range is **1** to **4095**. The **`reflector-port`** *`<interface>`* parameter specifies the interface to use as the reflector port. The *`<interface>`* parameter is specified in the format **`interface type`** *`<slot/port>`*; available interfaces differ by ASE switch model. Enter **`interface ?`** for a list of available interfaces. Using the **`no`** form of the command removes the mirroring session configuration.

Table 7. GVRP Configuration Commands

Prompt	Command	Description
(config-if)#	**[no] gvrp**	Enables GVRP on the port. Using the **no** form of the command disables the GVRP feature on the port.
(config)#	**[no] gvrp time [join-time** *<value>* **| leave-all-time** *<value>* **| leave-time** *<value>***]**	Configures the GVRP timers. Caution should be used when adjusting these timers; they must be the same on all GVRP-enabled devices in the network for GVRP to function properly. The **join-time** *<value>* parameter configures the join timer; valid *<value>* range **1** to **20** centiseconds; default value is **20** centiseconds. The **leave-all-time** *<value>* parameter configures the LeaveAll timer; valid *<value>* range **1000** to **5000** centiseconds; default value is **1000** centiseconds. The **leave-time** *<value>* parameter configures the leave timer; valid *<value>* range **60** to **300** centiseconds; default value is **60** centiseconds. Using the **no** form of the command returns the timer(s) to the default value.
(config)#	**[no] gvrp max-vlans** *<number>*	Specifies the maximum number of VLANs that can be simultaneously supported by GVRP. Valid *<number>* range is **1** to **4094**, with a default value of **20**. Using the **no** form of the command returns the maximum number of supported VLANs to the default setting.
(config)#	**[no] gvrp**	Enable GVRP globally on the ASE device. Using the **no** form of the command disables GVRP on the switch.

Table 8. Spanning Tree Configuration Commands

Prompt	Command	Description
(config)#	**[no] spanning-tree mode [mstp | rstp | stp]**	Enables spanning tree on the ASE device, and specifies whether the protocol used is STP (**stp**), RSTP (**rstp**), or MSTP (**mstp**). Using the **no** form of the command disables spanning tree on the switch.
(config)#	**[no] spanning-tree mst** *<instance>* **priority** *<priority>*	Configures the bridge priority for the spanning tree instance. The **mst** *<instance>* parameter specifies the bridge instance for which you are configuring priority; valid range is **0** to **7**, with **0** being the CIST and **1** to **7** being **MSTI1** through **MSTI7**, respectively. The *<priority>* parameter specifies the bridge priority; valid range is **0** to **61440**, in multiples of **4096**, with a default value of **16384**. Using the **no** form of the command returns the bridge priority to the default value.
(config)#	**[no] spanning-tree mst forward-time** *<value>*	Specifies the time that ports spend in the Listening and Learning states before moving to the Forwarding state. Valid *<value>* range is **4** to **30** seconds, and is set to **15** seconds by default. Using the **no** form of the command returns the timer to the default value.
(config)#	**[no] spanning-tree mst hello-time** *<value>*	Specifies the interval between transmitted BPDU messages. Valid *<value>* range is **1** to **10** seconds, and is set to **2** seconds by default. Using the **no** form of the command returns the timer to the default value.
(config)#	**[no] spanning-tree mst max-age** *<value>*	Specifies how long a port saves configuration information delivered in BPDU messages. Valid *<value>* range is **6** to **40** seconds, and is set to **20** seconds by default. The maximum age timer must be configured to be less than or equal to two times the forward delay timer. Using the **no** form of the command returns the timer to the default value.

Table 8. Spanning Tree Configuration Commands (Continued)

Prompt	Command	Description
`(config)#`	**`[no] spanning-tree mst max-age`** *`<number>`*	Specifies the number of hops a BPDU message can travel before being discarded. Valid *`<number>`* range is **6** to **40** hops, and is set to **20** hops by default. Using the **`no`** form of the command returns the maximum hop count to the default value.
`(config)#`	**`[no] spanning-tree transmit hold-count`** *`<number>`*	Specifies the maximum number of transmitted BPDU messages per second. Valid *`<number>`* range is **1** to **10**, and is set to **6** by default. Using the **`no`** form of the command returns the maximum number of transmitted BPDUs to the default value.
`(config)#`	**`[no] spanning-tree edge bpdu-filter`**	Enables BPDU filtering on all edge ports within the spanning tree instance. Using the **`no`** form of the command disables BPDU filtering.
`(config)#`	**`[no] spanning-tree bpdu-guard`**	Enables BPDU guarding on all edge ports within the spanning tree instance. Using the **`no`** form of the command disables BPDU guarding.
`(config)#`	**`[no] spanning-tree recovery interval`** *`<time>`*	Configures ports to automatically recover from errors. The **`interval`** *`<time>`* parameter specifies the delay before the port recovers; valid *`<time>`* range is **30** to **86400** seconds. This feature is disabled by default. Using the **`no`** form of the command disables automatic error recovery if it is has been enabled.
`(config)#`	**`[no] spanning-tree name`** *`<name>`* **`revision`** *`<number>`*	Configures the MSTP region name and revision number. The *`<name>`* parameter is specified as an ASCII string with a maximum length of 32 characters (by default it is specified as a hexadecimal number based on the switch's MAC address). Valid *`<number>`* range for revision numbers is **1** to **65535** with a default setting of **0**. Using the **`no`** form of the command returns the MSTP region to the default configuration.
`(config)#`	**`[no] spanning-tree mst`** *`<instance>`* **`vlan`** *`<vlan ids>`*	Maps the specified VLANs to the MSTI instance. The **`mst`** *`<instance>`* parameter specifies the MSTI to which you are mapping the VLANs; valid range is **0** to **7**, with **0** being the CIST and **1** to **7** being **MSTI1** through **MSTI7**, respectively. The *`<vlan ids>`* parameter specifies the VLANs to add to the MSTI; valid range is **1** to **4095**. VLAN IDs can be entered individually, in a list separated by commas, or in a range separated by a hyphen. Using the **`no`** form of the command removes the VLANs from the MSTI configuration.
`(config)#`	**`[no] spanning-tree aggregation`**	Enters the STP Aggregated Group configuration mode, in which spanning tree configuration can be completed for aggregated groups. Using the **`no`** form of the command removes the aggregated group from the STP configuration.
`(config)#`	**`interface`** *`<interface>`*	Enters the interface's configuration mode, in which spanning tree configuration can be completed for individual ports. The *`<interface>`* parameter is specified in the format **`interface type`** *`<slot/port>`*; available interfaces differ by ASE switch model. Enter **`interface ?`** for a list of available interfaces.

`(config-stp-aggr)#`
OR
`(config-if)#`
	`[no] spanning-tree`	Enables spanning tree on the port or the aggregated port group. Using the **`no`** form of the command disables spanning tree on the port or group.

Table 8. Spanning Tree Configuration Commands (Continued)

Prompt	Command	Description
(config-stp-aggr)# OR (config-if)#	**[no] spanning-tree mst** *<instance>* **cost** [*<number>* | **auto**]	Specifies the path cost associated with the port or aggregated port group. The **mst** *<instance>* parameter specifies the spanning tree instance for which you are configuring the port path cost; valid range is **0** to **7**, with **0** being the CIST and **1** to **7** being **MSTI1** through **MSTI7**, respectively. The *<number>* parameter specifies a specific cost for the path; valid range is **1** to **200000000**. The **auto** parameter specifies the path cost is automatically determined by spanning tree; this is the default setting. Using the **no** form of the command returns the path cost to the **auto** setting.
(config-stp-aggr)# OR (config-if)#	**[no] spanning-tree mst** *<instance>* **port-priority** *<number>*	Specifies the priority for the port or aggregated port group. Higher priority is assigned to ports with a lower numerical priority value. The **mst** *<instance>* parameter specifies the spanning tree instance for which you are configuring the port priority; valid range is **0** to **7**, with **0** being the CIST and **1** to **7** being **MSTI1** through **MSTI7**, respectively. The *<number>* parameter specifies a specific priority for the port; valid range is **0** to **240**, in multiples of **16**, and is set to **128** by default. Using the **no** form of the command returns the port priority to the default setting.
(config-stp-aggr)# OR (config-if)#	**[no] spanning-tree auto-edge**	Specifies that spanning tree automatically determines if the port or aggregated port group are edge ports. This feature is enabled by default. Using the **no** form of the command disables this feature.
(config-stp-aggr)# OR (config-if)#	**[no] spanning-tree edge**	Specifies that the port or aggregated port group are edge ports, regardless of any spanning tree detection. This feature is disabled by default. Using the **no** form of the command disables this feature once it has been enabled.
(config-stp-aggr)# OR (config-if)#	**[no] spanning-tree restricted-role**	Specifies that the port or aggregated port group operate in a restricted role. This feature is disabled by default. Using the **no** form of the command disables this feature once it has been enabled.
(config-stp-aggr)# OR (config-if)#	**[no] spanning-tree restricted-tcn**	Specifies that TCN BPDU messages are restricted on the port or aggregated port group. This feature is disabled by default. Using the **no** form of the command disables this feature once it has been enabled.
(config-stp-aggr)# OR (config-if)#	**[no] spanning-tree bpdu-guard**	Enables BPDU guarding on the port or aggregated port group. This feature is disabled by default. Using the **no** form of the command disables this feature once it has been enabled.
(config-stp-aggr)# OR (config-if)#	**[no] spanning-tree link-type [auto | point-to-point | shared]**	Specifies the link type used on the port or aggregated port group. By default, the switch automatically determines the port's link type based on the port's duplex mode (**auto** setting). The **point-to-point** parameter specifies the link is a point-to-point connection, and the **shared** parameter specifies the link is a shared connection. Using the **no** form of the command returns the port's link type to the default setting.

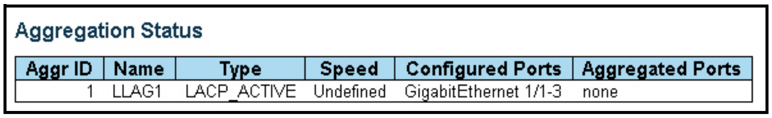
16. Troubleshooting

You can view several types of Layer 2 feature statistics on the ASE device that can aid in troubleshooting Layer 2 protocols and operations. Layer 2 statistics can be used to aid in debug procedures and other troubleshooting measures. Most Layer 2 feature statistics can be viewed using either the GUI or the CLI; however, Port Mirroring information can only be viewed using the CLI, and there are no compiled statistics to view for the GVRP feature.

Viewing LAG and LACP Statistics Using the GUI

Several LAG and LACP statistics are available to view using the ASE GUI. These statistics include details of active aggregation groups, LACP groups, LACP system status, LACP internal port status, and general LACP statistics.

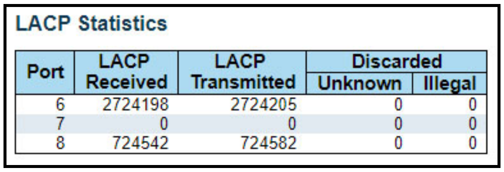
To view LAG group statistics, navigate to the **Monitor** tab, and select **Aggregation** > **Status**. The configured LAG groups and their types are displayed.



Aggregation Status

Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports
1	LLAG1	LACP_ACTIVE	Undefined	GigabitEthernet 1/1-3	none

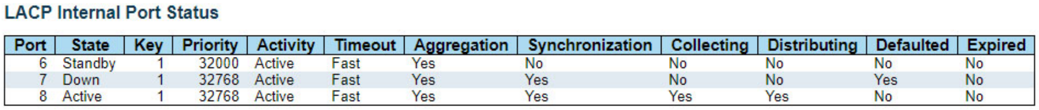
To view local LACP system statistics, as well as those for any configured LACP partners, navigate to the **Monitor** tab, and select **Aggregation** > **LACP** > **System Status**. The LACP system priority and addresses for the local system, and any configured partner systems, are displayed.



LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
6	2724198	2724205	0	0
7	0	0	0	0
8	724542	724582	0	0

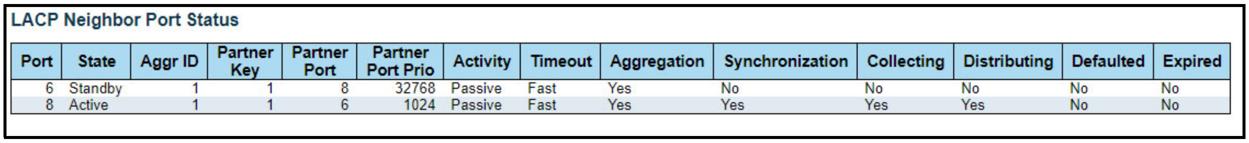
To view the LACP configuration for ports on the local system, navigate to the **Monitor** tab, and select **Aggregation** > **LACP** > **Internal Status**. The LACP settings for ports configured as part of the LACP group are displayed.



LACP Internal Port Status

Port	State	Key	Priority	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
6	Standby	1	32000	Active	Fast	Yes	No	No	No	No	No
7	Down	1	32768	Active	Fast	Yes	Yes	No	No	Yes	No
8	Active	1	32768	Active	Fast	Yes	Yes	Yes	Yes	No	No

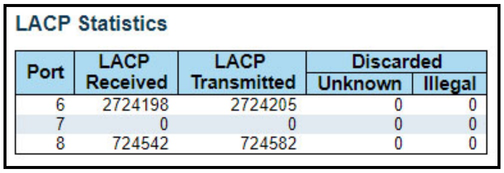
To view the LACP status of ports on the LACP neighbor, navigate to the **Monitor** tab, and select **Aggregation** > **LACP** > **Neighbor Status**. The LACP settings for ports configured as part of the neighbor LACP group are displayed.



LACP Neighbor Port Status

Port	State	Aggr ID	Partner Key	Partner Port	Partner Port Prio	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
6	Standby	1	1	8	32768	Passive	Fast	Yes	No	No	No	No	No
8	Active	1	1	6	1024	Passive	Fast	Yes	Yes	Yes	Yes	No	No

To view LACP statistics for all ports configured for LACP, navigate to the **Monitor** tab, and select **Aggregation** > **LACP** > **Neighbor Status**.

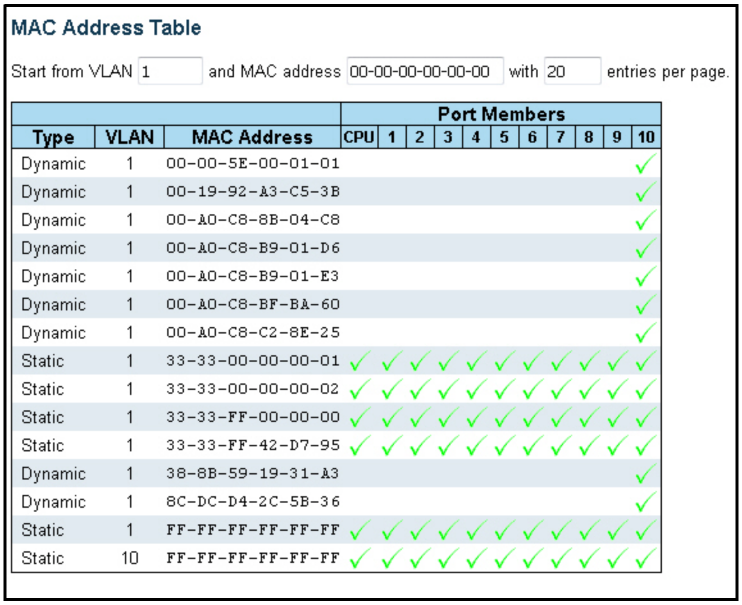


LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
6	2724198	2724205	0	0
7	0	0	0	0
8	724542	724582	0	0

Viewing MAC Address Table Statistics Using the GUI

To view statistics regarding MAC address table entries, navigate to the Monitor tab and select MAC Address Table. In the MAC Address Table display menu, each MAC address entry, along with is associated ports, is displayed.



MAC Address Table

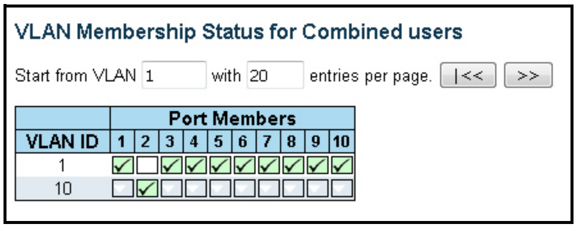
Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

Type	VLAN	MAC Address	Port Members										
			CPU	1	2	3	4	5	6	7	8	9	10
Dynamic	1	00-00-5E-00-01-01											✓
Dynamic	1	00-19-92-A3-C5-3B											✓
Dynamic	1	00-A0-C8-8B-04-C8											✓
Dynamic	1	00-A0-C8-B9-01-D6											✓
Dynamic	1	00-A0-C8-B9-01-E3											✓
Dynamic	1	00-A0-C8-BF-BA-60											✓
Dynamic	1	00-A0-C8-C2-8E-25											✓
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-00-00-00	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-42-D7-95	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic	1	38-8B-59-19-31-A3											✓
Dynamic	1	8C-DC-D4-2C-5B-36											✓
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	10	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Viewing VLAN Configurations and Statistics Using the GUI

VLAN statistics displayed using the GUI include displaying the combined status of all users in their VLAN memberships and port configurations.

To view the status of VLAN memberships for all users combined, navigate to the **Monitor** tab, and select **VLANs** > **Membership**. The VLAN status for all users is displayed as shown below.

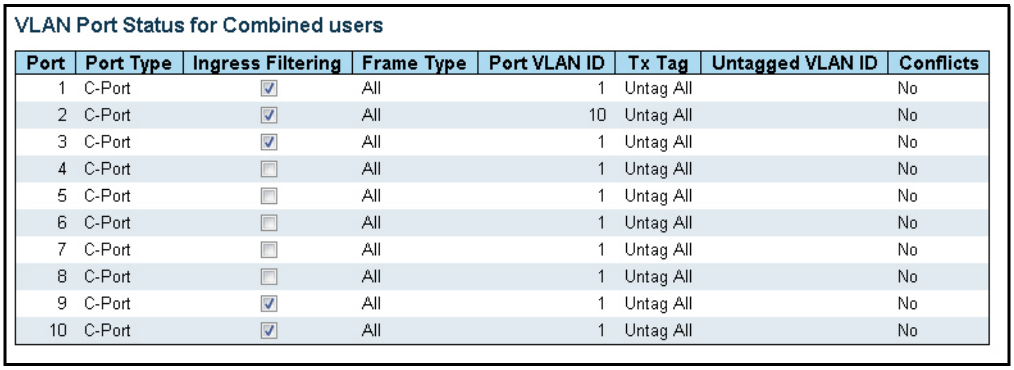


VLAN Membership Status for Combined users

Start from VLAN 1 with 20 entries per page.

VLAN ID	Port Members									
	1	2	3	4	5	6	7	8	9	10
1	☑	□	☑	☑	☑	☑	☑	☑	☑	☑
10	□	☑	□	□	□	□	□	□	□	□

To view the VLAN port configuration for all users, navigate to the **Monitor** tab, and select **VLANs** > **Ports**. The VLAN port configurations for all users combined is displayed as shown below.



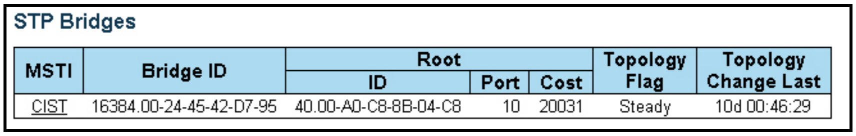
VLAN Port Status for Combined users

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag All		No
2	C-Port	☑	All	10	Untag All		No
3	C-Port	☑	All	1	Untag All		No
4	C-Port	☐	All	1	Untag All		No
5	C-Port	☐	All	1	Untag All		No
6	C-Port	☐	All	1	Untag All		No
7	C-Port	☐	All	1	Untag All		No
8	C-Port	☐	All	1	Untag All		No
9	C-Port	☑	All	1	Untag All		No
10	C-Port	☑	All	1	Untag All		No

Viewing Spanning Tree Configurations Using the GUI

You can view spanning tree statistics for configured bridges, ports, and traffic patterns using the GUI.

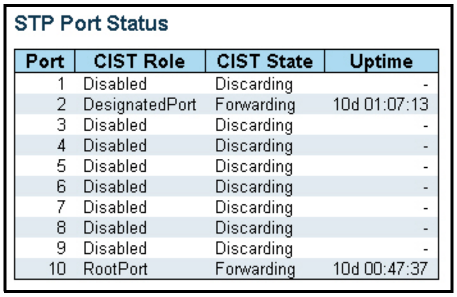
To view the configuration information for spanning tree bridges, navigate to the **Monitor** tab, and select **Spanning Tree** > **Bridge Status**. The configured MSTI, bridge ID, and root ID and port for the configured spanning tree bridges are displayed as shown below.



STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	16384.00-24-45-42-D7-95	40.00-A0-C8-8B-04-C8	10	20031	Steady	10d 00:46:29

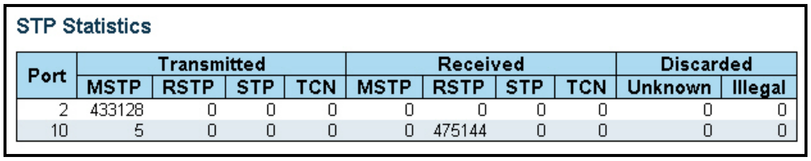
To view configuration information for spanning tree ports, navigate to the **Monitor** tab, and select **Spanning Tree** > **Port Status**. The configured CIST role, and state for each port configured with spanning tree, as shown below.



STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	DesignatedPort	Forwarding	10d 01:07:13
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	RootPort	Forwarding	10d 00:47:37

To view traffic statistics for spanning tree configurations, navigate to the **Monitor** tab, and select **Spanning Tree** > **Port Statistics**. Traffic statistics for each port using spanning tree are displayed as shown below.



STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
2	433128	0	0	0	0	0	0	0	0	0
10	5	0	0	0	0	475144	0	0	0	0

Viewing LAG and LACP Statistics Using the CLI

Several LAG and LACP statistics are available to view in the ASE CLI by using various **show** commands. These statistics include details of active aggregation groups, LACP groups, LACP system status, LACP internal port status, and general LACP statistics.

Enter the **show aggregation** command from the Enable mode prompt to display LACP aggregation group statistics. Enter the command as follows:

```
#show aggregation
Aggr ID  Name    Type           Speed     Configured Ports Aggregated Ports
-------  ------  -----------    --------  ---------------- ----------------
1        LLAG1   LACP_ACTIVE    Undefined GigabitEthernet 1/1-3 none
```

Enter the **show lacp [internal | neighbor | statistics | system-id] [details]** command from the Enable mode prompt to display LACP configurations and statistics. The **internal** parameter specifies that information about internal LACP configuration is displayed, the **neighbor** parameter specifies that LACP neighbor information is displayed, the **statistics** parameter specifies the LACP statistics are displayed, and the **system-id** parameter specifies that LACP system information is displayed. The optional **details** parameter specifies that detailed information is displayed. To display internal LACP configuration information, enter the command as follows:

```
#show lacp internal
Port        State     Key   Priority
----------  --------  ----  --------
Gi 1/1      Down      1     32002
Gi 1/2      Down      1     32002
Gi 1/3      Down      1     32002
```

Viewing MAC Address Table Statistics Using the CLI

Enter the **show mac address-table [address** *<mac address>* **| aging-time | conf | count [interface** *<interface>* **| vlan** *<id>***] | interface | learning [interface** *<interface>* **| vlan** *<id>* **| static | vlan** *<id>***]** command from the Enable mode prompt to display various MAC address table statistics. Using the optional **address** *<mac address>* parameter displays information about a specific MAC address. MAC addresses should be expressed in the following format **xx:xx:xx:xx:xx:xx** (for example, **00:A0:C8:00:00:01**). Using the optional **aging-time** parameter displays the configured aging time for table entries. Using the optional **conf** parameter specifies that MAC addresses added statically by users are displayed. Using the optional **count** parameter specifies that the total number of MAC addresses in the table is displayed. This number can be displayed on a per-interface basis (using the **interface** *<interface>* parameter) or on a per-vlan basis (using the **vlan** *<id>* parameter). The *<interface>* parameter is specified in the format **interface type** *<slot/port>*; available interfaces differ by ASE switch model. Enter **interface ?** for a list of available interfaces. Valid *<vlan id>* range is **1** to **4095**. Using the optional **interface** parameter specifies that MAC addresses are displayed on a per-interface basis. Using the optional **learning** parameter specifies that the address learning behavior for the table is displayed. This number can be displayed on a per-interface basis (using the **interface** *<interface>* parameter) or on a per-vlan basis (using the **vlan** *<id>* parameter). Using the optional **static** parameter specifies that all statically added MAC addresses are displayed. Using the optional **vlan** *<id>* parameter specifies that MAC addresses in the specified VLAN are displayed.

To display all MAC address statistics, enter the command as follows:

```
#show mac address-table
Type    VID  MAC Address       Ports
Dynamic 1    00:00:5e:00:01:01 GigabitEthernet 1/10
Dynamic 1    00:19:92:a3:c5:3b GigabitEthernet 1/10
Dynamic 1    00:a0:c8:8b:04:c8 GigabitEthernet 1/10
Dynamic 1    00:a0:c8:b9:01:d6 GigabitEthernet 1/10
Dynamic 1    00:a0:c8:b9:01:e3 GigabitEthernet 1/10
Dynamic 1    00:a0:c8:bf:ba:60 GigabitEthernet 1/10
Dynamic 1    00:a0:c8:c2:8e:25 GigabitEthernet 1/10
Static  1    33:33:00:00:00:01 GigabitEthernet 1/1-10 CPU
Static  1    33:33:00:00:00:02 GigabitEthernet 1/1-10 CPU
Static  1    33:33:ff:00:00:00 GigabitEthernet 1/1-10 CPU
Static  1    33:33:ff:42:d7:95 GigabitEthernet 1/1-10 CPU
Dynamic 1    38:8b:59:19:31:a3 GigabitEthernet 1/10
Static  1    ff:ff:ff:ff:ff:ff GigabitEthernet 1/1-10 CPU
Static  10   ff:ff:ff:ff:ff:ff GigabitEthernet 1/1-10 CPU
```

Viewing VLAN Information Using the CLI

There are several **show** commands that can be used to display various VLAN statistics and configuration information. All **show** commands are entered from the Enable mode prompt.

Use the **show vlan all [brief | id** *<vlan ids>* **| name** *<name>*] command to display the status of all configured VLANs on the ASE switch. Using the optional **brief** parameter limits the output to summary information. The **id** *<vlan ids>* parameter displays the VLAN status information by VLAN ID. The *<vlan ids>* parameter specifies a single VLAN ID, or a range of VLAN IDs separated by a hyphen or comma. Valid *<vlan ids>* range is **1** to **4095**. The optional **name** *<name>* parameter displays the VLAN status information by VLAN name. The following is sample output from this command:

```
#show vlan all
VLAN  Name                              Interfaces
----  --------------------------------  ----------
1     default                           Gi 1/1,3-10
10    VLAN0010                          Gi 1/2
```

Use the **show vlan brief [all]** command to display a brief summary of configured VLAN status. The optional **all** parameter specifies that information for all configured VLANs is shown. If the **all** parameter is not included, only access VLAN information is displayed. The following is sample output from this command:

```
#show vlan brief all
VLAN  Name                              Interfaces
----  --------------------------------  ----------
1     default                           Gi 1/1,3-10
10    VLAN0010                          Gi 1/2
```

Use the **show vlan id** *<vlan ids>* **[all]** command to display VLAN information by VLAN ID. The *<vlan ids>* parameter specifies a single VLAN ID, or a range of VLAN IDs separated by a hyphen or comma. Valid *<vlan ids>* range is **1** to **4095**. The optional **all** parameter specifies that information for all configured VLANs is shown. If the **all** parameter is not included, only access VLAN information is displayed. Enter the command as follows:

```
#show vlan id 5 all
```

Use the **show vlan ip-subnet [***<ipv4 address>***]** command to display VLAN information for all IPv4 subnet addresses. The optional *<ipv4 address>* parameter specifies that VLAN information for a specific IPv4 address is displayed. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). Enter the command as follows:

```
#show vlan ip-subnet
```

Use the **show vlan mac address [***<mac address>***]** command to display VLAN information by MAC address. The optional *<mac address>* parameter specifies that information for a single unicast MAC address is displayed. MAC addresses are entered in the format **HH:HH:HH:HH:HH:HH**. Enter the command as follows:

```
#show vlan mac address
```

Use the **show vlan name** *<name>* command to display information a single, named VLAN. Enter the command as follows:

```
#show vlan name MYVLAN1
```

Use the **show vlan protocol [eth2 | llc | snap]** command to display VLAN information by protocol. The **eth2** parameter specifies that VLAN information for the ETH2 protocol is displayed. The **llc** parameter specifies that VLAN information for the Link Layer Control (LLC) protocol is displayed. The **snap** parameter specifies that VLAN information for the Subnetwork Access Protocol (SNAP) is displayed. Enter the command as follows:

```
#show vlan protocol llc
```

Use the **show vlan status [admin | all | combined | conflicts | erps | gvrp | interface** *<interface>* **| mep | mstp | mvr | nas | rmirror | vcl | voice-vlan] [interface** *<interface>***]** command to display information for VLANs used by specific features on the ASE device. The **admin** parameter specifies that information for VLANs created by the administrator is displayed. The **all** parameter specifies that information for all user VLANs are displayed. The **combined** parameter specifies that status information for all VLANs is displayed. The **conflicts** parameter specifies that VLANs with conflicts are displayed. The **erps** parameter specifies that VLANs used by Ethernet Ring Protection Switching (ERPS) are displayed. The **gvrp** parameter specifies that VLANs used by GVRP are displayed. The **mep** parameter specifies that VLANs used by the maintenance endpoint (MEP) are displayed. The **mstp** parameter specifies that VLANs used by MSTP are displayed. The **mvr** parameter specifies that VLANs used by Multiple VLAN Registration (MVR) are displayed. The **nas** parameter specifies that VLANs used by network attached storage (NAS) are displayed. The **rmirror** parameter specifies that VLANs used by remote mirroring are displayed. The **vcl** parameter specifies that VLANs used by VCL are displayed. The **voice-vlan** parameter specifies that VLANs used by voice VLANs are displayed. In addition, you can display VLAN status for a single interface using the **interface** *<interface>* parameter, or you can optionally limit the output of one of the other parameters to single interface using the **interface** *<interface>* parameter. The *<interface>* parameter is specified in the format **interface type** *<slot/port>*; available interfaces differ by ASE switch model. Enter **interface ?** for a list of available interfaces.

The following is sample output from this command:

```
#show vlan status interface gigabitethernet 1/1
GigabitEthernet 1/1 :
---------------------
VLAN User PortType  PVID  Frame Type Ing Filter  Tx Tag  U  VID  Conflicts
--------- --------  -----  ---------  ---------  ------- --  ----
--------Combined  C-Port    1     All        Enabled     None    1        No
Admin     C-Port    1     All        Enabled     None    1

NAS                                                                No
GVRP                                                               No
MVR                                                                No
Voice VLAN                                                         No
MSTP                                                               No
ERPS                                                               No
MEP                                                                No
VCL                                                                No
RMirror                                                            No
```

Viewing Port Mirroring Statistics Using the CLI

To display port mirroring statistics using the CLI, enter the **show monitor session [***<session id>* **| all | remote]** command from the Enable mode prompt. The *<session id>* parameter specifies that information for a specific mirror session is displayed. The **all** parameter specifies that information for all configured mirroring sessions are displayed. The **remote** parameter specifies that information for all remote mirroring sessions are displayed.

To display mirroring information for a specific mirroring session, enter the command as follows:

```
#show monitor session 1
Session 1
---------
Mode                          : Disabled
Type                          : Mirror
Source VLAN(s)                :
CPU Port                      :
```

Viewing Spanning Tree Information Using the CLI

To view spanning tree configuration and statistics, enter the **show spanning-tree [active | detailed [interface** *<interface>***] | interface** *<interface>* **| mst** *<instance>* **[configuration] | summary]** command from the Enable mode prompt. Using the **active** parameter specifies that spanning tree for interfaces on which spanning tree is active are displayed. The **detailed** parameter specifies that detailed spanning tree information is displayed; this option can be limited to a single interface using the optional **interface** *<interface>* parameter. The **interface** *<interface>* parameter displays spanning tree information for a single interface. The *<interface>* parameter is specified in the format **interface type** *<slot/port>*; available interfaces differ by ASE switch model. Enter **interface ?** for a list of available interfaces. The **mst** *<instance>* parameter specifies that spanning tree information for a specific spanning tree instance is displayed. Valid *<instance>* range is **0** to **7**; this parameter can also display the VLAN mapping for the instance using the optional **configuration** parameter. The **summary** parameter specifies that the spanning tree information displayed is summarize.

Enter the command as follows:

```
#show spanning-tree active
```