

Switch Configuration for the ASA Services Module

This chapter describes how to configure the Catalyst 6500 series or Cisco 7600 series switch for use with the ASASM. Before completing the procedures in this chapter, configure the basic properties of your switch, including assigning VLANs to switch ports, according to the documentation that came with your switch.

This chapter includes the following sections:

- Information About the Switch, page 2-1
- Guidelines and Limitations, page 2-5
- Verifying the Module Installation, page 2-6
- Assigning VLANs to the ASA Services Module, page 2-7
- Using the MSFC as a Directly Connected Router (SVIs), page 2-10
- Configuring the Switch for ASA Failover, page 2-11
- Resetting the ASA Services Module, page 2-12
- Monitoring the ASA Services Module, page 2-12
- Feature History for the Switch for Use with the ASA Services Module, page 2-15

Information About the Switch

- Supported Switch Hardware and Software, page 2-1
- Backplane Connection, page 2-2
- ASA and IOS Feature Interaction, page 2-2

Supported Switch Hardware and Software

You can install the ASASM in the Catalyst 6500 series and Cisco 7600 series switches. The switch includes a switch (the supervisor engine) as well as a router (the MSFC).

The switch supports Cisco IOS software on both the switch supervisor engine and the integrated MSFC router.

Note The Catalyst operating system software is not supported.

The ASASM runs its own operating system.

Note Because the ASASM runs its own operating system, upgrading the Cisco IOS software does not affect the operation of the ASASM.

To view a matrix of hardware and software compatibility for the ASASM and Cisco IOS versions, see the *Cisco ASA Series Hardware and Software Compatibility*:

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

Backplane Connection

The connection between the ASASM and the switch is a single 20-GB interface.

ASA and IOS Feature Interaction

Some ASASM features interact with Cisco IOS features. The following features involve Cisco IOS software:

- Virtual Switching System (VSS)—No ASASM configuration is required.
- Autostate—The supervisor informs the ASASM when the last interface on a given VLAN has gone down, which assists in determining whether or not a failover switch is required.
- Clearing entries in the supervisor MAC address table on a failover switch—No ASASM configuration is required.
- Version compatibility—The ASASM will be automatically powered down if the supervisor/ASASM version compatibility matrix check fails.

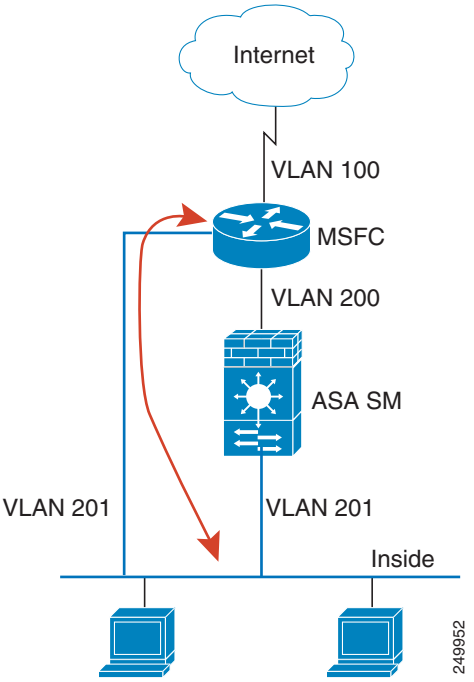
Information About SVIs

If you want to use the MSFC as a directly connected router (for example, as the default gateway connected to the ASASM outside interface), then add an ASASM VLAN interface to the MSFC as a switched virtual interface (SVI).

For security reasons, by default, you can configure one SVI between the MSFC and the ASASM; you can enable multiple SVIs, but be sure you do not misconfigure your network.

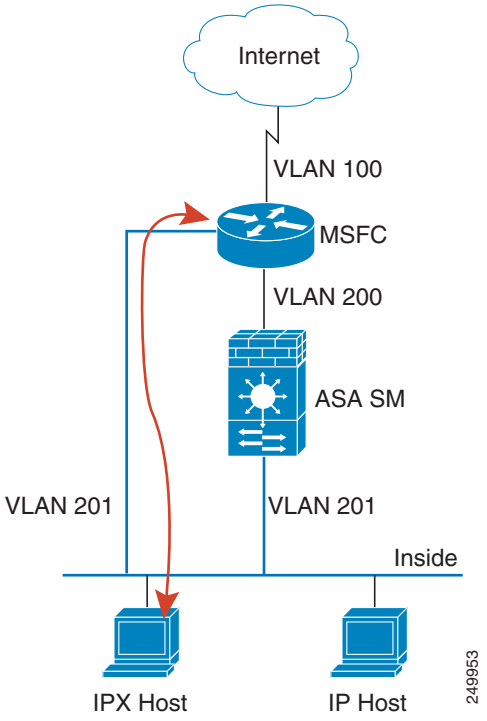
For example, with multiple SVIs, you could accidentally allow traffic to pass around the ASASM by assigning both the inside and outside VLANs to the MSFC. (See Figure 2-1.)

Figure 2-1 Multiple SVI Misconfiguration



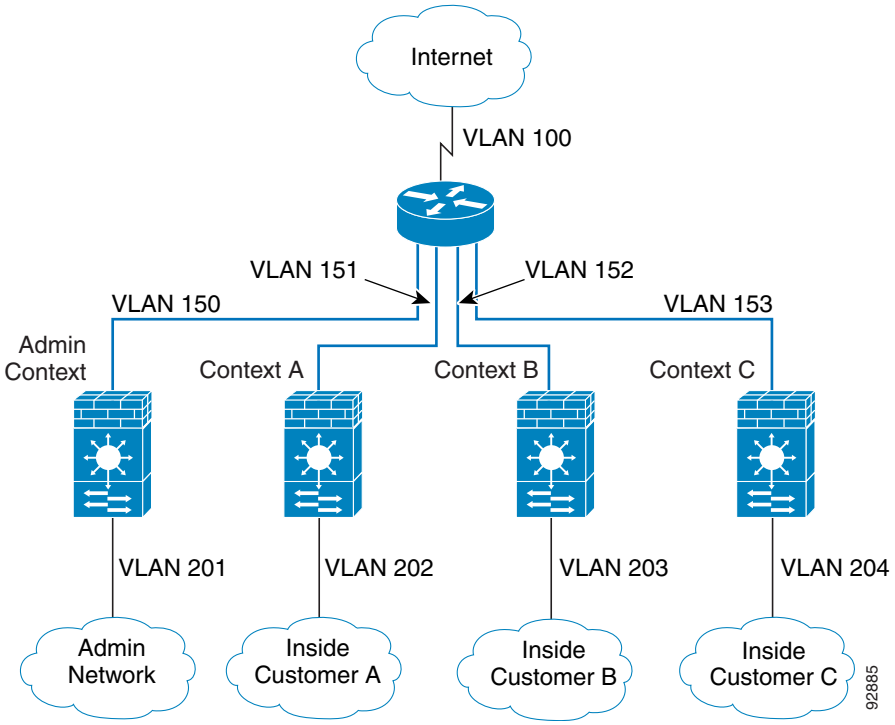
You might need to bypass the ASASM in some network scenarios. Figure 2-2 shows an IPX host on the same Ethernet segment as IP hosts. Because the ASASM in routed firewall mode only handles IP traffic and drops other protocol traffic like IPX (transparent firewall mode can optionally allow non-IP traffic), you might want to bypass the ASASM for IPX traffic. Make sure that you configure the MSFC with an access list that allows only IPX traffic to pass on VLAN 201.

Figure 2-2 Multiple SVIs for IPX



For transparent firewalls in multiple context mode, you need to use multiple SVIs because each context requires a unique VLAN on its outside interface (see Figure 2-3). You might also choose to use multiple SVIs in routed mode so that you do not have to share a single VLAN for the outside interface.

Figure 2-3 Multiple SVIs in Multiple Context Mode



Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

VLAN Guidelines and Limitations

- Use VLAN IDs 2 to 1001.
- You can use private VLANs with the ASASM. Assign the primary VLAN to the ASASM; the ASASM automatically handles secondary VLAN traffic. There is no configuration required on the ASASM for this feature; see the switch configuration guide for more information. See also the example in Assigning VLANs to the ASA Services Module, page 2-7.
- You cannot use reserved VLANs.
- You cannot use VLAN 1.
- If you are using ASASM failover within the same switch chassis, do not assign the VLAN(s) that you are reserving for failover and stateful communications to a switch port. However, if you are using failover between chassis, you must include the VLANs in the trunk port between the chassis.
- If you do not add the VLANs to the switch before you assign them to the ASASM, the VLANs are stored in the supervisor engine database and are sent to the ASASM as soon as they are added to the switch.

- You can configure a VLAN in the ASASM configuration before it has been assigned on the switch. Note that when the switch sends the VLAN to the ASASM, the VLAN defaults to be administratively up on the ASASM, regardless of whether the you shut them down in the ASASM configuration. You need to shut them down again in this case.

SPAN Reflector Guidelines

In Cisco IOS software Version 12.2SXJ1 and earlier, for each ASASM in a switch, the SPAN reflector feature is enabled. This feature allows multicast traffic (and other traffic that requires a central rewrite engine) to be switched when coming from the ASASM. The SPAN reflector feature uses one SPAN session. To disable this feature, enter the following command:

```
Router(config)# no monitor session servicemodule
```

Verifying the Module Installation

To verify that the switch acknowledges the ASASM and has brought it online, enter the following command.

Detailed Steps

Command	Purpose
show module [**switch** {**1** |**2**}] [*mod-num* | **all**]	Displays module information. For a switch in a VSS, enter the **switch** keyword.
Example: `Router# show module 1`	Ensure that the Status column shows "Ok" for the ASASM.

Examples

The following is sample output from the **show module** command:

```
Router# show module
Mod Ports Card Type                                  Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
 2    3  ASA Service Module                     WS-SVC-ASA-SM1     SAD143502E8
 4    3  ASA Service Module                     WS-SVC-ASA-SM1     SAD135101Z9
 5    5  Supervisor Engine 720 10GE (Active)    VS-S720-10G        SAL12426KB1
 6   16  CEF720 16 port 10GE                    WS-X6716-10GE      SAL1442WZD1

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
 2  0022.bdd4.016f to 0022.bdd4.017e   0.201 12.2(2010080 12.2(2010121 Ok
 4  0022.bdd3.f64e to 0022.bdd3.f655   0.109 12.2(2010080 12.2(2010121 PwrDown
 5  0019.e8bb.7b0c to 0019.e8bb.7b13   2.0   8.5(2)       12.2(2010121 Ok
 6  f866.f220.5760 to f866.f220.576f   1.0   12.2(18r)S1  12.2(2010121 Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ----------- ------- -------
2/0 ASA Application Processor   SVC-APP-PROC-1     SAD1436015D  0.202  Other
4/0 ASA Application Processor   SVC-APP-INT-1      SAD141002AK  0.106  PwrDown
 5  Policy Feature Card 3       VS-F6K-PFC3C       SAL12437BM2  1.0    Ok
 5  MSFC3 Daughterboard         VS-F6K-MSFC3       SAL12426DE3  1.0    Ok
 6  Distributed Forwarding Card WS-F6700-DFC3C     SAL1443XRDC  1.4    Ok
```

```
Base PID:
Mod  Model            Serial No.
---- ------------      ----------
 2 WS-SVC-APP-HW-1    SAD143502E8
 4 TRIFECTA           SAD135101Z9

Mod  Online Diag Status
---- -------------------
 2  Pass
2/0 Not Applicable
 4  Not Applicable
4/0 Not Applicable
 5  Pass
 6  Pass
```

Assigning VLANs to the ASA Services Module

This section describes how to assign VLANs to the ASASM. The ASASM does not include any external physical interfaces. Instead, it uses VLAN interfaces. Assigning VLANs to the ASASM is similar to assigning a VLAN to a switch port; the ASASM includes an internal interface to the Switch Fabric Module (if present) or the shared bus.

Prerequisites

See the switch documentation for information about adding VLANs to the switch and assigning them to switch ports.

Guidelines

- You can assign up to 16 firewall VLAN groups to each ASASM. (You can create more than 16 VLAN groups in Cisco IOS software, but only 16 can be assigned per ASASM.) For example, you can assign all the VLANs to one group; or you can create an inside group and an outside group; or you can create a group for each customer.
- There is no limit on the number of VLANs per group, but the ASASM can only use VLANs up to the ASASM system limit (see the ASASM licensing documentation for more information).
- You cannot assign the same VLAN to multiple firewall groups.
- You can assign a single firewall group to multiple ASASMs. VLANs that you want to assign to multiple ASASMs, for example, can reside in a separate group from VLANs that are unique to each ASASM.
- See VLAN Guidelines and Limitations, page 2-5.

Detailed Steps

	Command	Purpose
Step 1	**firewall vlan-group** *firewall_group vlan_range* **Example:** `Router(config)# firewall vlan-group 1 55-57`	Assigns VLANs to a firewall group. The *firewall_group* argument is an integer. The *vlan_range* argument can be one or more VLANs (2 to 1001) identified in one of the following ways: • A single number (*n*) • A range (*n-x*) Separate numbers or ranges by commas, as shown in the following example: **5,7-10,13,45-100**
Step 2	**firewall** [**switch** {**1** |**2**}] **module** *slot* **vlan-group** *firewall_group* **Example:** `Router(config)# firewall module 5 vlan-group 1`	Assigns the firewall groups to the ASASM. For a switch in a VSS, enter the **switch** argument. To view the slots where the ASASM is installed, enter the **show module** command. The *firewall_group* argument is one or more group numbers, which can be one of the following: • A single number (*n*) • A range (*n-x*) Separate numbers or ranges by commas, as shown in the following example: **5,7-10**

Examples

The following example shows how to create three firewall VLAN groups: one for each ASASM, and one that includes VLANs assigned to both ASASMs:

```
Router(config)# firewall vlan-group 10 55-57
Router(config)# firewall vlan-group 11 70-85
Router(config)# firewall vlan-group 12 100
Router(config)# firewall module 5 vlan-group 10,12
Router(config)# firewall module 8 vlan-group 11,12
```

The following example shows how to configure private VLANs on the switch by assigning the primary VLAN to the ASASM:

Step 1 Add the primary VLAN 200 to a firewall VLAN group, and assign the group to the ASASM:

```
Router(config)# firewall vlan-group 10 200
Router(config)# firewall module 5 vlan-group 10
```

Step 2 Designate VLAN 200 as the primary VLAN:

```
Router(config)# vlan 200
Router(config-vlan)# private-vlan primary
```

Step 3 Designate only one secondary isolated VLAN. Designate one or more secondary community VLANs.

```
Router(config)# vlan 501
Router(config-vlan)# private-vlan isolated
Router(config)# vlan 502
Router(config-vlan)# private-vlan community
Router(config)# vlan 503
Router(config-vlan)# private-vlan community
```

Step 4 Associate the secondary VLANs to the primary VLAN:

```
Router(config)# vlan 200
Router(config-vlan)# private-vlan association 501-503
```

Step 5 Classify the port mode. The mode of interface f1/0/1 is host. The mode of interface f1/0/2 is promiscuous.

```
Router(config)# interface f1/0/1
Router(config-ifc)# switchport mode private-vlan host
Router(config)# interface f1/0/2
Router(config-ifc)# switchport mode private-vlan promiscuous
```

Step 6 Assign VLAN membership to the host port. Interface f1/0/1 is a member of primary VLAN 200 and secondary isolated VLAN 501.

```
Router(config)# interface f1/0/1
Router(config-ifc)# switchport private-vlan host-association 200 501
```

Step 7 Assign VLAN membership to the promiscuous interface. Interface f1/0/2 is a member of primary VLAN 200. Secondary VLANs 501-503 are mapped to the primary VLAN.

```
Router(config)# interface f1/0/2
Router(config-ifc)# switchport private-vlan mapping 200 501-503
```

Step 8 If inter-VLAN routing is desired, configure a primary SVI and then map the secondary VLANs to the primary.

```
Router(config)# interface vlan 200
Router(config-ifc)# private-vlan mapping 501-503
```

Using the MSFC as a Directly Connected Router (SVIs)

If you want to use the MSFC as a directly connected router (for example, as the default gateway connected to the ASASM outside interface), then add an ASASM VLAN interface to the MSFC as a switched virtual interface (SVI). See Information About SVIs, page 2-3.

Restrictions

For security reasons, by default, you can configure one SVI between the MSFC and the ASASM; you can enable multiple SVIs, but be sure you do not misconfigure your network.

Detailed Steps

	Command	Purpose
Step 1	(Optional) **firewall multiple-vlan-interfaces** **Example:** `Router(config)# firewall multiple-vlan-interfaces`	Allows you to add more than one SVI to the ASASM.
Step 2	**interface vlan** *vlan_number* **Example:** `Router(config)# interface vlan 55`	Adds a VLAN interface to the MSFC.
Step 3	**ip address** *address mask* **Example:** `Router(config-if)# ip address 10.1.1.1 255.255.255.0`	Sets the IP address for this interface on the MSFC.
Step 4	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface.

Examples

The following example shows a typical configuration with multiple SVIs:

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall module 8 vlan-group 50-51
Router(config)# firewall multiple-vlan-interfaces
Router(config)# interface vlan 55
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# interface vlan 56
Router(config-if)# ip address 10.1.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```

Configuring the Switch for ASA Failover

This section includes the following topics:

- Assigning VLANs to the Secondary ASA Services Module, page 2-11
- Adding a Trunk Between a Primary Switch and Secondary Switch, page 2-11
- Ensuring Compatibility with Transparent Firewall Mode, page 2-11
- Enabling Autostate Messaging for Rapid Link Failure Detection, page 2-11

Assigning VLANs to the Secondary ASA Services Module

Because both units require the same access to the inside and outside networks, you must assign the same VLANs to both ASASMs on the switch(es). See Assigning VLANs to the Secondary ASA Services Module, page 2-11.

Adding a Trunk Between a Primary Switch and Secondary Switch

If you are using inter-switch failover, then you should configure an 802.1Q VLAN trunk between the two switches to carry the failover and state links. The trunk should have QoS enabled so that failover VLAN packets, which have a CoS value of 5 (higher priority), are treated with higher priority in these ports.

To configure the EtherChannel and trunk, see the documentation for your switch.

Ensuring Compatibility with Transparent Firewall Mode

To avoid loops when you use failover in transparent mode, use switch software that supports BPDU forwarding. Do not enable LoopGuard globally on the switch if the ASASM is in transparent mode. LoopGuard is automatically applied to the internal EtherChannel between the switch and the ASASM, so after a failover and a failback, LoopGuard causes the secondary unit to be disconnected because the EtherChannel goes into the err-disable state.

Enabling Autostate Messaging for Rapid Link Failure Detection

The supervisor engine can send autostate messages to the ASASM about the status of physical interfaces associated with ASASM VLANs. For example, when all physical interfaces associated with a VLAN go down, the autostate message tells the ASASM that the VLAN is down. This information lets the ASASM declare the VLAN as down, bypassing the interface monitoring tests normally required for determining which side suffered a link failure. Autostate messaging provides a dramatic improvement in the time the ASASM takes to detect a link failure (a few milliseconds as compared to up to 45 seconds without autostate support).

The switch supervisor sends an autostate message to the ASASM when:

- The last interface belonging to a VLAN goes down.
- The first interface belonging to a VLAN comes up.

Detailed Steps

Command	Purpose
firewall autostate **Example:** `Router(config)# firewall autostate`	Enables autostate messaging in Cisco IOS software. Autostate messaging is disabled by default.

Resetting the ASA Services Module

This section describes how to reset the ASASM. You might need to reset the ASASM if you cannot reach it through the CLI or an external Telnet session. The reset process might take several minutes.

Detailed Steps

Command	Purpose
hw-module [**switch** {**1** |**2**}] **module** *slot* **reset** **Example:** `Router# hw-module module 9 reset`	Resets the ASASM. For a switch in a VSS, enter the **switch** argument. The *slot* argument indicates the slot number in which the module is installed. To view the slots where the ASASM is installed, enter the **show module** command. **Note** To reset the ASASM when you are already logged in to it. enter either the **reload** or **reboot** command.

Examples

The following is sample output from the **hw-module module reset** command:

```
Router# hw-module module 9 reset

Proceed with reload of module? [confirm] y
% reset issued for module 9

Router#
00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...
```

Monitoring the ASA Services Module

To monitor the ASA, enter one of the following commands:

Command	Purpose
show firewall module [*mod-num*] **state**	Verifies the state of the ASA.
show firewall module [*mod-num*] **traffic**	Verifies that traffic is flowing through the ASA.

Command	Purpose
show firewall module [*mod-num*] **version**	Shows the software version of the ASA.
show firewall multiple-vlan-interfaces	Indicates the status of multiple VLAN interfaces (enabled or disabled).
show firewall vlan-group	Displays all configured VLAN groups.
show interface vlan	Displays the status and information about the configured VLAN interface.

Examples

The following is sample output from the **show firewall module** [*mod-num*] **state** command:

```
Router> show firewall module 11 state
Firewall module 11:
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 3,6,7,20-24,40,59,85,87-89,99-115,150,188-191,200,250,
     501-505,913,972
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:
Vlans allowed and active in management domain:
Vlans in spanning tree forwarding state and not pruned:
```

The following is sample output from the **show firewall module** [*mod-num*] **traffic** command:

```
Router> show firewall module 11 traffic
Firewall module 11:

Specified interface is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0014.1cd5.bef6 (bia 0014.1cd5.bef6)
  MTU 1500 bytes, BW 6000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 1000Mb/s, media type is unknown
  input flow-control is on, output flow-control is on
  Members in this channel: Gi11/1 Gi11/2 Gi11/3 Gi11/4 Gi11/5 Gi11/6
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queuing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 10000 bits/sec, 17 packets/sec
     8709 packets input, 845553 bytes, 0 no buffer
     Received 745 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     18652077 packets output, 1480488712 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The following is sample output from the **show firewall multiple-vlan-interfaces** command:

```
Router# show firewall multiple-vlan-interfaces
Multiple firewall vlan interfaces feature is enabled
```

The following is sample output from the **show firewall module** command:

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

The following is sample output from the **show firewall module** [*mod-num*] **version** command:

```
Router# show firewall module 2 version
ASA Service Module 2:

Sw Version: 100.7(8)19
```

The following is sample output from the **show firewall vlan-group** command:

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

The following is sample output from the **show interface vlan** command:

```
Router# show interface vlan 55
Vlan55 is up, line protocol is up
  Hardware is EtherSVI, address is 0008.20de.45ca (bia 0008.20de.45ca)
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  L2 Switched:ucast:196 pkt, 13328 bytes - mcast:4 pkt, 256 bytes
  L3 in Switched:ucast:0 pkt, 0 bytes - mcast:0 pkt, 0 bytes mcast
  L3 out Switched:ucast:0 pkt, 0 bytes
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     4 packets output, 256 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Feature History for the Switch for Use with the ASA Services Module

Table 2-1 lists each feature change and the platform release in which it was implemented.

Table 2-1 Feature History for the Switch for Use with the ASASM

Feature Name	Platform Releases	Feature Information
ASA Services Module support on the Cisco Catalyst 6500 switch	8.5(1)	The ASASM is a high-performance security services module for the Catalyst 6500 series switch, which you configure according to the procedures in this chapter. We introduced or modified the following commands: **firewall transparent, mac address auto, firewall autostate** (IOS), **interface vlan**.
ASA Services Module support on the Cisco 7600 switch	9.0(1)	The Cisco 7600 series now supports the ASASM.
Support for private VLANs	9.1(2)	You can use private VLANs with the ASASM. Assign the primary VLAN to the ASASM; the ASASM automatically handles secondary VLAN traffic. There is no configuration required on the ASASM for this feature; see the switch configuration guide for more information.