

Beste praktijken en security tips voor Cisco Business-routers bij gebruik van VLAN's

Doel

Het doel van dit artikel is om de concepten en stappen voor het uitvoeren van best practices en security tips bij het configureren van VLAN's op Cisco Business-apparatuur uit te leggen.

Inhoud

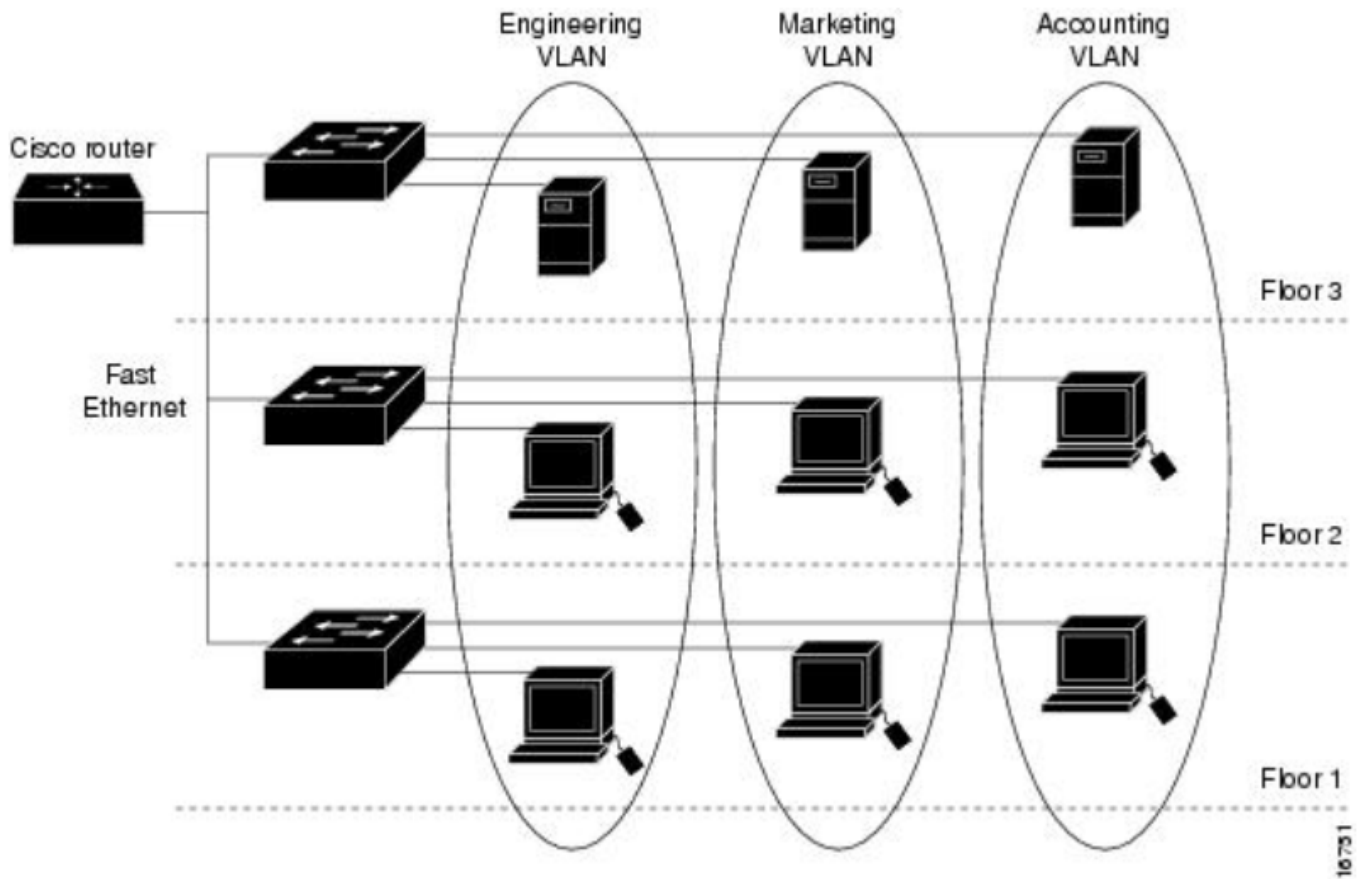
- [Uitleg over enkele termen voor onervaren gebruikers](#)
- [Best practice 1 - Toewijzing van VLAN-poorten De grondbeginselen van het toewijzen van poorten Toegangspoorten configureren Trunkpoorten configureren Veelgestelde vragen](#)
- [Best practice 2 - Het standaard-VLAN VLAN 1 en ongebruikte poorten Veelgestelde vragen](#)
- [Best practice 3 - Een doodlopend VLAN maken voor ongebruikte poorten](#)
- [Best practice 4 - IP-telefoons op een VLAN](#)
- [Best practice 5 - Routing tussen VLAN's](#)

Inleiding

Wilt u uw bedrijfsnetwerk efficiënter maken en tegelijkertijd veilig houden? Een van de manieren om dit te doen, is door op de juiste manier VLAN's (Virtual Local Area Network) in te stellen.

Een VLAN is een logische groep werkstations, servers en netwerkapparaten die zich ondanks hun geografische spreiding in hetzelfde LAN (Local Area Network) lijken te bevinden. Wanneer hardware zich in hetzelfde VLAN bevindt, is het mogelijk om het verkeer tussen apparatuur gescheiden en veiliger te houden.

Binnen uw organisatie kunnen bijvoorbeeld de afdelingen Engineering, Marketing en Accounting bestaan. Werknemers van deze afdelingen werken op verschillende verdiepingen van het gebouw, maar ze moeten nog steeds toegang hebben tot en communiceren over informatie binnen hun eigen afdeling. VLAN's zijn essentieel voor het delen van documenten en webservices.



Maak bij het configureren van VLAN's gebruik van best practices om uw netwerk veilig te houden. Maak de volgende slimme keuzes bij het instellen van VLAN's. U zult er geen spijt van krijgen.

Toepasselijke apparaten

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

Het is misschien interessant om te weten dat de RV160 of RV260 Series routers maximaal zestien VLAN's kunnen verwerken terwijl de RV34x Series routers maximaal 32 VLAN's ondersteunen. De RV320 ondersteunt tot zeven VLAN's. Als u wilt weten hoeveel VLAN's uw router kan verwerken, raadpleegt u het gegevensblad voor uw specifieke model op de [Cisco-website](#). Selecteer **Support** en voer uw modelnummer in of voer een zoekopdracht voor het gegevensblad en modelnummer uit.

Uitleg over enkele termen voor onervaren gebruikers

Toegangspoort: een toegangspoort verwerkt verkeer voor slechts één VLAN. Toegangspoorten worden vaak aangeduid als poorten zonder tags omdat er slechts één VLAN op die poort aanwezig is en het verkeer zonder tags kan worden doorgevoerd.

Trunkpoort: een poort op een switch die verkeer voor meerdere VLAN's verwerkt. Trunkpoorten worden vaak aangeduid als getagde poorten omdat er meerdere VLAN's op die poort aanwezig zijn en het verkeer voor alle VLAN's, op één na, moet worden getagd.

Native VLAN: het ene VLAN in een trunkpoort dat geen tag ontvangt. Verkeer zonder tags wordt verzonden naar het native VLAN. Daarom moeten beide zijden van een trunk hetzelfde native VLAN hebben om ervoor te zorgen dat verkeer op de juiste plek terechtkomt.

Best practice 1 - Toewijzing van VLAN-poorten

De grondbeginselen van het toewijzen van poorten

- Elke LAN-poort kan als toegangspoort of trunkpoort worden ingesteld.
- U kunt de VLAN's uitsluiten die u niet op de trunk wilt hebben.
- Een VLAN kan in meerdere poorten worden geplaatst.

Toegangspoorten configureren

- Eén VLAN toegewezen op een LAN-poort
- Het VLAN waaraan deze poort wordt toegewezen, moet worden gelabeld als *Untagged* (*Zonder tag*)
- Alle andere VLAN's moeten voor die poort worden gelabeld als *Excluded* (*Uitgesloten*)

Geef deze instellingen op via **LAN > VLAN Settings** (LAN > VLAN-instellingen). Selecteer de *VLAN-id's* en klik op het pictogram *edit* (bewerken). Selecteer het vervolgkeuzemenu voor een van de LAN-interfaces voor weergegeven VLAN's om de VLAN-tagging te bewerken. Klik op **Apply** (Toepassen).

Bekijk dit voorbeeld waarin aan elk VLAN een eigen LAN-poort is toegewezen:

The screenshot shows the 'VLAN Settings' page for a Cisco RV260W router. On the left, a navigation menu has 'LAN' (1) and 'VLAN Settings' (2) highlighted. The main area contains 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 features a table with columns for VLAN ID and LAN1 through LAN8. VLANs 1 and 200 are checked. For each LAN port, there is a dropdown menu for tagging. For LAN1, the dropdown is open, showing options: Untagged, Tagged, Tagged, and Excluded. The 'Apply' button (6) is in the top right corner.

Deze afbeelding van een grafische gebruikersinterface (GUI) is afkomstig van een RV260W router. Uw opties kunnen licht afwijken. Op RV34x Series routers worden de labels *Untagged* (Zonder tag), *Excluded* (Uitgesloten) en *Tagged* (Getagd) afgekort tot alleen de eerste letter. Het proces is wel hetzelfde.

VLANs to Port Table



VLAN ID	LAN1	LAN2	LAN3	LAN4
1	U ▼	U ▼	U ▼	U ▼



U : Untagged, T : Tagged, E : Excluded


Trunkpoorten configureren

- Twee of meer VLAN's delen één LAN-poort
- Een van de VLAN's kan zijn gelabeld als *Untagged* (Zonder tag).
- De overige VLAN's die onderdeel zijn van de trunkpoort moeten zijn gelabeld als *Tagged* (Getagd).
- De VLAN's die niet onderdeel zijn van de trunkpoort moeten voor die poort zijn gelabeld als *Excluded* (Uitgesloten).

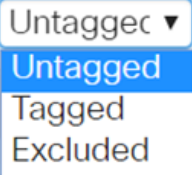
Bekijk dit voorbeeld van verschillende VLAN's die zich allemaal op trunkpoorten bevinden. U stelt

deze correct in door de *VLAN-id's* te selecteren die moeten worden bewerkt. **Klik** op het pictogram *edit* (bewerken). Volg de bovenstaande aanbevelingen om de VLAN's te wijzigen op basis van uw behoeften. Is het u ook opgevallen dat VLAN 1 is uitgesloten van elke LAN-poort? Dit wordt uitgelegd in de sectie [Best practice voor het standaard-VLAN VLAN 1](#).

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 

Veelgestelde vragen

Waarom blijft een VLAN zonder tags wanneer dit het enige VLAN op die poort is?

Aangezien er slechts één VLAN is toegewezen op een toegangspoort, wordt het uitgaande verkeer van de poort verzonden zonder VLAN-tag op de frames. Wanneer het frame de switchpoort (inkomend verkeer) bereikt, voegt de switch de VLAN-tag toe.

Waarom worden VLAN's getagd als ze onderdeel zijn van een trunk?

Dit wordt gedaan om te voorkomen dat doorgelaten verkeer naar het verkeerde VLAN op die poort wordt gestuurd. De VLAN's delen die poort. De manier waarop is vergelijkbaar met appartementnummers die aan een adres worden toegevoegd om ervoor te zorgen dat de post naar het juiste appartement in dat gedeelte gebouw gaat.

Waarom wordt verkeer niet getagd als dit onderdeel is van het native VLAN?

Een native VLAN is een manier om verkeer zonder tags via een of meer switches te verwerken. De switch wijst frames zonder tags die binnenkomen op een getagde poort toe aan het native VLAN. Als een frame op het native VLAN een trunkpoort (getagd) verlaat, verwijdert de switch de VLAN-tag.

Waarom worden VLAN's uitgesloten als ze zich niet op die poort bevinden?

Hierdoor blijft het verkeer alleen op die trunk voor de VLAN's die de gebruiker specifiek wil. Dit wordt beschouwd als een best practice.

Best practice 2 - Het standaard-VLAN VLAN 1 en ongebruikte poorten

Alle poorten moeten aan een of meer VLAN's worden toegewezen, inclusief het native VLAN. Op Cisco Business-routers is VLAN 1 standaard toegewezen aan alle poorten.

Een beheer-VLAN is het VLAN dat wordt gebruikt om de apparaten in uw netwerk extern te beheren, te bewaken en te monitoren met Telnet, SSH, SNMP, syslog of Cisco's FindIT. Standaard is dit ook VLAN 1. Vanuit het oogpunt van security is het een goed idee om het beheer en het dataverkeer van gebruikers te scheiden. Daarom wordt u aangeraden VLAN 1 alleen voor beheerdoeleinden te gebruiken bij het configureren van VLAN's.

Als u voor beheerdoeleinden extern met een Cisco-switch wilt kunnen communiceren, moet de switch een IP-adres hebben dat op het beheer-VLAN is geconfigureerd. Gebruikers in andere VLAN's kunnen in dat geval geen sessies voor externe toegang met de switch tot stand brengen, tenzij ze in het beheer-VLAN worden gerouteerd, wat een extra security laag oplevert. Daarnaast moet de switch worden geconfigureerd om alleen versleutelde SSH-sessies voor extern beheer te accepteren. Klik op de volgende links naar de Cisco Community-website voor meer informatie over dit onderwerp:

- [Discussie 1 over beheer-VLAN's](#)
- [Discussie 2 over beheer-VLAN's](#)

Veelgestelde vragen

Waarom wordt het standaard-VLAN VLAN 1 niet aanbevolen om uw netwerk virtueel te segmenteren?

De belangrijkste reden is dat kwaadwillenden weten dat VLAN 1 het standaard-VLAN is en vaak wordt gebruikt. Ze kunnen deze kennis gebruiken om toegang tot andere VLAN's te krijgen door middel van 'VLAN hopping'. De kwaadwillende kan in dat geval gespoofd verkeer dat zich voordoet als VLAN 1 verzenden om toegang te krijgen tot trunkpoorten en daarmee ook andere VLAN's.

Kan ik een ongebruikte poort toegewezen laten aan het standaard-VLAN VLAN 1?

Als u uw netwerk veilig wilt houden, moet u dat niet doen. Het is raadzaam om al deze poorten zo te configureren dat ze worden gekoppeld aan andere VLAN's dan het standaard-VLAN VLAN 1.

Ik wil mijn productie-VLAN's niet toewijzen aan een ongebruikte poort. Wat kan ik doen?

U wordt aangeraden een doodlopend VLAN te maken volgens de instructies in de volgende sectie van dit artikel.

Best practice 3 - Een doodlopend VLAN maken voor ongebruikte poorten

Stap 1. Ga naar **LAN > VLAN Settings** (LAN > VLAN-instellingen).

Kies een willekeurig nummer voor het VLAN. Op dit VLAN moeten de opties voor DHCP, routing tussen VLAN's en apparaatbeheer niet zijn ingeschakeld. Zo blijven de andere VLAN's beter beveiligd. Gebruik een ongebruikte LAN-poort voor dit VLAN. In het onderstaande voorbeeld is VLAN 777 gemaakt en toegewezen aan LAN5. Dit moet worden gedaan met alle ongebruikte LAN-poorten.

The screenshot shows the configuration page for LAN settings. On the left sidebar, 'LAN' is selected (1), and 'VLAN Settings' is highlighted (2). The main table (4) lists VLANs 1, 30, 40, 50, and 777. The '777' VLAN is selected (3) and its configuration is shown in a dropdown menu (5) with 'Untagged' selected. The table columns are VLAN ID, LAN1, LAN2, LAN3, LAN4, and LAN5.

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	Untagged	Excluded	Excluded	Excluded	Excluded

De andere VLAN's worden uitgesloten van deze LAN-poort.

Stap 2. Klik op de knop *Apply* (Toepassen) om uw configuratiewijzigingen op te slaan.

Best practice 4 - IP-telefoons op een VLAN

Voor spraakverkeer gelden strenge QoS-vereisten (Quality of Service). Als uw bedrijf computers en IP-telefoons op hetzelfde VLAN gebruikt, proberen beide apparaattypen de beschikbare bandbreedte te gebruiken zonder rekening te houden met het andere apparaattype. Om dit conflict te vermijden, is het een goed idee om afzonderlijke VLAN's te gebruiken voor spraakverkeer voor IP-telefonie en dataverkeer. Bekijk de volgende artikelen en video's voor meer informatie over deze configuratie:

- [Cisco Tech Talk: Voice VLAN Setup and Configuration Using Cisco Small Business Products \(video\) \(Installatie en configuratie van spraak-VLAN met Cisco Small Business-producten\)](#)
- [Configuring Auto Voice VLAN with QoS on the SG500 Series Switch \(Automatische spraak-VLAN met QoS configureren op de SG500 Series switch\)](#)
- [Voice VLAN Configuration on the 200/300 Series Managed Switches \(Configuratie van spraak-VLAN op de 200/300 Series beheerde switches\)](#)
- [Cisco Tech Talk: Configuring Auto-Voice VLAN on SG350 en SG550 Series switches \(video\) \(Automatische spraak-VLAN op SG350 en SG550 Series switches configureren\)](#)

Best practice 5 - Routering tussen VLAN's

VLAN's zijn zo ingesteld dat verkeer gescheiden kan worden, maar soms heeft u VLAN's nodig om tussen elkaar te routeren. Dit is routering tussen VLAN's en dit wordt doorgaans niet aanbevolen. Als dit toch noodzakelijk wordt geacht binnen uw bedrijf, moet u het zo veilig mogelijk instellen. Wanneer u routering tussen VLAN's gebruikt, moet u verkeer naar servers met vertrouwelijke servers beperken door middel van ACL's (toegangscontrolelijsten).

ACL's filteren pakketten om de verplaatsing van pakketten door een netwerk te beheren. Pakketfilters bieden security door de toegang van verkeer, gebruikers en apparaten tot een netwerk te beperken en te voorkomen dat verkeer een netwerk verlaat. IP-toeganglijsten beperken de kans op spoofing en denial-of-service aanvallen en maken dynamische, tijdelijke gebruikerstoegang via een firewall mogelijk.

- [Inter-VLAN Routing on an RV34x Router with Targeted ACL Restrictions \(Routering tussen VLAN's op een RV34x router met gerichte ACL-beperkingen\)](#)

- [Cisco Tech Talk: Configuring Inter-VLAN Routing on SG250 Series switches \(video\) \(Routing tussen VLAN's op SG250 Series switches configureren\)](#)
- [Cisco Tech Talk: Inter-VLAN Configuration on RV180 and RV180W \(video\) \(Configuratie tussen VLAN's op RV180 en RV180W\)](#)
- [RV34x Inter-VLAN Access Limitation \(CSCvo92300 bug fix\) \(Beperking van toegang tussen VLAN's met RV34X \(fix voor CSCvo92300-bug\)\)](#)

Conclusie

U kent nu enkele best practices voor het instellen van veilige VLAN's. Houd deze tips in gedachten wanneer u VLAN's voor uw netwerk configureert. Hieronder vindt u verwijzingen naar artikelen die stapsgewijze instructies bevatten. Deze helpen u op weg naar een productief, efficiënt netwerk dat uw bedrijf precies biedt wat het nodig heeft.

- [Configuring VLAN Settings on the RV160 and RV260 \(VLAN-instellingen configureren op de RV160 en RV260\)](#)
- [Configure Virtual Local Area Network \(VLAN\) Settings on an RV34x Series Router \(VLAN-instellingen configureren op een RV34x Series router\)](#)
- [Configure VLAN Membership on RV320 and RV325 VPN Routers \(VLAN-lidmaatschap configureren op RV320 en RV325 VPN routers\)](#)
- [Configure Virtual Local Area Network \(VLAN\) Membership on an RV Series Router \(VLAN-lidmaatschap configureren op een RV Series router\)](#)
- [Configure VLAN Interface IPv4 Address on an Sx350 or SG350X Switch through the CLI \(IPv4-adres van VLAN-interface op een Sx350 of SG350X switch configureren via de CLI\)](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.