

Best Practices und Sicherheitstipps für VLAN bei Cisco Business Routern

Ziel

In diesem Artikel werden die Konzepte und Schritte zur Umsetzung von Best Practices und Sicherheitstipps beim Konfigurieren von VLANs auf Cisco Business-Geräten erläutert.

Inhalt

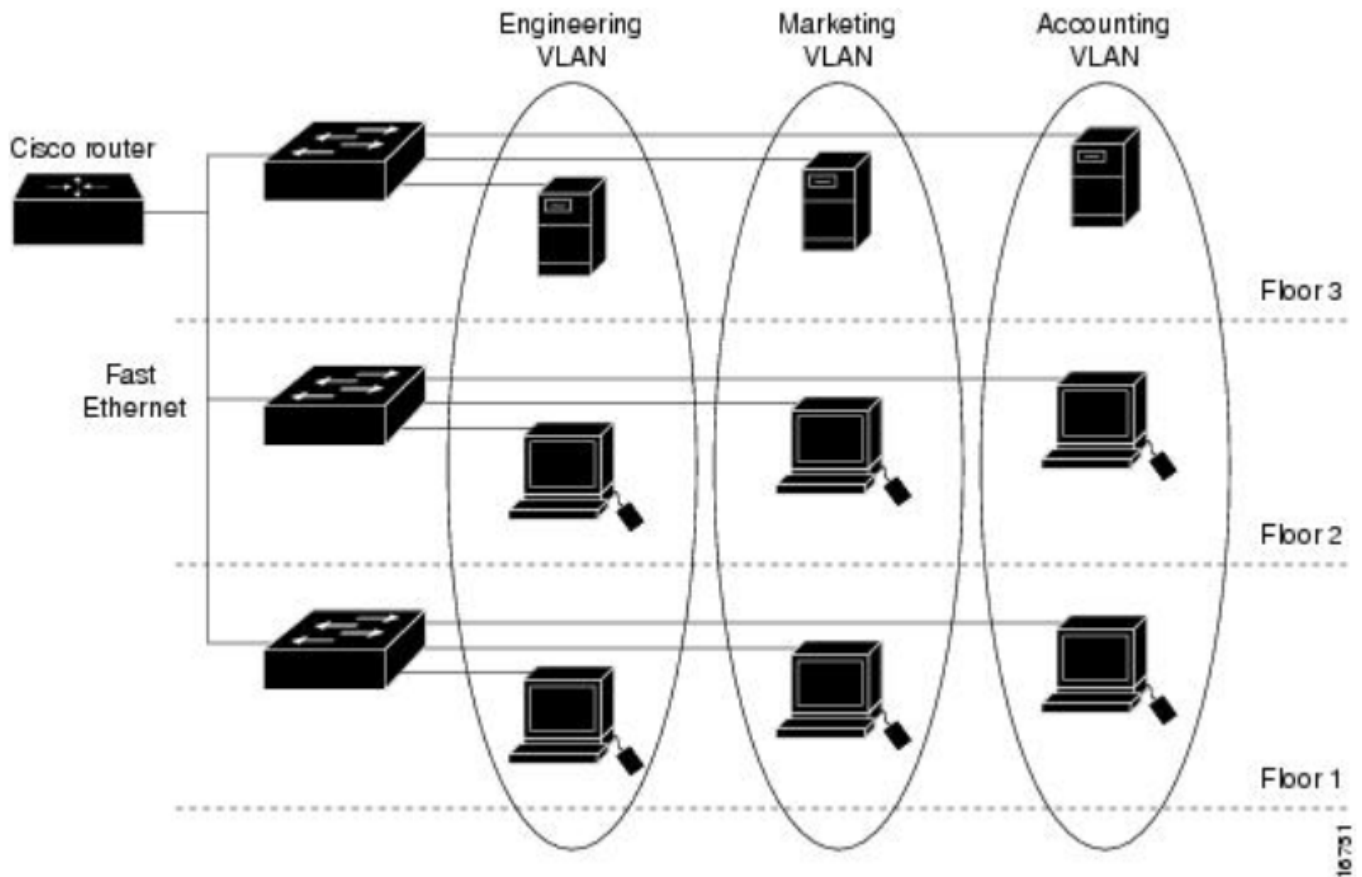
- [Die wichtigsten Begriffe für Einsteiger](#)
- [Best Practice 1: VLAN-Port-Zuweisung Grundlagen zur Portzuweisung Konfigurieren von Access-Ports Konfigurieren von Trunk-Ports Häufig gestellte Fragen](#)
- [Best Practice 2: Standard-VLAN 1 und nicht verwendete Ports Häufig gestellte Fragen](#)
- [Best Practice 3: Erstellen eines „Dead End“-VLAN für nicht verwendete Ports](#)
- [Best Practice 4: IP-Telefone in einem VLAN](#)
- [Best Practice 5: Inter-VLAN-Routing](#)

Einleitung

Möchten Sie die Effizienz Ihres Unternehmensnetzwerks erhöhen, ohne bei der Sicherheit Kompromisse einzugehen? Eine Möglichkeit dafür ist die korrekte Einrichtung von Virtual Local Area Networks (VLANs).

Ein VLAN ist eine logische Gruppe von Workstations, Servern und Netzwerkgeräten, die trotz ihrer geografischen Verteilung zum selben Local Area Network (LAN) gehören. Kurz gesagt: Wenn die Hardware in denselben VLANs platziert ist, kann der Datenverkehr zwischen den Geräten besser getrennt und geschützt werden.

Angenommen, Sie haben eine Technik-, eine Marketing- und eine Buchhaltungsabteilung. Die Mitarbeiter der einzelnen Abteilungen sind über die verschiedenen Etagen des Gebäudes verteilt, müssen aber dennoch auf Informationen aus ihrer Abteilung zugreifen und diese innerhalb der Abteilung weitergeben können. Dies ist für die gemeinsame Nutzung von Dokumenten und Webdiensten unerlässlich.



VLANs müssen unter Berücksichtigung von Best Practices eingerichtet werden, um die Sicherheit Ihres Netzwerks zu gewährleisten. Beachten Sie beim Einrichten von VLANs die unten genannten bewährten Tipps. Sie werden es nicht bereuen!

Unterstützte Geräte

- RV042
- RV110W
- RV130
- RV132
- RV134W
- RV160W
- RV215W
- RV260
- RV260P
- RV260W
- RV320
- RV325
- RV340
- RV340W
- RV345
- RV345P

Möglicherweise ist es für Sie relevant zu wissen, dass die Router der RV160- oder RV260-Serie bis zu 16 VLANs unterstützen, während die Router der RV34x-Serie bis zu 32 VLANs unterstützen. Beim RV320 werden bis zu 7 VLANs unterstützt. Wie viele VLANs Ihr Router unterstützt, können Sie dem Datenblatt zum jeweiligen Modell auf der [Cisco Website](#) entnehmen. Wählen Sie **Support** aus, und geben Sie die Modellnummer ein, oder suchen Sie einfach nach

dem Datenblatt und der Modellnummer.

Die wichtigsten Begriffe für Einsteiger

Access-Port: Ein Access-Port leitet Datenverkehr für ein bestimmtes VLAN weiter. Access-Ports werden häufig als ungetaggte Ports bezeichnet, da an einem Port jeweils nur ein VLAN vorhanden ist und Datenverkehr ohne Tags weitergeleitet werden kann.

Trunk-Port: Ein Port auf einem Switch, der Datenverkehr für mehr als ein VLAN weiterleitet. Trunk-Ports werden häufig als getaggte Ports bezeichnet, da an einem Port mehr als ein VLAN vorhanden ist und der Datenverkehr für alle außer einem VLAN getaggt werden muss.

Natives VLAN: Das einzige VLAN an einem Trunk-Port, das kein Tag erhält. Jeglicher Datenverkehr ohne Tag wird an das native VLAN gesendet. Aus diesem Grund muss sichergestellt sein, dass auf beiden Seiten eines Trunks dasselbe native VLAN vorhanden ist, da der Datenverkehr sonst nicht an die richtige Stelle weitergeleitet wird.

Best Practice 1: VLAN-Port-Zuweisung

Grundlagen zur Portzuweisung

- Jeder LAN-Port kann als Access-Port oder Trunk-Port eingerichtet werden.
- VLANs, die nicht für den Trunk verwendet werden sollen, müssen ausgeschlossen werden.
- Ein VLAN kann an mehr als einem Port platziert werden.

Konfigurieren von Access-Ports

- An einem LAN-Port wird ein einziges VLAN zugewiesen.
- Das VLAN, dem dieser Port zugewiesen ist, sollte als *ungetaggt gekennzeichnet werden*.
- Alle anderen VLANs sollten für diesen Port als *ausgeschlossen* gekennzeichnet werden.

Um dies ordnungsgemäß festzulegen, navigieren Sie zu **LAN > VLAN Settings** (LAN > VLAN-Einstellungen). Wählen Sie die *VLAN-IDs* aus, und **klicken** Sie auf das Symbol zum *Bearbeiten*. Öffnen Sie das Dropdown-Menü für eine der aufgeführten LAN-Schnittstellen für VLANs, um die VLAN-Tags zu bearbeiten. Klicken Sie auf **Apply** (Anwenden).

In diesem Beispiel ist jedem VLAN ein eigener LAN-Port zugewiesen:

The screenshot shows the 'VLAN Settings' page for a Cisco RV260W router. On the left, a navigation menu has 'LAN' selected (1) and 'VLAN Settings' highlighted (2). The main area displays a table of VLANs:

VLAN ID	Name	Enabled	Port	IP Address	DHCP Server
1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0	fec0::1/64 DHCP Disabled
200	Test	Enabled	Enabled	192.168.2.1/24 255.255.255.0	fec0::1::1/64 DHCP Disabled

Below the table is the 'Assign VLANs to ports' section. It shows a table with columns for VLAN ID and LAN1 through LAN8. For VLAN 1, the assignment for LAN1 is 'Untagged' (4), and a dropdown menu is open (5) showing 'Tagged', 'Untagged', and 'Excluded' options. The 'Apply' button (6) is at the top right.

Dieses Bild der grafischen Benutzeroberfläche (GUI) stammt von einem RV260W-Router. Die angezeigten Optionen können in Ihrem Fall leicht abweichen. Beispiel: Bei der RV34x-Serie wird für die Kennzeichnungen *Untagged* (Ungetaggt), *Excluded* (Ausgeschlossen) und *Tagged* (Getaggt) jeweils nur der erste Buchstaben angegeben. Der Prozess ist dennoch der gleiche.

VLANs to Port Table



VLAN ID LAN1 LAN2 LAN3 LAN4

1



U : Untagged, **T** : Tagged, **E** : Excluded


Konfigurieren von Trunk-Ports

- Zwei oder mehr VLANs teilen sich einen LAN-Port.
- Eines der VLANs kann als *ungetaggt* gekennzeichnet werden.
- Die übrigen VLANs, die Teil des Trunk-Ports sind, müssen als *getaggt* gekennzeichnet werden.
- Die VLANs, die nicht Teil des Trunk-Ports sind, müssen als für diesen Port *ausgeschlossen* gekennzeichnet werden.


In diesem Beispiel befinden sich verschiedene VLANs an Trunk-Ports. Um dies richtig

festzulegen, wählen Sie die zu bearbeitenden *VLAN-IDs* aus. **Klicken** Sie auf das Symbol zum *Bearbeiten*. Nehmen Sie je nach Ihren Anforderungen Änderungen vor. Beachten Sie dabei die oben genannten Empfehlungen. Haben Sie bemerkt, dass VLAN 1 von jedem LAN-Port ausgeschlossen ist? Dies wird im Abschnitt mit der [Best Practice für Standard-VLAN 1](#) erläutert.

Assign VLANs to ports

2 

<input type="checkbox"/>	VLAN ID	LAN1	LAN2	LAN3	LAN4
1 <input checked="" type="checkbox"/>	1	Excluded ▼	Excluded ▼	Excluded ▼	Excluded ▼
<input checked="" type="checkbox"/>	30	Tagged ▼	Tagged ▼	Untaggec ▼	Untaggec ▼
<input checked="" type="checkbox"/>	40	Tagged ▼	Untaggec ▼	Tagged ▼	Untaggec ▼
<input checked="" type="checkbox"/>	50	Untaggec ▼	Tagged ▼	Tagged ▼	Tagged ▼

3 

Häufig gestellte Fragen

Warum bleibt ein VLAN ungetaggt, wenn es das einzige VLAN an diesem Port ist?

Da einem Access-Port nur ein einziges VLAN zugewiesen ist, wird ausgehender Datenverkehr vom Port ohne VLAN-Tag auf den Frames gesendet. Wenn der Frame den Switch-Port erreicht (eingehender Datenverkehr), fügt der Switch das VLAN-Tag hinzu.

Warum werden VLANs getaggt, wenn sie Teil eines Trunks sind?

Dies geschieht, damit passierender Datenverkehr nicht an das falsche VLAN an diesem Port gesendet wird. Die VLANs teilen sich diesen Port. Sie können sich dies vorstellen wie bei einem größeren Wohngebäude, bei dem die Wohnungsnummern Teil der Adresse sind, damit Post richtig zugestellt werden kann.

Warum bleibt der Datenverkehr ungetaggt, wenn er Teil des nativen VLAN ist?

Ein natives VLAN ist eine Möglichkeit, Daten ohne Tag über einen oder mehrere Switches zu übertragen. Der Switch ordnet alle nicht getaggten Frames, die an einem getaggten Port ankommen, dem nativen VLAN zu. Wenn ein Frame im nativen VLAN einen Trunk-Port (getaggt) verlässt, entfernt der Switch das VLAN-Tag.

Warum werden VLANs ausgeschlossen, wenn sie sich nicht am jeweiligen Port befinden?

Dadurch wird der Datenverkehr an diesem Trunk auf die vom Benutzer gewünschten VLANs beschränkt. Dies gilt als Best Practice.

Best Practice 2: Standard-VLAN 1 und nicht verwendete Ports

Alle Ports müssen einem oder mehreren VLANs zugewiesen werden (das native VLAN eingeschlossen). Bei Cisco Business Routern ist VLAN 1 standardmäßig allen Ports zugewiesen.

Ein Management-VLAN ist ein VLAN, das verwendet wird, um die Geräte in Ihrem Netzwerk per Telnet, SSH, SNMP, Syslog oder Cisco FindIT aus der Ferne zu verwalten, zu steuern und zu überwachen. Standardmäßig ist dies auch VLAN 1. Ein bewährtes Sicherheitsverfahren besteht darin, den Management- und Benutzerdatenverkehr zu trennen. Daher wird empfohlen, VLAN 1 beim Konfigurieren von VLANs nur für Managementzwecke zu verwenden.

Um zu Verwaltungszwecken remote mit einem Cisco Switch kommunizieren zu können, muss auf dem Switch eine IP-Adresse im Management-VLAN konfiguriert sein. Benutzer in anderen VLANs können keine Remotezugriffssitzungen zum Switch einrichten, es sei denn, sie werden in das Management-VLAN weitergeleitet, sodass eine zusätzliche Sicherheitsebene gegeben ist. Außerdem sollte der Switch so konfiguriert werden, dass er nur verschlüsselte SSH-Sitzungen für das Remote-Management akzeptiert. Auf der Cisco Community-Website finden Sie unter folgenden Links Diskussionen zu diesem Thema:

- [Management-VLAN – Diskussion 1](#)
- [Management-VLAN – Diskussion 2](#)

Häufig gestellte Fragen

Warum wird VLAN 1 als Standard-VLAN nicht für die virtuelle Segmentierung des Netzwerks empfohlen?

Der Hauptgrund dafür ist, dass Hacker wissen, dass VLAN 1 der Standard ist und häufig verwendet wird. Sie können sich damit per „VLAN-Hopping“ Zugriff auf andere VLANs verschaffen. Wie der Name schon sagt, können Hacker gefälschten Datenverkehr senden, der sich als VLAN 1 ausgibt, was den Zugriff auf Trunk-Ports und damit andere VLANs ermöglicht.

Kann ich einen nicht verwendeten Port dem Standard-VLAN 1 zugewiesen lassen?

Um Ihr Netzwerk zu schützen, sollten Sie dies nicht tun. Es wird empfohlen, alle Ports so zu konfigurieren, dass sie anderen VLANs als dem Standard-VLAN 1 zugeordnet werden.

Ich möchte keines meiner Produktions-VLANs einem nicht verwendeten Port zuweisen. Was kann ich tun?

Es wird empfohlen, gemäß den Anweisungen im nächsten Abschnitt dieses Artikels ein „Dead-End“-VLAN zu erstellen.

Best Practice 3: Erstellen eines „Dead End“-VLAN für nicht verwendete Ports

Schritt 1: Navigieren Sie zu **LAN > VLAN Settings**.

Wählen Sie eine beliebige Zahl für das VLAN aus. Stellen Sie sicher, dass DHCP, Inter-VLAN-Routing und Gerätemanagement in diesem VLAN nicht aktiviert sind. Dadurch sind die anderen VLANs besser geschützt. Weisen Sie nicht verwendete LAN-Ports diesem VLAN zu. Im folgenden Beispiel wurde *VLAN 777* erstellt und *LAN5* zugewiesen. Dies sollte für alle nicht verwendeten LAN-Ports erfolgen.

The screenshot shows a network configuration interface. On the left, a sidebar contains navigation options: LAN (1), Port Settings, VLAN Settings (2), Option 82 Settings, Static DHCP, 802.1X Configuration, Router Advertisement, Wireless, and Routing. The main area displays a table for VLAN configuration. The table has columns for VLAN ID, LAN1, LAN2, LAN3, LAN4, and LAN5. The rows show VLANs 1, 30, 40, and 50, all with 'Excluded' status for LAN1-LAN4 and 'Untagged' for LAN5. A new VLAN '777' is being configured, with a dropdown menu open for its status, showing options: Untagged (selected), Tagged, and Excluded. A '3' is next to the '777' entry, and a '4' is next to the edit icon. A '5' is next to the dropdown menu.

VLAN ID	LAN1	LAN2	LAN3	LAN4	LAN5
1	Untagged	Untagged	Untagged	Untagged	Excluded
30	Tagged	Tagged	Tagged	Tagged	Excluded
40	Tagged	Tagged	Tagged	Tagged	Excluded
50	Tagged	Tagged	Tagged	Tagged	Excluded
777	Excluded	Excluded	Excluded	Excluded	Untagged

Beachten Sie, dass die anderen VLANs von diesem LAN-Port ausgeschlossen sind.

Schritt 2. **Klicken Sie** auf die Schaltfläche *Apply* (Anwenden), um die vorgenommenen Konfigurationsänderungen zu speichern.

Best Practice 4: IP-Telefone in einem VLAN

Für den Sprachverkehr gelten strenge QoS-Anforderungen (Quality of Service). Wenn sich in Ihrem Unternehmen Computer und IP-Telefone im selben VLAN befinden, versucht jedes Gerät, die verfügbare Bandbreite zu nutzen, ohne das andere Gerät zu berücksichtigen. Um diesen Konflikt zu vermeiden, empfiehlt es sich, separate VLANs für den IP-Telefonie-Sprachverkehr und den Datenverkehr zu verwenden. Weitere Informationen zu dieser Konfiguration finden Sie in den folgenden Artikeln und Videos:

- [Cisco Tech Talk: Einrichtung und Konfiguration eines Sprach-VLAN mit Cisco Small Business-Produkten \(Video\)](#)
- [Konfigurieren von Auto-Voice-VLAN mit QoS auf einem Switch der SG500-Serie](#)
- [Konfiguration eines Sprach-VLAN auf den Managed Switches der 200-/300-Serie](#)
- [Cisco Tech Talk: Konfigurieren von Auto-Voice-VLAN auf Switches der SG350- und SG550-Serie \(Video\)](#)

Best Practice 5: Inter-VLAN-Routing

VLANs werden so eingerichtet, dass der Datenverkehr getrennt werden kann. Manchmal müssen VLANs jedoch in der Lage sein, untereinander zu routen. Dies ist Inter-VLAN-Routing und wird in der Regel nicht empfohlen. Wenn dies für Ihr Unternehmen erforderlich ist, richten Sie es so sicher wie möglich ein. Wenn Sie Inter-VLAN-Routing verwenden, stellen Sie sicher, dass der Datenverkehr mithilfe von Zugriffskontrolllisten (Access Control Lists, ACLs) auf Server mit vertraulichen Informationen beschränkt wird.

Mithilfe von ACLs wird eine Paketfilterung durchgeführt, um den Weg von Paketen durch ein Netzwerk zu steuern. Die Paketfilterung bietet Sicherheit, indem sie den Zugang von Datenverkehr zu einem Netzwerk beschränkt, den Zugriff von Benutzern und Geräten auf ein Netzwerk beschränkt und verhindert, dass Datenverkehr ein Netzwerk verlässt. IP-Zugriffslisten reduzieren die Wahrscheinlichkeit von Spoofing und Denial-of-Service-Angriffen und ermöglichen dynamischen, temporären Benutzerzugriff durch eine Firewall.

- [Inter-VLAN-Routing auf einem RV34x-Router mit gezielten ACL-Einschränkungen](#)

- [Cisco Tech Talk: Konfigurieren von Inter-VLAN-Routing auf Switches der SG250-Serie \(Video\)](#)
- [Cisco Tech Talk: Inter-VLAN-Konfiguration auf RV180 und RV180W \(Video\)](#)
- [Inter-VLAN-Zugriffsbeschränkung bei RV34x \(Bugfix CSCvo92300\)](#)

Schlussfolgerung

Jetzt kennen Sie einige Best Practices für die Einrichtung sicherer VLANs. Beachten Sie diese Tipps, wenn Sie VLANs für Ihr Netzwerk konfigurieren. Nachfolgend sind einige Artikel aufgeführt, die Schritt-für-Schritt-Anweisungen enthalten. Diese unterstützen Sie beim Erstellen eines produktiven, effizienten Netzwerks, das genau zu Ihrem Unternehmen passt.

- [Konfigurieren der VLAN-Einstellungen auf RV160 und RV260](#)
- [Konfigurieren von Einstellungen für ein virtuelles LAN \(VLAN\) auf einem Router der RV34x-Serie](#)
- [Konfigurieren der VLAN-Zugehörigkeit auf RV320- und RV325-VPN-Routern](#)
- [Konfigurieren der Zugehörigkeit zu virtuellen LANs \(VLANs\) auf einem Router der RV-Serie](#)
- [Konfigurieren der IPv4-Adresse der VLAN-Schnittstelle auf einem Sx350- oder SG350X-Switch über die CLI](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.