Catalyst Switches der Serien 2960/2950 mit Sprach-VLAN - Konfigurationsbeispiel

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Voice VLAN - Übersicht
Konfigurieren
Netzwerkdiagramm
Konfigurationen
Basierend auf einem vertrauenswürdigen CoS-Wert
Bei Verwendung eines IP-Telefons eines anderen Anbieters
Basierend auf einem vertrauenswürdigen DSCP-Wert im IP-Header
Überprüfung
Zugehörige Informationen

Einleitung

Dieses Dokument enthält eine Beispielkonfiguration für Sprach-VLAN auf Cisco Catalyst Switches der Serien 2960/2950. Dieses Dokument zeigt insbesondere, wie die Sprach-VLAN-Funktion auf einem Cisco Catalyst 2950 Switch konfiguriert wird.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Grundkenntnisse der Konfiguration von Cisco Catalyst Switches der Serien 2960/2950
- Grundlegende Kenntnisse des Sprach-VLANs

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco Catalyst Switch der Serie 2950.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Voice VLAN - Übersicht

Mit der Sprach-VLAN-Funktion können die Switch-Ports Sprachdatenverkehr mit Layer-3-IP-Rangfolge und Layer-2-CoS-Werten (Class of Service) von einem IP-Telefon übertragen. Der Switch basiert auf **IEEE 802.1p CoS** und unterstützt Quality of Service (QoS). Klassifizierung und Planung werden zum Senden von Netzwerkverkehr vom Switch verwendet. Sie können das Cisco IP-Telefon so konfigurieren, dass Datenverkehr mit einer IEEE 802.1p-Priorität weitergeleitet wird, und den Switch so konfigurieren, dass die von einem IP-Telefon zugewiesene Verkehrspriorität vertrauenswürdig ist oder überschrieben wird.

Sie können den Switch-Port, der mit einem IP-Telefon verbunden ist, so konfigurieren, dass ein VLAN für Sprachverkehr und ein anderes VLAN für Datenverkehr von einem Gerät, das an den Zugriffsport des IP-Telefons angeschlossen ist, verwendet wird. Sie können die Access Ports am Switch so konfigurieren, dass sie **Cisco Discovery Protocol (CDP)**-Pakete senden, um ein angeschlossenes IP-Telefon anzuweisen, Sprachdatenverkehr an den Switch mit einer der folgenden Methoden zu senden:

- Im Sprach-VLAN mit einem Layer-2-CoS-Prioritätswert versehen
- Im Zugriffs-VLAN mit einem Prioritätswert für Layer 2-CoS versehen
- Im Zugriffs-VLAN unmarkiert (kein Layer-2-CoS-Prioritätswert)

Der Switch kann Datenverkehr verarbeiten, der von dem Gerät stammt, das an den Zugriffsport am IP-Telefon angeschlossen ist. Sie können die Switch-Ports konfigurieren, die CDP-Pakete senden, die das angeschlossene IP-Telefon anweisen, den Modus (vertrauenswürdiger oder nicht vertrauenswürdiger Modus) für den Zugriffsport auf dem Telefon zu konfigurieren.

Im **vertrauenswürdigen Modus** leitet der Zugriffsport des IP-Telefons den Datenverkehr vom PC unverändert weiter. Im **nicht vertrauenswürdigen Modus** empfängt der Zugriffsport des IP-Telefons den gesamten Datenverkehr in IEEE 802.1Q-Frames, die einen konfigurierten Layer-2-CoS-Wert enthalten. Der standardmäßige CoS-Wert für Layer 2 ist 0. Der nicht vertrauenswürdige Modus ist der Standardwert.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Sprach-VLAN-Funktionen.

Im Switch ist die Sprach-VLAN-Funktion standardmäßig deaktiviert. Wenn Sie das Sprach-VLAN auf dem Port aktivieren, wird der gesamte nicht getaggte Datenverkehr entsprechend der standardmäßigen CoS-Priorität gesendet. Bevor Sie das Sprach-VLAN aktivieren, aktivieren Sie die QoS auf dem Switch, indem Sie den globalen Konfigurationsbefehl **mls qos** ausführen und den Vertrauensstatus des Ports auf **Vertrauenswürdigkeit** konfigurieren, indem Sie den Schnittstellenkonfigurationsbefehl **mls qos trust cos** ausgeben.

Standardmäßig verwirft ein Switch-Port alle getaggten Frames in der Hardware. Um getaggte Frames auf einem Switch-Port zu akzeptieren, muss einer dieser Befehle auf dem Port konfiguriert werden:

- **switchport voice vlan dot1p**
- **switchport voice vlan *V_VLAN_ID***
- **Trunk im Switch-Port-Modus**

Verwenden Sie den Befehl **switchport voice vlan dot1p, um den Switch-Port anzuweisen, das Prioritäts-Tagging IEEE 802.1p zu verwenden, um den gesamten Sprachdatenverkehr mit einer höheren Priorität über das native (Access-)VLAN weiterzuleiten.**

Mit dem Befehl **switchport voice vlan *V_VLAN_ID*** können Sie ein bestimmtes Sprach-VLAN konfigurieren, sodass das IP-Telefon Sprachdatenverkehr in IEEE 802.1Q-Frames mit einem Layer-2-CoS-Wert senden kann. Das Cisco IP-Telefon kann auch nicht getaggten Sprachverkehr senden oder eine eigene Konfiguration verwenden, um Sprachdatenverkehr an das Zugriffs-VLAN des Switches zu senden.

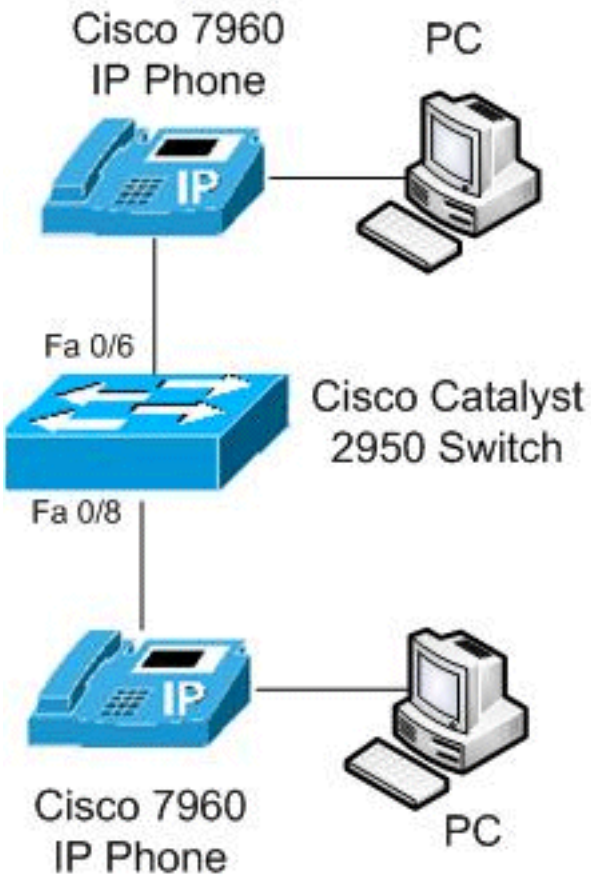
Verwenden Sie den Befehl **switchport priority extends trust (Vertrauensebene), um den Vertrauensstatus auf das mit dem IP-Telefon verbundene Gerät (PC) auszudehnen.** Mit diesem Befehl weist der Switch das Telefon an, wie die Datenpakete von dem Gerät verarbeitet werden, das an den Zugriffsport am Cisco IP-Telefon angeschlossen ist. Von PC generierte Pakete verwenden im 802.1q-Header einen zugewiesenen CoS-Wert. Das Telefon sollte die Priorität von Frames, die vom PC aus am Telefon-Port ankommen, nicht ändern (vertrauenswürdig).

Sie müssen **CDP** auf dem Switch-Port aktivieren, an den das IP-Telefon angeschlossen ist. Standardmäßig ist CDP global auf den Switch-Schnittstellen aktiviert. CDP ist der Mechanismus, der zwischen dem Switch und dem Cisco IP-Telefon verwendet wird, um das Cisco IP-Telefon für die Kommunikation mit dem Switch-Port zu konfigurieren. CDP ist proprietär zu Cisco Systems, und die Telefone anderer Hersteller können diese Methode möglicherweise nicht verwenden, um das IP-Telefon so zu konfigurieren, dass es der Port-Konfiguration des Switches entspricht.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Dieses Diagramm ist ein Beispiel für eine Sprach-VLAN-Konfiguration auf einem Cisco Catalyst 2950 Switch. Die Switch-Ports FastEthernet 0/6 und 0/8 sind mit einem Cisco IP-Telefon verbunden, und der Access-Port auf beiden IP-Telefonen ist mit dem PC verbunden.

Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

Basierend auf einem vertrauenswürdigen CoS-Wert

Im 2950-Switch hat der FastEthernet 0/6-Port **VLAN 10** für Sprach-VLAN mit **dot1p** konfiguriert, um **IEEE 802.1p**-Prioritäts-Tagging für Sprachdatenverkehr zu verwenden, und den **Vertrauensmodus** für Datenverkehr vom PC konfiguriert, der mit dem der an den Zugriffsport des Cisco IP-Telefons-Ports verbunden ist. Hier **vertraut** das Cisco IP-Telefon einem Laptop oder PC über CoS, und der Datenverkehr verwendet **natives VLAN**. Diese Konfiguration wird in der Regel für Management-Workstations, Benutzer mit hoher Priorität oder eine Anwendung mit hohem CoS-Wert verwendet.

Wenn ein Cisco Telefon CDP mit dem Switch ausführt, wird die Vertrauensgrenze immer auf das IP-Telefon ausgedehnt. Das heißt, die Pakete des IP-Telefons werden nie von CoS 5 in den CoS-Standard geändert. Aus diesem Grund **wird** der **Befehl switchport priority extends trust** für den Laptop oder PC verwendet. Sie wird über CDP gesendet, um dem IP-Telefon mitzuteilen, dass Pakete mit hoher Priorität nicht umgeschrieben werden sollen.

Der FastEthernet 0/8-Port ist mit separaten VLANs für den Sprach- und Datenverkehr konfiguriert. In diesem Beispiel wird **VLAN 10** für Sprachdatenverkehr und **VLAN 20** für Datenverkehr verwendet. Diese Konfiguration wird für typische Cisco IP-Telefone verwendet, **ohne** dem Laptop

oder PCs **vertrauen zu müssen**. Der Datenverkehr verwendet den Frame-Typ IEEE 802.1Q.

Mit dem Befehl **mls qos trust cos** überprüft der Port des Catalyst-Switches den CoS-Wert im Ethernet-Header für die Klassifizierung des eingehenden Datenverkehrs und vertraut dem CoS-Wert des getaggten Pakets, der vom Cisco IP-Telefon ausgeht. Standardmäßig wird der Ethernet-Port nicht vertrauenswürdig, sodass der Datenverkehr aus dem Sprach-VLAN und dem Daten-VLAN nicht vertrauenswürdig ist.

Mit dem Befehl **priority-queue out** (**priorisierte Warteschlange ausstellen**) erhalten Sprachpakete direkte Privilegien, wenn versucht wird, Port zu verlassen, der Jitter verhindert. Der Befehl spanning tree portfast entfernt die Schnittstelle aus dem Spanning Tree-Protokoll, und der Befehl bpduguard schützt das Netzwerk, wenn jemand versucht, einen neuen Switch anzuschließen, nachdem er das IP-Telefon abgezogen hat. Wenn ein Switch angeschlossen werden soll, wird der Port deaktiviert. Diese werden in der Regel den Telefonanschlüssen hinzugefügt.

Cisco Catalyst Switch der Serie 2950

```
Switch#configure terminal
Switch(config)#mls qos
Switch(config)#interface fastethernet 0/6

!--- Set the interface to classify incoming traffic
packets by using the packet CoS value. Switch(config-
if)#mls qos trust cos

!--- Configure the phone to use IEEE 802.1p priority
tagging for voice traffic. Switch(config-if)#switchport
voice vlan dot1p
Switch(config-if)#switchport voice vlan 10

!--- Trust the CoS value the PC sends in on the data
VLAN. Switch(config-if)#switchport priority extend trust
Switch(config-if)#priority-queue out
Switch(config-if)#spanning-tree portfast
Switch(config-if)#spanning-tree bpduguard enable
Switch(config-if)#exit


Switch(config)#interface gigabitethernet0/8
Switch(config-if)#mls qos trust cos

!--- Configure specified VLANs for voice and data
traffic. Switch(config-if)#switchport voice vlan 10
Switch(config-if)#switchport access vlan 20

Switch(config-if)#priority-queue out
Switch(config-if)#spanning-tree portfast
Switch(config-if)#spanning-tree bpduguard enable
Switch(config-if)#exit
```

Bei Verwendung eines IP-Telefons eines anderen Anbieters

Wenn Sie ein IP-Telefon verwenden, das nicht von Cisco stammt und das Cisco proprietäre CDP nicht erkennt und automatisch den Trunk-Port einrichtet, müssen Sie den Trunk manuell konfigurieren. In diesem Konfigurationsbeispiel beschränken wir die VLANs auf 10 und 20 und blockieren das native Standard-VLAN 1 oder VLAN 0. **VLAN 10** wird für Sprachdatenverkehr und **VLAN 20** für Datenverkehr verwendet. Das IP-Telefon eines anderen Anbieters erhält das richtige

VLAN für seine getaggten Pakete durch manuelle Konfiguration oder über die TFTP-Datei, die es beim Hochfahren herunterlädt. In diesem Beispiel wird diese Konfiguration verwendet:

Cisco Catalyst Switch der Serie 2950

```
Switch#configure terminal
Switch(config)#interface fastethernet 0/6

!---Trusts tagged packets CoS value; all untagged
packets reset DSCP value in IP header to 0.
Switch(config-if)#mls qos trust cos

!--- Turn off DTP (dynamic trunking protocol).
Switch(config-if)#switchport nonegotiate

!--- Forces the port into trunking mode. Switch(config-
if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 20

!--- Restricts the VLANs. Switch(config-if)#switchport
trunk allowed vlans 10,20
Switch(config-if)#priority-queue out
Switch(config-if)#spanning-tree portfast trunk
Switch(config-if)#spanning-tree bpduguard enable
Switch(config-if)#exit
```

Basierend auf einem vertrauenswürdigen DSCP-Wert im IP-Header

Hier verwenden wir statt eines CoS-Werts einen vertrauenswürdigen DSCP-Wert (DiffService Code Points), da CoS die Bedeutung des Pakets anhand seines L2-Headers nachvollziehen kann. DSCP ist ein 6-Bit-Feld innerhalb des IP-Pakets. Verwenden Sie den **Befehl mls qos trust DSCP, um den DSCP-Wert im IP-Header zu vertrauen.** In diesem Fall legt das IP-Telefon sein DSCP korrekt in seine Pakete ein, und das Laptop legt sein DSCP korrekt fest. In diesem Beispiel wird diese Konfiguration verwendet:

Cisco Catalyst Switch der Serie 2950

```
Switch#configure terminal
Switch(config)#interface fastethernet 0/6

!---Trust the DSCP value in the IP header.
Switch(config-if)#mls qos trust DSCP

!--- IP phone VLAN Switch(config-if)#switchport voice
vlan 10
Switch(config-if)#switchport access vlan 20

!--- Trust the DSCP value the PC sends in on the data
VLAN. Switch(config-if)#switchport priority extend trust
Switch(config-if)#priority-queue out
Switch(config-if)#spanning-tree portfast
Switch(config-if)#spanning-tree bpduguard enable
Switch(config-if)#exit
```

Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- Mit dem Befehl **show interfaces *interface-id* switchport** überprüfen Sie Ihre Sprach-VLAN-Konfiguration.Beispiele:

```
Switch#show interfaces FastEthernet 0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: dot1p
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: trusted
```

- Verwenden Sie den Befehl **show running-config interface *interface-id*, um Ihre Sprach-VLAN-Einträge für eine bestimmte Schnittstelle zu überprüfen.**Beispiele:

```
Switch#show running-config interface fastEthernet 0/6
Building configuration...

Current configuration : 139 bytes
!
interface FastEthernet0/6
 switchport voice vlan dot1p
 switchport voice vlan 10
 switchport priority extend trust
 mls qos trust cos
 priority-queue out
 spanning-tree portfast
 spanning-tree bpduguard enable
end

Switch#show running-config interface fastEthernet 0/8
Building configuration...

Current configuration : 137 bytes
!
interface FastEthernet0/8
 switchport voice vlan 10
 switchport access vlan 20
 mls qos trust cos
 priority-queue out
 spanning-tree portfast
 spanning-tree bpduguard enable
```

```
end
```

Zugehörige Informationen

- Support-Seite für Cisco Catalyst Switches der Serie 2950
- Support-Seite für Cisco Catalyst Switches der Serie 2960
- Produkt-Support für Switches
- Support für LAN-Switching-Technologie
- Technischer Support und Dokumentation für Cisco Systeme