Critical Voice VLAN Support

Critical Voice VLAN Support puts phone traffic into the configured voice VLAN of a port if the authentication server becomes unreachable.

With normal network connectivity, when an IP phone successfully authenticates on a port, the authentication server puts the phone into the voice domain. If the authentication server becomes unreachable, IP phones cannot authenticate. In multidomain authentication (MDA) mode or multiauthentication mode, you can configure the Critical Voice VLAN support feature to put phone traffic into the configured voice VLAN of the port.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Critical Voice VLAN Support

- Use different VLANs for voice and data.
- The voice VLAN must be configured on the switch.

- ACLs are not supported on fixed Cisco Integrated Services Routers (ISRs).

- This feature does not support standard ACLs on the switch port.

Information About Critical Voice VLAN Support

Critical Voice VLAN Support in Multidomain Authentication Mode

If a critical voice VLAN is deployed using an interface in multidomain authentication (MDA) mode, the host mode is changed to multihost and the first phone device is installed as a static forwarding entries. Any additional phone devices are installed as dynamic forwarding entry in the Host Access Table (HAT).

For further information about host modes, see the *802.1X Authentication Services Configuration Guide*.

Note If a critical port is already authorized and reauthentication occurs, the switch puts the port in the critical-authentication state in the current VLAN, which might be the one previously assigned by the RADIUS server.

Note Inaccessible authentication bypass is compatible with guest VLAN. When a guest VLAN is enabled on a 802.1X port, the features interact as follows: if all RADIUS servers are not available and if a client is connected to a critical port and was previously assigned to a guest VLAN, the switch keeps the port in the guest VLAN.

Critical Voice VLAN Support in Multiauthentication Mode

If the critical authentication feature is deployed in multiauthentication mode, only one phone device will be allowed and a second phone trying to authorize will trigger a violation.

The **show authentication sessions** command displays the critical voice client data. A critically authorized voice client in multiauthentication host mode will be in the "authz success" and "authz fail" state.

Note If critical voice is required, then critical data should be configured too. Otherwise, the critical voice client will be displayed in the "authz fail" state while the voice VLAN will be open.

How to Configure Critical Voice VLAN Support

Configuring Critical Voice VLAN Support in Multidomain Authentication Mode

Perform this task on a port to configure critical voice VLAN support in multidomain authentication (MDA) mode.

✎

Note   To configure MDA mode, see the "Configuring the Host Mode" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **authentication event server dead action authorize vlan** *vlan-id*
5. **authentication event server dead action authorize voice**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitethernet 0/1`	Specifies the port to be configured and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**authentication event server dead action authorize vlan** *vlan-id* **Example:** Switch(config-if)# authentication event server dead action authorize vlan 40	Configures a critical data VLAN. **Note** This step is only required if the **authentication event server dead action authorize vlan** *vlan-id* command is not configured on the port.
Step 5	**authentication event server dead action authorize voice** **Example:** Switch(config-if)# authentication event server dead action authorize voice	Enables the Critical Voice VLAN feature, which puts phone traffic into the configured voice VLAN of a port if the authentication server becomes unreachable.

Configuring Critical Voice VLAN Support in Multiauthentication Mode

Perform this task to configure critical voice VLAN support in multiauthentication mode.

Note To configure multiauthentication mode, see the "Configuring the Host Mode" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **authentication event server dead action reinitialize vlan** *vlan-id*
5. **authentication event server dead action authorize voice**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Switch> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Switch# configure terminal	Enters global configuration mode.
Step 3	**interface** *type slot/port* **Example:** Switch(config)# interface gigabitethernet 0/1	Specifies the port to be configured and enters interface configuration mode.
Step 4	**authentication event server dead action reinitialize vlan** *vlan-id* **Example:** Switch(config-if)# authentication event server dead action reinitialize vlan 40	Configures a critical data VLAN. **Note** This step is only required if the **authentication event server dead action authorize vlan** *critical-data-vlan-id* command is not configured on the port.
Step 5	**authentication event server dead action authorize voice** **Example:** Switch(config-if)# authentication event server dead action authorize voice	Enables the Critical Voice VLAN support feature, which puts phone traffic into the configured voice VLAN of a port if the authentication server becomes unreachable.

Configuration Examples for Critical Voice VLAN Support

Example: Critical Voice VLAN Support in Multidomain Authentication Mode

The following example shows how to enable the Critical Voice VLAN feature in MDA host-mode:

```
Switch(config) interface GigabitEthernet 0/0/0
Switch(config-if)# switchport access vlan 110
Switch(config-if)# switchport voice vlan 110
Switch(config-if)# no ip address
Switch(config-if)# authentication event server dead action authorize vlan 12
Switch(config-if)# authentication event server dead action authorize voice
Switch(config-if)# authentication host-mode multi-domain
Switch(config-if)# authentication port-control auto
Switch(config-if)# mab
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# end
```

Example: Critical Voice VLAN Support in Multiauthentication Mode

The following example shows how to enable the Critical Voice VLAN support feature in multiauthentication mode:

```
Switch(config) interface GigabitEthernet 0/0/0
Switch(config-if)# switchport access vlan 110
Switch(config-if)# switchport voice vlan 110
Switch(config-if)# no ip address
Switch(config-if)# authentication event server dead action reinitialize vlan 12
Switch(config-if)# authentication event server dead action authorize voice
Switch(config-if)# authentication host-mode multi-auth
Switch(config-if)# authentication port-control auto
Switch(config-if)# mab
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IEEE 802.1X commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	• *Catalyst 4500 Series Switch Cisco IOS Command Reference, Release 12.2(25)SGA* • *Catalyst 3750 Switch Command Reference, Cisco IOS Release 12.2(25)SEE*

Standards and RFCs

Standard/RFC	Title
IEEE 802.1X	*Port Based Network Access Control*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Critical Voice VLAN Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Critical Voice VLAN Support

Feature Name	Releases	Feature Information
Critical Voice VLAN Support	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE	This feature enables critical voice VLAN support, which puts phone traffic into the configured voice VLAN of a port if the authentication server becomes unreachable. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.

Feature Name	Releases	Feature Information
Critical VLAN with Multi-auth	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE	This feature adds support for the Critical Voice VLAN feature in multiauthentication mode. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.