

VLAN Subinterfaces

This chapter tells how to configure VLAN subinterfaces.

Note For multiple context mode, complete all tasks in this section in the system execution space. To change from the context to the system execution space, enter the **changeto system** command.

- About VLAN Subinterfaces, on page 1
- Licensing for VLAN Subinterfaces, on page 1
- Guidelines and Limitations for VLAN Subinterfaces, on page 2
- Default Settings for VLAN Subinterfaces, on page 3
- Configure VLAN Subinterfaces and 802.1Q Trunking, on page 3
- Monitoring VLAN Subinterfaces, on page 5
- Examples for VLAN Subinterfaces, on page 5
- History for VLAN subinterfaces, on page 6

About VLAN Subinterfaces

VLAN subinterfaces let you divide a physical or EtherChannel interface into multiple logical interfaces that are tagged with different VLAN IDs. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk. Because VLANs allow you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or ASAs. This feature is particularly useful in multiple context mode so that you can assign unique interfaces to each context.

You can configure a primary VLAN, as well as one or more secondary VLANs. When the ASA receives traffic on the secondary VLANs, it maps it to the primary VLAN.

Licensing for VLAN Subinterfaces

Model	License Requirement
Firepower 1010	Standard License: 60

Model	License Requirement
Firepower 1120	Standard License: 512
Firepower 1140, 1150	Standard License: 1024
Firepower 2100	Standard License: 1024
Secure Firewall 3100	Standard License: 1024
Firepower 4100	Standard License: 1024
Firepower 9300	Standard License: 1024
ASAv	Throughput capability: 100 Mbps: 25 1 Gbps: 50 2 Gbps: 200 10 Gbps: 1024
ISA 3000	Standard License: 5 Security Plus License: 100

Note For an interface to count against the VLAN limit, you must assign a VLAN to it. For example:

```
interface gigabitethernet 0/0.100
  vlan 100
```

Guidelines and Limitations for VLAN Subinterfaces

Model Support

- 1010—VLAN subinterfaces are not supported on switch ports or VLAN interfaces.
- For ASA models, you cannot configure subinterfaces on the Management interface. See Management Slot/Port Interface for subinterface support.

Additional Guidelines

- Preventing untagged packets on the physical interface—If you use subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. This property is also true for the active physical interface for EtherChannel links. Because the physical or EtherChannel interface must be enabled for the subinterface to pass traffic, ensure that the physical or EtherChannel interface does not pass traffic by leaving out the **nameif** command. If you want to let

the physical or EtherChannel interface pass untagged packets, you can configure the **nameif** command as usual.

- All subinterfaces on the same parent interface must be either bridge group members or routed interfaces; you cannot mix and match.
- The ASA does not support the Dynamic Trunking Protocol (DTP), so you must configure the connected switch port to trunk unconditionally.
- You might want to assign unique MAC addresses to subinterfaces defined on the ASA, because they use the same burned-in MAC address of the parent interface. For example, your service provider might perform access control based on the MAC address. Also, because IPv6 link-local addresses are generated based on the MAC address, assigning unique MAC addresses to subinterfaces allows for unique IPv6 link-local addresses, which can avoid traffic disruption in certain instances on the ASA. You can automatically generate unique MAC addresses; see Automatically Assign MAC Addresses.



Note If you manually assign a MAC address, be sure to assign MAC addresses to all subinterfaces on the same physical interface to avoid unexpected behavior and outages.

Default Settings for VLAN Subinterfaces

This section lists default settings for interfaces if you do not have a factory default configuration.

Default State of Interfaces

The default state of an interface depends on the type and the context mode.

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.

In single mode or in the system execution space, interfaces have the following default states:

- Physical interfaces—Disabled.
- VLAN subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.

Configure VLAN Subinterfaces and 802.1Q Trunking

Add a VLAN subinterface to a physical or EtherChannel interface.

Before you begin

For multiple context mode, complete this procedure in the system execution space. To change from the context to the system execution space, enter the **changeto system** command.

Procedure

Step 1 Specify the new subinterface:

interface {*physical_interface* | **port-channel** *number*}.*subinterface*

Example:

```
ciscoasa(config)# interface gigabitethernet 0/1.100
```

The **port-channel** *number* argument is the EtherChannel interface ID, such as **port-channel 1**.

The *subinterface* ID is an integer between 1 and 4294967293.

Step 2 Specify the VLAN for the subinterface:

vlan *vlan_id* [**secondary** *vlan_range*]

Example:

```
ciscoasa(config-subif)# vlan 101 secondary 52 64,66-74
```

The *vlan_id* is an integer between 1 and 4094. Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information.

The secondary VLANs can be separated by spaces, commas, and dashes (for a contiguous range). When the ASA receives traffic on the secondary VLANs, it maps the traffic to the primary VLAN.

You cannot assign the same VLAN to multiple subinterfaces. You cannot assign a VLAN to the physical interface. Each subinterface must have a VLAN ID before it can pass traffic. To change a VLAN ID, you do not need to remove the old VLAN ID with the **no** option; you can enter the **vlan** command with a different VLAN ID, and the ASA changes the old ID. To remove some secondary VLANs from the list, you can use the **no** command and only list the VLANs to remove. You can only selectively remove listed VLANs; you cannot remove a single VLAN in a range, for example.

Examples

The following example maps a set of secondary VLANs to VLAN 200:

```
interface gigabitethernet 0/6.200
   vlan 200 secondary 500 503 600-700
```

The following example removes secondary VLAN 503 from the list:

```
no vlan 200 secondary 503
show running-config interface gigabitethernet0/6.200
!
interface GigabitEthernet0/6.200
 vlan 200 secondary 500 600-700
 no nameif
 no security-level
```

```
no ip address
```

Related Topics

Licensing for VLAN Subinterfaces, on page 1

Monitoring VLAN Subinterfaces

See the following commands:

- **show interface**

  Displays interface statistics.

- **show interface ip brief**

  Displays interface IP addresses and status.

- **show vlan mapping**

  Shows the interface, secondary VLANs, and the primary VLANs to which they are mapped.

Examples for VLAN Subinterfaces

The following example configures parameters for a subinterface in single mode:

```
interface gigabitethernet 0/1
  no nameif
  no security-level
  no ip address
  no shutdown
interface gigabitethernet 0/1.1
  vlan 101
  nameif inside
  security-level 100
  ip address 192.168.6.6 255.255.255.0
  no shutdown
```

The following example shows how VLAN mapping works with the Catalyst 6500. Consult the Catalyst 6500 configuration guide on how to connect nodes to PVLANS.

ASA Configuration

```
interface GigabitEthernet1/1
  description Connected to Switch GigabitEthernet1/5
  no nameif
  no security-level
  no ip address
  no shutdown
!
interface GigabitEthernet1/1.70
  vlan 70 secondary 71 72
  nameif vlan_map1
  security-level 50
  ip address 10.11.1.2 255.255.255.0
```

```
  no shutdown
!
interface GigabitEthernet1/2
  nameif outside
  security-level 0
  ip address 172.16.171.31 255.255.255.0
  no shutdown

Catalyst 6500 Configuration

vlan 70
  private-vlan primary
  private-vlan association 71-72
!
vlan 71
  private-vlan community
!
vlan 72
  private-vlan isolated
!
interface GigabitEthernet1/5
  description Connected to ASA GigabitEthernet1/1
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 70-72
  switchport mode trunk
!
```

History for VLAN subinterfaces

Table 1: History for VLAN Subinterfaces

Feature Name	Version	Feature Information
Increased VLANs	7.0(5)	Increased the following limits: • ASA5510 Base license VLANs from 0 to 10. • ASA5510 Security Plus license VLANs from 10 to 25. • ASA5520 VLANs from 25 to 100. • ASA5540 VLANs from 100 to 200.
Increased VLANs	7.2(2)	VLAN limits were 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).
Increased VLANs for the ASA 5580	8.1(2)	The number of VLANs supported on the ASA 5580 are increased from 100 to 250.
Support to map a Secondary VLANs to a Primary VLAN	9.5(2)	You can now configure one or more secondary VLANs for a subinterface. When the ASA receives traffic on the secondary VLANs, it maps it to the primary VLAN. We introduced or modified the following commands: **vlan secondary, show vlan mapping**

Feature Name	Version	Feature Information
Increased VLANs for the ISA 3000	9.13(1)	The maximum VLANs for the ISA 3000 with the Security Plus license increased from 25 to 100.