

# Konfigurieren der VLAN-Schnittstelleneinstellungen (Virtual Local Area Network) auf einem Cisco Switch der Serie Business 350

## Ziel

Mit einem Virtual Local Area Network (VLAN) können Sie ein Local Area Network (LAN) logisch in verschiedene Broadcast-Domänen segmentieren. In Umgebungen, in denen über das Netzwerk möglicherweise vertrauliche Daten übertragen werden, kann durch die Erstellung von VLANs die Sicherheit verbessert werden. Eine Übertragung kann dann auf ein spezifisches VLAN beschränkt werden. Nur die Benutzer, die zu einem VLAN gehören, können auf die Daten in diesem VLAN zugreifen und sie ändern. Mithilfe von VLANs kann auch die Leistung verbessert werden, da Broadcasts und Multicasts seltener an unnötige Ziele gesendet werden müssen.

Sie können ein VLAN erstellen, dies hat jedoch keine Auswirkungen, bis das VLAN mindestens einem Port entweder manuell oder dynamisch angeschlossen ist. Ports müssen immer einem oder mehreren VLANs angehören.

Jedes VLAN muss mit einer eindeutigen VLAN-ID (VID) mit einem Wert zwischen 1 und 4094 konfiguriert werden. Das Gerät behält sich die VID 4095 als Discard-VLAN vor. Alle dem Discard VLAN klassifizierten Pakete werden beim Eingang verworfen und nicht an einen Port weitergeleitet.

Dieser Artikel enthält Anweisungen zum Konfigurieren der VLAN-Schnittstelleneinstellungen auf einem Cisco Business-Switch der Serie 350.

## Unterstützte Geräte | Softwareversion

- CBS 350 ([Datenblatt](#)) | 3.0.0.69 ([Laden Sie die aktuelle Version herunter](#))
- CBS350-2X ([Datenblatt](#)) | 3.0.0.69 ([Laden Sie die aktuelle Version herunter](#))
- CBS350-4X ([Datenblatt](#)) | 3.0.0.69 ([Laden Sie die aktuelle Version herunter](#))

## Konfigurieren der VLAN-Schnittstelleneinstellungen auf einem Switch

**Wichtig:** Bevor Sie mit den Schritten unten fortfahren, stellen Sie sicher, dass VLANs auf dem Switch konfiguriert wurden. Um zu erfahren, wie Sie die VLAN-Einstellungen auf Ihrem Switch konfigurieren, klicken Sie [hier](#), um Anweisungen zu erhalten.

### Schritt 1

Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **VLAN Management > Interface Settings** aus.



## Schritt 2

Wählen Sie in der Dropdown-Liste Schnittstellentyp eine Schnittstelle aus, und klicken Sie auf **Los**, um eine Liste der Ports oder LAGs auf der Schnittstelle zu füllen.

- Port - Wählen Sie in der Dropdown-Liste "Schnittstellentyp" die Option Port aus, wenn nur ein Port ausgewählt werden muss.
- LAG: Wählen Sie in der Dropdown-Liste "Schnittstellentyp" die zu konfigurierende LAG aus. Dies betrifft die in der LAG-Konfiguration definierte Portgruppe.

## Interface Settings Table



Filter: *Interface Type* equals to

Port of Unit 1 ▾

Port of Unit 1

LAG

erface

1

2

Go

## Schritt 3

Klicken Sie auf das Optionsfeld für den Port oder die LAG, den Sie ändern möchten. Klicken Sie auf das **Bearbeitungssymbol**.

## Interface Settings Table



Filter: *Interface Type* equals to

Port of Unit 1 ▾

Go

Entry No.

Interface

Switchport Mode

Interface  
VLAN Mode

1



1

GE1

Layer 2

Access

## Schritt 3

Klicken Sie im Dropdown-Menü auf das Optionsfeld für den gewünschten VLAN-Modus für die Schnittstelle.

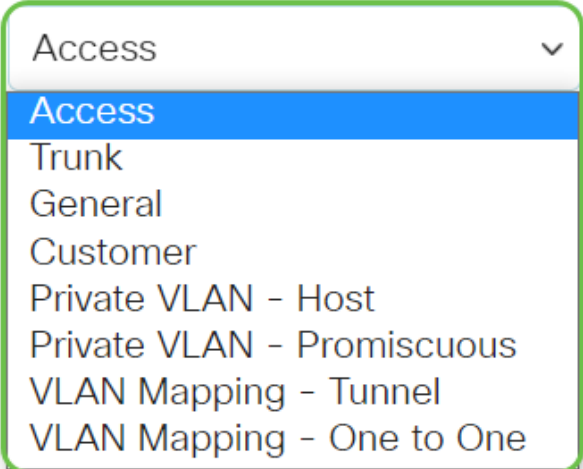
## Edit Interface Settings

Interface:  Unit  Port   LAG

Switchport Mode:  Layer 2  
 Layer 3

Interface VLAN Mode:

Ethertype Tagging:



- Access (Zugriff): Die Schnittstelle ist ein nicht markiertes Mitglied eines einzelnen VLANs. Wenn diese Option ausgewählt ist, fahren Sie mit [Schritt 10 fort](#).
- Trunk - Die Schnittstelle ist ein nicht markiertes Mitglied von maximal einem VLAN und ein markiertes Mitglied von einem oder mehreren VLANs. Wenn diese Option ausgewählt ist, fahren Sie mit [Schritt 10 fort](#).
- Allgemein - Die Schnittstelle kann ein markiertes oder nicht markiertes Mitglied eines oder mehrerer VLANs sein.
- Kunde - Die Schnittstelle befindet sich im Q-in-Q-Modus. Auf diese Weise kann der Verbindungspartner seine eigenen VLAN-Vereinbarungen im gesamten Anbieternetzwerk nutzen. Wenn diese Option ausgewählt ist, fahren Sie mit [Schritt 10 fort](#).
- Private VLAN - Host (Privates VLAN - Host): Mit dieser Option wird die Schnittstelle entweder als isoliert oder als Community festgelegt. Sie können dann entweder ein isoliertes oder ein Community-VLAN im sekundären VLAN - Host-Bereich auswählen.
- Private VLAN - Promiscuous (Privates VLAN - Promiscuous): Diese Option legt die Schnittstelle als Promiscuous fest.
- VLAN Mapping (VLAN-Zuordnung) - Tunnel (Tunnel): Wählen Sie diese Option aus, um die Schnittstelle als VLAN-Tunnel-Edge-Port festzulegen.
- VLAN-Zuordnung - Eins zu Eins - Wählen Sie diese Option aus, um die Schnittstelle als VLAN festzulegen, das einem Edge-Port zugeordnet wird.

### Schritt 4 (optional)

Wählen Sie im Feld *Ethertype Tagging* eine Ether-type-Tagging-Methode für das S-VLAN-Tag aus.

- Ether-type Tagging:
- Use Global Setting (Dot1q)
  - Dot1q - 8100
  - Dot1ad - 88a8
  - 9100
  - 9200

#### Schritt 5 (optional)

Klicken Sie auf das Optionsfeld für den gewünschten Rahmentyp, den die Schnittstelle empfangen kann. Frames, die nicht diesen Frame-Typ darstellen, werden beim Eingang verworfen. Diese Optionen sind nur im *allgemeinen Modus* verfügbar.

Frame Type:

- Admit All
- Admit Tagged Only
- Admit Untagged Only

- Admit All (Alle zulassen) - Die Schnittstelle akzeptiert alle Frames (nicht getaggte, getaggte und priorisierte getaggte Frames).
- Admit Tagged Only (Nur zugewiesen): Die Schnittstelle akzeptiert nur markierte Frames.
- Nur Untagged zulassen - Die Schnittstelle akzeptiert nur nicht getaggte und mit Priorität gekennzeichnete Frames.

#### Schritt 6 (optional)

Aktivieren Sie **Aktivieren**, um die Eingangsfiltrierung auf der Schnittstelle zu aktivieren. Wenn die Eingangsfiltrierung aktiviert ist, verwirft die Schnittstelle alle eingehenden Frames, die als VLANs klassifiziert sind, zu denen die Schnittstelle nicht gehört. Dies ist nur im *allgemeinen Modus* verfügbar.

Ingress Filtering:

Enable

#### Schritt 7 (optional)

Wählen Sie das primäre VLAN aus der Dropdown-Liste Primary VLAN (Primäres VLAN) aus. Das primäre VLAN wird verwendet, um Layer-2-Verbindungen von Promiscuous-Ports zu isolierten

Ports und zu Community-Ports zu ermöglichen.

**Hinweis:** Alternativ können Sie diese Option leer lassen, wenn sich die Schnittstelle nicht im privaten VLAN-Modus befindet, und mit [Schritt 10](#) fortfahren.

Primary VLAN:

None ▾

### Schritt 8 (optional)

Wählen Sie ein isoliertes oder ein Community-VLAN für Hosts aus, die nur ein einzelnes sekundäres VLAN benötigen.

Secondary VLAN - Host:

110

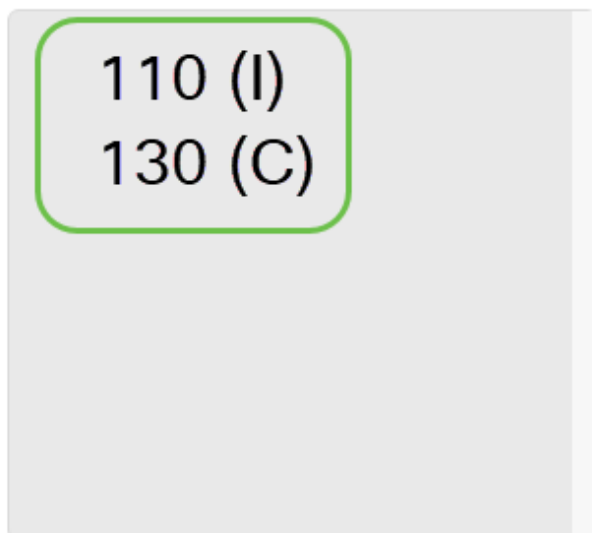
**Hinweis:** Die Dropdown-Liste Sekundäres VLAN - Host ist nur verfügbar, wenn Private VLAN - Host ausgewählt wurde. Um zu erfahren, wie private VLAN-Einstellungen auf einem Switch konfiguriert werden, klicken Sie [hier](#), um Anweisungen zu erhalten.

### Schritt 9 (optional)

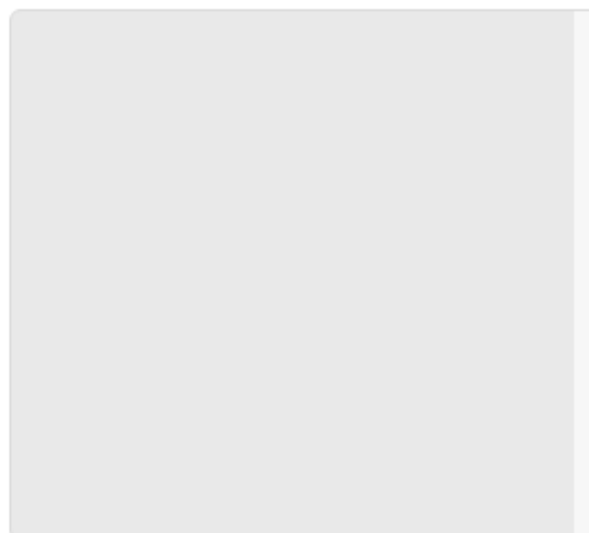
Verschieben Sie bei Promiscuous-Ports alle sekundären VLANs, die für die normale Paketweiterleitung erforderlich sind, aus den verfügbaren sekundären VLANs, und klicken Sie dann auf die > Schaltfläche. Promiscuous- und Trunk-Ports können Mitglieder in mehreren VLANs sein.

**Hinweis:** Diese Bereiche sind nur verfügbar, wenn Private VLAN - Promiscuous ausgewählt wurde.

Available Secondary VLANs:



Selected Secondary VLANs:

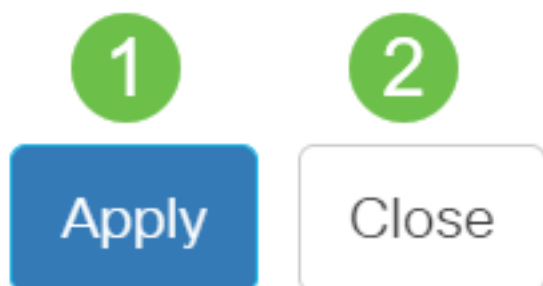


Legend: I - Isolated C - Community

Um zu erfahren, wie private VLAN-Einstellungen auf einem Switch konfiguriert werden, klicken Sie [hier](#), um Anweisungen zu erhalten.

#### Schritt 10

Klicken Sie auf **Übernehmen** und dann auf **Schließen**.



#### **Schritt 11**

Klicken Sie auf **Speichern**, um die Einstellungen in der Startkonfigurationsdatei zu speichern.



Sie sollten jetzt die VLAN-Schnittstelleneinstellungen auf Ihrem Cisco Business Switch der Serie 350 konfiguriert haben.