CHAPTER 12

Transparent Mode Interfaces

This chapter includes tasks to complete the interface configuration for all models in transparent firewall mode.

- Information About Transparent Mode Interfaces, page 12-1
- Licensing Requirements for Transparent Mode Interfaces, page 12-2
- Guidelines and Limitations for Transparent Mode Interfaces, page 12-4
- Default Settings for Transparent Mode Interfaces, page 12-5
- Completing Interface Configuration in Transparent Mode, page 12-6
- Turning Off and Turning On Interfaces, page 12-17
- Monitoring Interfaces, page 12-17
- Configuration Examples for Transparent Mode Interfaces, page 12-18
- Feature History for Transparent Mode Interfaces, page 12-19

Note

For multiple context mode, complete the tasks in this section in the context execution space. Enter the `changeto context` name command to change to the context you want to configure.

Information About Transparent Mode Interfaces

- Bridge Groups in Transparent Mode, page 12-1
- Security Levels, page 12-2

Bridge Groups in Transparent Mode

If you do not want the overhead of security contexts, or want to maximize your use of security contexts, you can group interfaces together in a bridge group, and then configure multiple bridge groups, one for each network. Bridge group traffic is isolated from other bridge groups; traffic is not routed to another bridge group within the Cisco ASA, and traffic must exit the ASA before it is routed by an external router back to another bridge group in the ASA. Although the bridging functions are separate for each bridge group, many other functions are shared between all bridge groups. For example, all bridge groups share a syslog server or AAA server configuration. For complete security policy separation, use security contexts with one bridge group in each context. At least one bridge group is required per context or in single mode.
Information About Transparent Mode Interfaces

Each bridge group requires a management IP address. For another method of management, see Management Interface, page 9-2.

Note

The ASA does not support traffic on secondary networks; only traffic on the same network as the management IP address is supported.

Security Levels

Each interface must have a security level from 0 (lowest) to 100 (highest). For example, you should assign your most secure network, such as the inside host network, to level 100. While the outside network connected to the Internet can be level 0. Other networks, such as DMZs can be in between. You can assign interfaces to the same security level. See Allowing Same Security Level Communication, page 12-16 for more information.

The level controls the following behavior:

- Network access—By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an ACL to the interface.

  If you enable communication for same security interfaces (see Allowing Same Security Level Communication, page 12-16), there is an implicit permit for interfaces to access other interfaces on the same security level or lower.

- Inspection engines—Some application inspection engines are dependent on the security level. For same security interfaces, inspection engines apply to traffic in either direction.
  - NetBIOS inspection engine—Applied only for outbound connections.
  - SQL*Net inspection engine—If a control connection for the SQL*Net (formerly OraServ) port exists between a pair of hosts, then only an inbound data connection is permitted through the ASA.

- Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).

  If you enable communication for same security interfaces, you can filter traffic in either direction.

- established command—This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

  If you enable communication for same security interfaces, you can configure established commands for both directions.

Licensing Requirements for Transparent Mode Interfaces
<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5506-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 5</td>
</tr>
<tr>
<td></td>
<td>Security Plus License: 30</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 536</td>
</tr>
<tr>
<td></td>
<td>Security Plus License: 636</td>
</tr>
<tr>
<td>ASA 5512-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 50</td>
</tr>
<tr>
<td></td>
<td>Security Plus License: 100</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 716</td>
</tr>
<tr>
<td></td>
<td>Security Plus License: 916</td>
</tr>
<tr>
<td>ASA 5515-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 100</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 916</td>
</tr>
<tr>
<td>ASA 5525-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 200</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 1316</td>
</tr>
<tr>
<td>ASA 5545-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 300</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 1716</td>
</tr>
<tr>
<td>ASA 5555-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 500</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 2516</td>
</tr>
<tr>
<td>ASA 5585-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base and Security Plus License: 1024</td>
</tr>
<tr>
<td></td>
<td>Interface Speed for SSP-10 and SSP-20:</td>
</tr>
<tr>
<td></td>
<td>Base License—1-Gigabit Ethernet for fiber interfaces</td>
</tr>
<tr>
<td></td>
<td>10 GE I/O License (Security Plus)—10-Gigabit Ethernet for fiber interfaces</td>
</tr>
<tr>
<td></td>
<td>(SSP-40 and SSP-60 support 10-Gigabit Ethernet by default.)</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base and Security Plus License: 4612</td>
</tr>
</tbody>
</table>
Guidelines and Limitations for Transparent Mode Interfaces

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

- For the ASA 5512-X and higher in multiple context mode, configure the physical interfaces in the system execution space according to Chapter 9, “Basic Interface Configuration (ASA Appliances).” Then, configure the logical interface parameters in the context execution space according to this chapter. For the ASASM in multiple context mode, configure switch ports and VLANs on the switch, and then assign VLANs to the ASASM according to the ASASM quick start guide.

The ASAv does not support multiple context mode.

- You can only configure context interfaces that you already assigned to the context in the system configuration using the allocate-interface command.

Firewall Mode Guidelines

- You can configure up to 250 bridge groups in single mode or per context in multiple mode. Note that you must use at least 1 bridge group; data interfaces must belong to a bridge group.

- Each bridge group can include up to 4 interfaces.

- For IPv4, a management IP address is required for each bridge group for both management traffic and for traffic to pass through the ASA.

Unlike routed mode, which requires an IP address for each interface, a transparent firewall has an IP address assigned to the entire bridge group. The ASA uses this IP address as the source address for packets originating on the ASA, such as system messages or AAA communications. In addition to the bridge group management address, you can optionally configure a management interface for some models; see Management Interface, page 9-2 for more information.
The management IP address must be on the same subnet as the connected network. You cannot set the subnet to a host subnet (255.255.255.255). The ASA does not support traffic on secondary networks; only traffic on the same network as the management IP address is supported. See Configuring Bridge Groups, page 12-7 for more information about management IP subnets.

- For IPv6, at a minimum you need to configure link-local addresses for each interface for through traffic. For full functionality, including the ability to manage the ASA, you need to configure a global IPv6 address for each bridge group.
- For multiple context mode, each context must use different interfaces; you cannot share an interface across contexts.
- For multiple context mode, each context typically uses a different subnet. You can use overlapping subnets, but your network topology requires router and NAT configuration to make it possible from a routing standpoint.

**Failover Guidelines**
Do not finish configuring failover interfaces with the procedures in this chapter. See Chapter 7, “Failover for High Availability,” to configure the failover and state links. In multiple context mode, failover interfaces are configured in the system configuration.

**IPv6 Guidelines**
No support for IPv6 anycast addresses in transparent mode.

**VLAN ID Guidelines for the ASASM**
You can add any VLAN ID to the configuration, but only VLANs that are assigned to the ASA by the switch can pass traffic. To view all VLANs assigned to the ASA, use the `show vlan` command.

If you add an interface for a VLAN that is not yet assigned to the ASA by the switch, the interface will be in the down state. When you assign the VLAN to the ASA, the interface changes to an up state. See the `show interface` command for more information about interface states.

## Default Settings for Transparent Mode Interfaces

This section lists default settings for interfaces if you do not have a factory default configuration. For information about the factory default configurations, see Factory Default Configurations, page 2-13.

### Default Security Level
The default security level is 0. If you name an interface “inside” and you do not set the security level explicitly, then the ASA sets the security level to 100.

**Note**
If you change the security level of an interface, and you do not want to wait for existing connections to time out before the new security information is used, you can clear the connections using the `clear local-host` command.

### Default State of Interfaces for the ASASM
- In single mode or in the system execution space, VLAN interfaces are enabled by default.
- In multiple context mode, all allocated interfaces are enabled by default, no matter what the state of the interface is in the system execution space. However, for traffic to pass through the interface, the interface also has to be enabled in the system execution space. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

**Jumbo Frame Support**

By default, the ASASM supports jumbo frames. Just configure the MTU for the desired packet size according to Configuring the MAC Address, MTU, and TCP MSS, page 12-11.

### Completing Interface Configuration in Transparent Mode

- Task Flow for Completing Interface Configuration, page 12-6
- Configuring Bridge Groups, page 12-7
- Configuring General Interface Parameters, page 12-8
- Configuring a Management Interface (ASA 5512-X and Higher and ASAv), page 12-10
- Configuring the MAC Address, MTU, and TCP MSS, page 12-11
- Configuring IPv6 Addressing, page 12-14
- Allowing Same Security Level Communication, page 12-16

### Task Flow for Completing Interface Configuration

**Step 1**
Set up your interfaces depending on your model:
- ASA 5512-X and higher—Chapter 9, “Basic Interface Configuration (ASA Appliances).”
- ASASM—ASASM quick start guide.
- ASAv—Chapter 10, “Basic Interface Configuration (ASAv).”

**Step 2**
(Multiple context mode) Allocate interfaces to the context according to Configure Multiple Contexts, page 6-14.

**Step 3**
(Multiple context mode) Enter the `chargeto context name` command to change to the context you want to configure.

**Step 4**
Configure one or more bridge groups, including the IPv4 address. See Configuring Bridge Groups, page 12-7.

**Step 5**
Configure general interface parameters, including the bridge group it belongs to, the interface name, and security level. See Configuring General Interface Parameters, page 12-8.

**Step 6**
(Optional) Configure a management interface. See Configuring a Management Interface (ASA 5512-X and Higher and ASAv), page 12-10.

**Step 7**
(Optional) Configure the MAC address and the MTU. See Configuring the MAC Address, MTU, and TCP MSS, page 12-11.

**Step 8**
Step 9  (Optional) Allow same security level communication, either by allowing communication between two interfaces or by allowing traffic to enter and exit the same interface. See Allowing Same Security Level Communication, page 12-16.

Configuring Bridge Groups

Each bridge group requires a management IP address. The ASA uses this IP address as the source address for packets originating from the bridge group. The management IP address must be on the same subnet as the connected network. For IPv4 traffic, the management IP address is required to pass any traffic. For IPv6 traffic, you must, at a minimum, configure the link-local addresses to pass traffic, but a global management address is recommended for full functionality, including remote management and other management operations.

Guidelines and Limitations

You can configure up to 250 bridge groups in single mode or per context in multiple mode. Note that you must use at least one bridge group; data interfaces must belong to a bridge group.

Note

For a separate management interface (for supported models), a non-configurable bridge group (ID 301) is automatically added to your configuration. This bridge group is not included in the bridge group limit.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Interface bvi bridge_group_number</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;ciscoasa(config)# interface bvi 1</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>ip address ip_address [mask] [standby ip_address]</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2</td>
</tr>
</tbody>
</table>
Examples

The following example sets the management address and standby address of bridge group 1:

ciscoasa(config)# interface bvi 1
  ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

What to Do Next


Configuring General Interface Parameters

This procedure describes how to set the name, security level, and bridge group for each transparent interface.

To configure a separate management interface, see Configuring a Management Interface (ASA 5512-X and Higher and ASAv), page 12-10.

For the ASA 5512-X and higher and the ASAv, you must configure interface parameters for the following interface types:

- Physical interfaces
- VLAN subinterfaces
- Redundant interfaces
- EtherChannel interfaces

For the ASASM, you must configure interface parameters for the following interface types:

- VLAN interfaces

Guidelines and Limitations

- You can configure up to four interfaces per bridge group.
- For information about security levels, see Security Levels, page 12-2.
- If you are using failover, do not use this procedure to name interfaces that you are reserving for failover and Stateful Failover communications. See Chapter 7, “Failover for High Availability,” to configure the failover and state links.

Prerequisites

- Set up your interfaces depending on your model:
  - ASA 5512-X and higher—Chapter 9, “Basic Interface Configuration (ASA Appliances).”
  - ASASM—ASASM quick start guide.
  - ASAv—Chapter 10, “Basic Interface Configuration (ASAv).”
- In multiple context mode, you can only configure context interfaces that you already assigned to the context in the system configuration according to Configure Multiple Contexts, page 6-14.
- In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, enter the changeto context name command.
Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Entry the interface configuration mode.</td>
</tr>
<tr>
<td>interface [(redundant number</td>
<td>The redundant number argument is the redundant interface ID, such as redundant 1.</td>
</tr>
<tr>
<td>port-channel number</td>
<td>The port-channel number argument is the EtherChannel interface ID, such as port-channel 1.</td>
</tr>
<tr>
<td>physical_interface).[subinterface]</td>
<td>See Enable the Physical Interface and Configure Ethernet Parameters, page 9-14 section for a description of the physical interface ID. Do not use this procedure for Management interfaces; see Configuring a Management Interface (ASA 5512-X and Higher and ASAv), page 12-10 to configure the Management interface.</td>
</tr>
<tr>
<td>mapped_name)</td>
<td>Append the subinterface ID to the physical or redundant interface ID separated by a period (.).</td>
</tr>
<tr>
<td>Example:</td>
<td>In multiple context mode, enter the mapped_name if one was assigned using the allocate-interface command.</td>
</tr>
<tr>
<td>ciscoasa(config)# interface gigabitethernet 0/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Assigns the interface to a bridge group, where number is an integer between 1 and 100. You can assign up to four interfaces to a bridge group. You cannot assign the same interface to more than one bridge group.</td>
</tr>
<tr>
<td>bridge-group number</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>ciscoasa(config-if)# bridge-group 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Names the interface.</td>
</tr>
<tr>
<td>nameif name</td>
<td>The name is a text string up to 48 characters, and is not case-sensitive. You can change the name by reentering this command with a new value. Do not enter the no form, because that command causes all commands that refer to that name to be deleted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>ciscoasa(config-if)# nameif inside</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Sets the security level, where number is an integer between 0 (lowest) and 100 (highest).</td>
</tr>
<tr>
<td>security-level number</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>ciscoasa(config-if)# security-level 50</td>
<td></td>
</tr>
</tbody>
</table>

What to Do Next

- (Optional) Configure a management interface. See Configuring a Management Interface (ASA 5512-X and Higher and ASAv), page 12-10.
- (Optional) Configure the MAC address and the MTU. See Configuring the MAC Address, MTU, and TCP MSS, page 12-11.
Completing Interface Configuration in Transparent Mode

Configuring a Management Interface (ASA 5512-X and Higher and ASAv)

You can configure one management interface separate from the bridge group interfaces in single mode or per context. For more information, see Management Interface, page 9-2.

Restrictions

- See Management Interface, page 9-2.
- Do not assign this interface to a bridge group; a non-configurable bridge group (ID 101) is automatically added to your configuration. This bridge group is not included in the bridge group limit.
- If your model does not include a Management interface, you must manage the transparent firewall from a data interface; skip this procedure. (For example, on the ASASM.)
- In multiple context mode, you cannot share any interfaces, including the Management interface, across contexts. To provide management per context, you can create subinterfaces of the Management interface and allocate a Management subinterface to each context. Note that the ASA 5512-X through ASA 5555-X do not allow subinterfaces on the Management interface, so for per-context management, you must connect to a data interface.

Prerequisites

- Complete the procedures in Chapter 9, “Basic Interface Configuration (ASA Appliances).”
- In multiple context mode, you can only configure context interfaces that you already assigned to the context in the system configuration according to Configure Multiple Contexts, page 6-14.
- In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, enter the changeto context name command.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>If you are not already in interface configuration mode, enters interface configuration mode for the management interface.</td>
</tr>
<tr>
<td>interface {{port-channel number</td>
<td>management slot/port[.subinterface]</td>
</tr>
<tr>
<td>Example: ciscoasa(config)# interface management 0/0/1</td>
<td>Redundant interfaces do not support Management slot/port interfaces as members. You also cannot set a redundant interface comprised of non-Management interfaces as management-only.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Names the interface.</td>
</tr>
<tr>
<td>nameif name</td>
<td>In multiple context mode, enter the mapped_name if one was assigned using the allocate-interface command.</td>
</tr>
<tr>
<td>Example: ciscoasa(config-if)# nameif management</td>
<td>The name is a text string up to 48 characters, and is not case-sensitive. You can change the name by reentering this command with a new value. Do not enter the no form, because that command causes all commands that refer to that name to be deleted.</td>
</tr>
</tbody>
</table>
### Completing Interface Configuration in Transparent Mode

#### Step 3
Do one of the following:

- **ip address ip_address [mask] [standby ip_address]**

  **Example:**
  
  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

  **Purpose:** Sets the IP address manually.
  
  **Note** For use with failover, you must set the IP address and standby address manually; DHCP is not supported.

  The **ip_address** and **mask** arguments set the interface IP address and subnet mask.

  The **standby ip_address** argument is used for failover. See [Configure Active/Standby Failover](#) or [Configure Active/Active Failover](#) for more information.

- **ip address dhcp [setroute]**

  **Example:**
  
  ```
  ciscoasa(config-if)# ip address dhcp
  ```

  **Purpose:** Obtains an IP address from a DHCP server.

  The **setroute** keyword lets the ASA use the default route supplied by the DHCP server.

  Reenter this command to reset the DHCP lease and request a new lease.

  If you do not enable the interface using the **no shutdown** command before you enter the **ip address dhcp** command, some DHCP requests might not be sent.

- **security-level number**

  **Example:**
  
  ```
  ciscoasa(config-if)# security-level 50
  ```

  **Purpose:** Sets the security level, where **number** is an integer between 0 (lowest) and 100 (highest).

#### What to Do Next

- (Optional) Configure the MAC address and the MTU. See [Configuring the MAC Address, MTU, and TCP MSS](#).

- (Optional) Configure IPv6 addressing. See [Configuring IPv6 Addressing](#).

### Configuring the MAC Address, MTU, and TCP MSS

This section describes how to configure MAC addresses for interfaces, how to set the MTU, and set the TCP MSS.

#### Information About MAC Addresses

By default, the physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address.

For the ASASM, all VLANs use the same MAC address provided by the backplane.

A redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. If you assign a MAC address to the redundant interface using this command, then it is used regardless of the member interface MAC addresses.
Completing Interface Configuration in Transparent Mode

For an EtherChannel, all interfaces that are part of the channel group share the same MAC address. This feature makes the EtherChannel transparent to network applications and users, because they only see the one logical connection; they have no knowledge of the individual links. The port-channel interface uses the lowest numbered channel group interface MAC address as the port-channel MAC address. Alternatively you can manually configure a MAC address for the port-channel interface. In multiple context mode, you can automatically assign unique MAC addresses to interfaces, including an EtherChannel port interface. We recommend manually, or in multiple context mode, automatically configuring a unique MAC address in case the group channel interface membership changes. If you remove the interface that was providing the port-channel MAC address, then the port-channel MAC address changes to the next lowest numbered interface, thus causing traffic disruption.

In multiple context mode, if you share an interface between contexts, you can assign a unique MAC address to the interface in each context. This feature lets the ASA easily classify packets into the appropriate context. Using a shared interface without unique MAC addresses is possible, but has some limitations. See How the ASA Classifies Packets, page 6-3 for more information. You can assign each MAC address manually, or you can automatically generate MAC addresses for shared interfaces in contexts. See Assign MAC Addresses to Context Interfaces Automatically, page 6-23 to automatically generate MAC addresses. If you automatically generate MAC addresses, you can use this procedure to override the generated address.

For single context mode, or for interfaces that are not shared in multiple context mode, you might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address.

Information About the MTU and TCP MSS

See Control Fragmentation with the Maximum Transmission Unit and TCP Maximum Segment Size, page 9-7.

Prerequisites

- Set up your interfaces depending on your model:
  - ASA 5512-X and higher—Chapter 9, “Basic Interface Configuration (ASA Appliances).”
  - ASASM—ASASM quick start guide.
  - ASAv—Chapter 10, “Basic Interface Configuration (ASAv).”
- In multiple context mode, you can only configure context interfaces that you already assigned to the context in the system configuration according to Configure Multiple Contexts, page 6-14.
- In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, enter the changeto context name command.
- To increase the MTU above 1500, enable jumbo frames on supported models according to Enable Jumbo Frame Support, page 9-22. Jumbo frames are supported by default on the ASASM; you do not need to enable them.
Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;For the ASA 5512-X and higher and the ASAv:&lt;br&gt;`interface { (redundant number</td>
<td>port-channel number</td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;<code>mac-address mac_address [standby mac_address]</code></td>
<td>Assigns a private MAC address to this interface. The mac_address is in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE is entered as 000C.F142.4CDE. The first two bytes of a manual MAC address cannot be A2 if you also want to use auto-generated MAC addresses. For use with failover, set the standby MAC address. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.</td>
</tr>
<tr>
<td><strong>Step 3</strong>&lt;br&gt;<code>mtu interface_name bytes</code></td>
<td>Sets the MTU between 300 and 9198 bytes (9000 for the ASAv). The default is 1500 bytes.&lt;br&gt;Note When you set the MTU for a redundant or port-channel interface, the ASA applies the setting to all member interfaces. For models that support jumbo frames, if you enter a value for any interface that is greater than 1500, then you need to enable jumbo frame support. See Enable Jumbo Frame Support, page 9-22.</td>
</tr>
<tr>
<td><strong>Step 4</strong>&lt;br&gt;<code>sysopt connection tcpmss [minimum] bytes</code></td>
<td>Sets the maximum TCP segment size in bytes, between 48 and any maximum number. The default value is 1380 bytes. You can disable this feature by setting bytes to 0. For the minimum keyword, sets the maximum segment size to be no less than bytes, between 48 and 65535. The minimum feature is disabled by default (set to 0).</td>
</tr>
</tbody>
</table>
What to Do Next


Configuring IPv6 Addressing

This section describes how to configure IPv6 addressing.

- Information About IPv6, page 12-14
- Configuring a Global IPv6 Address, page 12-15
- Configuring IPv6 Neighbor Discovery, page 12-16

Information About IPv6

This section includes information about how to configure IPv6.

- IPv6 Addressing, page 12-14
- Modified EUI-64 Interface IDs, page 12-14
- Unsupported Commands, page 12-15

IPv6 Addressing

You can configure two types of unicast addresses for IPv6:

- Global—The global address is a public address that you can use on the public network. This address needs to be configured for each bridge group, and not per-interface. You can also configure a global IPv6 address for the management interface.

- Link-local—The link-local address is a private address that you can only use on the directly-connected network. Routers do not forward packets using link-local addresses; they are only for communication on a particular physical network segment. They can be used for address configuration or for the ND functions such as address resolution and neighbor discovery. Because the link-local address is only available on a segment, and is tied to the interface MAC address, you need to configure the link-local address per interface.

At a minimum, you need to configure a link-local address for IPv6 to operate. If you configure a global address, a link-local address is automatically configured on each interface, so you do not also need to specifically configure a link-local address. If you do not configure a global address, then you need to configure the link-local address, either automatically or manually.

Note

If you want to only configure the link-local addresses, see the `ipv6 enable` (to auto-configure) or `ipv6 address link-local` (to manually configure) command in the command reference.

Modified EUI-64 Interface IDs

RFC 3513: Internet Protocol Version 6 (IPv6) Addressing Architecture requires that the interface identifier portion of all unicast IPv6 addresses, except those that start with binary value 000, be 64 bits long and be constructed in Modified EUI-64 format. The ASA can enforce this requirement for hosts attached to the local link.
When this feature is enabled on an interface, the source addresses of IPv6 packets received on that interface are verified against the source MAC addresses to ensure that the interface identifiers use the Modified EUI-64 format. If the IPv6 packets do not use the Modified EUI-64 format for the interface identifier, the packets are dropped and the following system log message is generated:

%ASA-3-325003: EUI-64 source address check failed.

The address format verification is only performed when a flow is created. Packets from an existing flow are not checked. Additionally, the address verification can only be performed for hosts on the local link. Packets received from hosts behind a router will fail the address format verification, and be dropped, because their source MAC address will be the router MAC address and not the host MAC address.

Unsupported Commands

The following IPv6 commands are not supported in transparent firewall mode, because they require router capabilities:

- ipv6 address autoconfig
- ipv6 nd prefix
- ipv6 nd ra-interval
- ipv6 nd ra-lifetime
- ipv6 nd suppress-ra

Configuring a Global IPv6 Address

To configure a global IPv6 address for a bridge group or management interface, perform the following steps.

Note

Configuring the global address automatically configures the link-local address, so you do not need to configure it separately.

Restrictions

The ASA does not support IPv6 anycast addresses.

Prerequisites

- Set up your interfaces depending on your model:
  - ASA 5512-X and higher—Chapter 9, “Basic Interface Configuration (ASA Appliances).”
  - ASASM—ASASM quick start guide.
  - ASAv—Chapter 10, “Basic Interface Configuration (ASAv).”
- In multiple context mode, you can only configure context interfaces that you already assigned to the context in the system configuration according to Configure Multiple Contexts, page 6-14.
- In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, enter the `changeto context name` command.
Completing Interface Configuration in Transparent Mode

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>For the bridge group:</td>
<td></td>
</tr>
<tr>
<td><code>interface bvi bridge_group_id</code></td>
<td>If you are not already in interface configuration mode, enters</td>
</tr>
<tr>
<td>For the management interface:</td>
<td>interface configuration mode.</td>
</tr>
<tr>
<td><code>interface management_interface_id</code></td>
<td></td>
</tr>
<tr>
<td>Example: ciscoasa(config)## interface bvi 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>ipv6 address ipv6-address/prefix-length [standby ipv6-address]</code></td>
<td>Assigns a global address to the interface. When you assign a</td>
</tr>
<tr>
<td>Example: ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48</td>
<td>global address, the link-local address is automatically created for</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>(Optional) <code>ipv6 enforce-eui64 if_name</code></td>
<td>Enforces the use of Modified EUI-64 format interface identifiers</td>
</tr>
<tr>
<td>Example: ciscoasa(config)# ipv6 enforce-eui64 inside</td>
<td>in IPv6 addresses on a local link.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Configuring IPv6 Neighbor Discovery**


**Allowing Same Security Level Communication**

By default, interfaces on the same security level cannot communicate with each other, and packets cannot enter and exit the same interface. This section describes how to enable inter-interface communication when interfaces are on the same security level.

**Information About Inter-Interface Communication**

Allowing interfaces on the same security level to communicate with each other is useful if you want traffic to flow freely between all same security interfaces without ACLs.

If you enable same security interface communication, you can still configure interfaces at different security levels as usual.
Turning Off and Turning On Interfaces

This section describes how to turn off and on an interface.

All interfaces are enabled by default. In multiple context mode, if you disable or reenable the interface within a context, only that context interface is affected. But if you disable or reenable the interface in the system execution space, then you affect that interface for all contexts.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>same-security-traffic permit inter-interface</td>
<td>Enables interfaces on the same security level so that they can communicate with each other.</td>
</tr>
</tbody>
</table>

Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Ciscoasa(config)# interface (vlan number</td>
<td>If you are not already in interface configuration mode, enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>mapped_name)</td>
<td>In multiple context mode, enter the mapped_name if one was assigned using the allocate-interface command.</td>
</tr>
<tr>
<td>Example:</td>
<td>Ciscoasa(config)# interface vlan 100</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>shutdown</td>
<td>Disables the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Ciscoasa(config-if)# shutdown</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>no shutdown</td>
<td>Reenables the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Ciscoasa(config-if)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>

Monitoring Interfaces

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface</td>
<td>Displays interface statistics.</td>
</tr>
<tr>
<td>show interface ip brief</td>
<td>Displays interface IP addresses and status.</td>
</tr>
<tr>
<td>show bridge-group</td>
<td>Shows bridge group information.</td>
</tr>
</tbody>
</table>
Configuration Examples for Transparent Mode Interfaces

The following example includes two bridge groups of three interfaces each, plus a management-only interface:

interface gigabitethernet 0/0
    nameif inside1
    security-level 100
    bridge-group 1
    no shutdown
interface gigabitethernet 0/1
    nameif outside1
    security-level 0
    bridge-group 1
    no shutdown
interface gigabitethernet 0/2
    nameif dmz1
    security-level 50
    bridge-group 1
    no shutdown
interface bvi 1
    ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

interface gigabitethernet 1/0
    nameif inside2
    security-level 100
    bridge-group 2
    no shutdown
interface gigabitethernet 1/1
    nameif outside2
    security-level 0
    bridge-group 2
    no shutdown
interface gigabitethernet 1/2
    nameif dmz2
    security-level 50
    bridge-group 2
    no shutdown
interface bvi 2
    ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9

interface management 0/0
    nameif mgmt
    security-level 100
    ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
    no shutdown
### Feature History for Transparent Mode Interfaces

Table 12-1 lists each feature change and the platform release in which it was implemented.

#### Table 12-1  Feature History for Interfaces in Transparent Mode

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased VLANs</td>
<td>7.0(5)</td>
<td>Increased the following limits:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA5510 Base license VLANs from 0 to 10.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA5510 Security Plus license VLANs from 10 to 25.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA5520 VLANs from 25 to 100.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA5540 VLANs from 100 to 200.</td>
</tr>
<tr>
<td>Increased VLANs</td>
<td>7.2(2)</td>
<td>The maximum number of VLANs for the Security Plus license on the ASA 5505 was increased from 5 (3 fully functional; 1 failover; one restricted to a backup interface) to 20 fully functional interfaces. In addition, the number of trunk ports was increased from 1 to 8. Now there are 20 fully functional interfaces, you do not need to use the backup interface command to cripple a backup ISP interface; you can use a fully-functional interface for it. The backup interface command is still useful for an Easy VPN configuration. VLAN limits were also increased for the ASA 5510 (from 10 to 50 for the Base license, and from 25 to 100 for the Security Plus license), the ASA 5520 (from 100 to 150), the ASA 5550 (from 200 to 250).</td>
</tr>
<tr>
<td>Gigabit Ethernet Support for the ASA 5510</td>
<td>7.2(3)</td>
<td>The ASA 5510 now supports GE (Gigabit Ethernet) for port 0 and 1 with the Security Plus license. If you upgrade the license from Base to Security Plus, the capacity of the external Ethernet0/0 and Ethernet0/1 ports increases from the original FE (Fast Ethernet) (100 Mbps) to GE (1000 Mbps). The interface names will remain Ethernet 0/0 and Ethernet 0/1. Use the speed command to change the speed on the interface and use the show interface command to see what speed is currently configured for each interface.</td>
</tr>
<tr>
<td>Security Plus License</td>
<td></td>
<td>You can now include the native VLAN in an ASA 5505 trunk port.</td>
</tr>
<tr>
<td>Native VLAN support for the ASA 5505</td>
<td>7.2(4)/8.0(4)</td>
<td>We introduced the following command: switchport trunk native vlan.</td>
</tr>
</tbody>
</table>
### Feature History for Transparent Mode Interfaces (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jumbo packet support for the ASA 5580</td>
<td>8.1(1)</td>
<td>The Cisco ASA 5580 supports jumbo frames. A jumbo frame is an Ethernet packet larger than the standard maximum of 1518 bytes (including Layer 2 header and FCS), up to 9216 bytes. You can enable support for jumbo frames for all interfaces by increasing the amount of memory to process Ethernet frames. Assigning more memory for jumbo frames might limit the maximum use of other features, such as ACLs. We introduced the following command: <code>jumbo-frame reservation</code>.</td>
</tr>
<tr>
<td>Increased VLANs for the ASA 5580</td>
<td>8.1(2)</td>
<td>The number of VLANs supported on the ASA 5580 are increased from 100 to 250.</td>
</tr>
<tr>
<td>IPv6 support for transparent mode</td>
<td>8.2(1)</td>
<td>IPv6 support was introduced for transparent firewall mode.</td>
</tr>
<tr>
<td>Support for Pause Frames for Flow Control on the ASA 5580 10-Gigabit Ethernet Interfaces</td>
<td>8.2(2)</td>
<td>You can now enable pause (XOFF) frames for flow control. We introduced the following command: <code>flowcontrol</code>.</td>
</tr>
<tr>
<td>Bridge groups for transparent mode</td>
<td>8.4(1)</td>
<td>If you do not want the overhead of security contexts, or want to maximize your use of security contexts, you can group interfaces together in a bridge group, and then configure multiple bridge groups, one for each network. Bridge group traffic is isolated from other bridge groups. You can configure up to eight bridge groups of four interfaces each in single mode or per context. We introduced the following commands: <code>interface bvi</code>, <code>show bridge-group</code>.</td>
</tr>
<tr>
<td>Transparent mode bridge group maximum increased to 250</td>
<td>9.3(1)</td>
<td>The bridge group maximum was increased from 8 to 250 bridge groups. You can configure up to 250 bridge groups in single mode or per context in multiple mode, with 4 interfaces maximum per bridge group. We modified the following commands: <code>interface bvi</code>, <code>bridge-group</code>.</td>
</tr>
</tbody>
</table>