VLAN

Ett virtuellt LAN, VLAN, är en teknik som delar upp switchportar i olika broadcast domains. När en switch tar emot en L2-frame med en destinations MAC-adress som den inte känner till så skickas L2 frame:n ut på samtliga fysiska interface inom det VLANet. Om switchen får svar från destinations MAC-adressen så bygger den en post i sitt MAC address-table med MAC-adressen och vilket interface den finns via. Detta sker inom ett VLAN, så om en enhet i VLAN 1 skickar en L2 frame med destinations MAC-adress till en enhet som finns i VLAN 2 kommer kommunikationen inte att fungera på egen hand.

VLAN knyts oftast ihop med ett IP-nät och kommunikation mellan VLAN:en sker genom en router eller L3-switch. Rent tekniskt går det att placera flera IP-nät i samma VLAN. Best practice är ett 1-till-1 förhållande mellan IP-nät och VLAN.

VLAN

Konfiguration

Skapa VLAN

Ett VLAN skapas i konfigurationsläge. Ett VLAN till delas ett nummer mellan 1 och 1001 och mellan 1006 och 4096. VLAN 1 är default VLAN och kan inte tas bort. VLAN 1002-1005 är reserverade. Det är rekommenderat att tilldela ett namn till VLAN:et för att det ska vara igenkännligt, men det är inte ett tekniskt krav. VLAN 1-1005 kallas för normal range och VLAN 1006-4096 för extended range, detta då äldre switchar ej hade stöd för extended range.

```
vlan 1000
 name NATIVE_VLAN
```

Verifiera att VLANet har skapats med `show vlan id 1000`. Det går även att se samtliga VLAN med `show vlan brief`.

Det går att avaktivera ett VLAN utan att ta bort det genom att sätta det i läget *suspend*. Accessportar som är tilldelade ett VLAN som är suspeneded fungerar ej, trafik som kommer in på de portarna droppas.

```
vlan 1999
 state suspend
```

VLAN sparas i running-configuration om man skapar VLAN manuellt och ej använder sig av Vlan Trunking Protocol.

Tilldela VLAN till accessport

En accessport, en port som ansluta sig direkt mot en enhet som ej VLAN taggar själv, kan ha 1 data-VLAN och 1 voice-VLAN. När trafik kommer in på porten så taggar switchen paketen med VLAN numret i L2 frame headern. När trafik skickas ut på porten så tas VLAN numret bort från L2 frame header. Skulle man tilldela ett VLAN som inte finns till en accessport så skapas det VLANet då.

```
interface GigabitEthernet1/0/1
 switchport access vlan 1337
 switchport mode access
```

VLAN Trunking

VLAN Trunking är när man tillåter flera VLAN att kommunicera över samma port. Trunk-portar används när man ansluter L2 mellan switchar eller upp till routrar. Trunking är en Cisco-term, i övriga världen kallar man dessa för taggade portar.

Historiskt sett har det funnits två stycken protokoll för trunking, ISL och 802.1Q. ISL (Inter-Switch Link) är Cisco propertiärt, förstår ej native VLAN och används inte i praktiken längre. Den öppna standarden som är definierad av IEEE, 802.1q, används av samtliga leverantörer. Benämns ofta enbart som en dot1q trunk.

802.1q har något som heter native VLAN. Trafik som inte har blivit taggade tidigare i nätet hamnar på native VLAN. Per default är native VLAN 1, best practice är att byta native VLAN till ett VLAN som inte används till någonting annat, detta för att skydda mot VLAN hopping attacker. Matchar inte native VLAN kan dessa kollidera, trafik som skickas ut på native VLAN 777 tas emot på native VLAN 666.

```
interface Port-channel1
 switchport trunk native vlan 666
 switchport trunk allowed vlan 800
 switchport mode trunk
```

När man lägger till VLAN på Cisco-switchar gäller det att hålla tungan rätt i mun. Nyckelordet add är viktigt vid tillägg för att undvika onödiga driftstopp. Använd gärna Configuration Rollback för att undvika längre driftstopp vid misstag. Det går att redigera flera VLAN åt gången genom att använda bindestreck för en serie eller VLAN separerade med kommatcken, ex. `10-20,30`.

switchport trunk allowed vlan 10	Gör att enbart vlan 10 tillåts på trunken och tar bort övriga redan tillåtna VLAN
switchport trunk allowed vlan all	Tillåt alla VLAN över en trunk
switchport trunk allowed except 10-20	Tillåt alla VLAN mellan 1 och 4096, förutom 10 till 20
switchport trunk allowed vlan none	Tillåt inga VLAN över trunken
switchport trunk allowed vlan remove 10,20	Ta bort VLAN 10 och 20 från trunken men tillåt resterande som redan är tillåtna

Stänga av Native VLAN beteendet

Det går att stänga av default native-VLAN beteendet, dvs att det som skickas ut på native VLANet skickas otaggat. Det gör man genom det globala kommandot `vlan dot1q tag native`, då skickas all trafik ut på trunkar VLAN-taggat.

Konfigurera trunkinterface på en router

```
interface Port-channel1.50
 encapsulation dot1Q 50
```

Subinterface numret (po1.50) måste inte matcha VLAN ID:t, men är man inte galen så matchar man.

Det är rekommenderat att skapa ett subinterface för native VLAN. Om det inte görs så skickas otaggad trafik ut via fysiska interfacets konfiguration.

```
interface Port-channel1.1337
 encapsulation dot1Q 1337 native
```

Konfiguration i äldre enheter, VLAN Database Mode

I äldre Catalyst-switchar och routrar så skapas VLANen i VLAN database configuration mode.

```
Switch3# vlan database
Switch3(vlan)# vlan 21
Switch3(vlan)# show current
Switch3(vlan)# show proposed
Switch3(vlan)# show current 22
```

```
Switch3(vlan)# vlan 22 name VLAN-NAME
Switch3(vlan)# show proposed 22
Switch3(vlan)# vlan 21 state suspend
Switch3(vlan)# vlan 21 state active
Switch3(vlan)# apply
```

Show kommandon, VLAN database mode

Kommando	Förklaring
show vlan brief	Se VLAN databas
show current	Se nuvarande VLAN databas efter att man har öpnat VLAN databasen
show proposed	Se föreslagen VLAN databas efter att man har öpnat VLAN databasen och utfört förändring

Private VLAN

Om man önskar att begränsa kommunikation inom ett VLAN kan man använda sig av private VLAN. Ett enda IP-nät kan användas inom ett private VLAN men inga av portarna tilldelade VLANet kan kommunicera med varandra. Private VLAN delar upp VLANs i secondary VLANs (sub-VLANs) och primary VLANs. Sett från utsidan så används primary VLAN precis som ett vanligt VLAN, men internt så används secondary VLANs med andra VLAN IDn. Ett primary VLAN kan alltså beskriveas som ett kluster som innehåller fler secondary VLANs.

image.png

Secondary VLANs kan agera på två sätt:
- som Community VLANs
- som Isolated VLANs

Portar som är tilldelade ett Community VLAN kan kommunicera med varandra direkt men kan inte kommunicera med andra VLAN. Beteendet här är alltså likt det vanliga VLAN beteendet.
Portar som är tilldelade ett Isolated VLAN kan inte kommunicera med andra portar inom Isolated VLANet eller med andra VLAN.

Ett enda primary VLAN kan associeras med flera secondary VLANs. Ett secondary VLAN kan enbart associeras med ett primary VLAN.

Portar som leder till något utanför private VLAN domänen, ex. upplänk till en router, konfigurereas som *promiscuous ports*. Promiscuous porten är inte associeras med något secondary VLAN utan

direkt med primary VLANet. Det som är ansluted mot promiscuous porten kan kommunicera med alla sekondära VLAN och alla sekondära VLAN kan kommunicera med det som är kopplat till promiscuous porten. Promiscuous portar beter sig som accessportar, de använder inte VLAN tagging såsom en dot1q trunk.

Trafik från primära eller sekondära VLAN kan **alltid** skickas ut över en dot1q trunk. Om paketet kom från en community eller isolated port och skickas över dot1q trunk så taggas det med sekundära VLANet. Om det paketet kom från en promiscuous port och skickas över dot1q trunk så taggas det med primära VLANet. När paketet har traverserat trunken så behandlas det på korrekt sätt, såsom om ex. isolated eller promiscuous port var lokalt ansluten.

Det finns två speciella trunktyper tillhörande private VLAN:
- Promiscuous PVLAN Trunk
- Isolated PVLAN Trunk

image.png

När ett paket från ett sekondärt VLAN ska skickas ut över en Promiscuous PVLAN Trunk så skrivs VLAN taggen om till det primära VLAN ID:t.

När ett paket från ett sekondärt VLAN ska skickas ut över en Isolated PVLAN Trunk så skrivs VLAN ID:t om från det primära VLAN ID:t till det som används för sekondärt isolated VLAN. En Isolated PVLAN Trunk används när paket skyfflas från en switch som förstår private VLAN till en switch som inte förstår private VLAN, men som kan hantera *protected ports,* även känt som Private VLAN Edge. Här konfigureras accessportar med `switchport protected` . Protected ports kan inte prata med andra protected ports men kan prata fritt med övriga portar, det går alltså att skapa VLAN-isolering inom samma switch med hjälp av protected ports.

Konfiguration

```
# Skapa private VLAN
vlan 199
 name Isolated
 private-vlan isolated
vlan 101
 name Community
 private-vlan community
vlan 100
 name Primary
 private-vlan primary
 private-vlan association 101,199
```

```
# Konfigurera interface för vlan 101
interface fa0/1
 switchport mode private-vlan host
 switchport private-vlan host-association 100 101

# Konfigurera promiscuous port
interface fa0/2
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 100 101,199

# Konfiguera SVI, om L3 routing används i samma switch
interface Vlan 100
 private-vlan mapping 101,199
```

Dynamic Trunking Protocol

DTP är ett Cisco propertiärt protokoll för att dynamiskt konfigurera trunklänkar. När det är påslaget finns det i två lägen:
- dynamic auto, läget förhandlas automatiskt men föredrar att vara en accessport
- dynamic desirable, läget förhandlas automatiskt men föredrar att vara en trunkport

För att en trunk ska förhandlas måste ena sidan vara konfigurerad som dynamic desirable eller hårdkonfad som trunk och fortfarande skickar DTP-meddelanden. DTP-meddelanden innehåller även VTP (Vlan Trunking Protocol) domänen.

DTP konfigureras genom switchport mode dynamic auto eller switchport mode dynamic desirable. Det ersätter alltså hårt konfigurerad access eller trunk. En hårt konfigurerad accessport eller trunkport skickar fortfarande DTP meddelanden om det inte stängs av.

DTP kan stängas av på interface-nivå med kommandot `switchport nonegotiate`.

DTP-status kan kontrolleras med `show dtp` och `show dtp interface`.

Q-in-Q

Q-in-Q tunneling är en teknik för att sträcka VLAN över ett annat VLAN. Det kan exempelvis användas för att ett företag ska kunna VLAN-taggga över en service providers nät. När trafik kommer in på en specifik port så läggs en extra VLAN-tag på i Ethernet-headern. Förutom på portarna som är anslutna mot Q-in-Q endpoints så switchas sedan paketen precis som vilket paket

som helst i nätet. Se till att ej använda samma VLAN som native VLAN någonstans, i värsta fall kan det skickas ut till någon annan kund eller nullas om inte native VLAN beteendet är avstängt med `vlan dot1q tag native`.

Konfiguration

```
vlan 100
 name Q-in-Q_Kund1

interface GigabitEthernet1/0/1
 switchport mode dot1q-tunnel
 switchport access vlan 100
 l2protocol-tunnel cdp
 l2protocol-tunnel stp
 l2protocol-tunnel vtp
 l2protocol-tunnel lldp
```

VLAN Trunking Protocol

VTP är ett protokoll som ska tillåta enkelt skapande av VLAN. Konceptet är att när ett VLAN skapas på en master-switch så skapas det på samtliga andra switchar i VTP-domänen istället för att man ska behöva skapa dem manuellt. VTP annonserar VLAN ID, VLAN namn, VLAN typ och status för VLANet. VTP finns i tre versioner, VTPv1, VTPv2 och VTPv3.

VTPv1 har enbart stöd för normal range VLANs.

Förbättringar i VTPv2 innehåller stöd för:
- Token Ring Concentrator Relay Function och Bridge Relay Function (TrCRF och TrBRF) typ VLANs, dessa används ej i Ethernet.
- Stöd för okända Type-Length-Value (TLV) records.
- Optimerad VLAN databas konsistens kontroll, i VTPv1 sker kontrollen vid modifiering av VLAN databasen, i VTPv2 så antar man att den redan har skett i switchen där VLANet lades till.

För att stänga av VTP använder sig många av `vtp mode transparent`. Det stänger dock inte av VTP, switchen bryr sig inte om VTP-meddelanden lokalt men den skickar fortfarande vidare VTP paket så länge domänen matchar den som är konfigurerad på den lokala switchen. En switch utan konfigurerad VTP domän skickar vidare samtliga VTP-meddelanden.

VLANen sparas ej i running-configuration utan i filen `vlan.dat` när man använder sig av VTP..

Skräckprotokollet VTP

I VTPv1 och VTPv2 är det den switch som har högst revisionsnummer den som bestämmer. Så om en switch med ett högt revisionsnummer men med helt annan VLAN-konfiguration än nuvarande kopplas in i ett nät kan hela L2-domänen gå sönder då VTP modifierar nätet enligt den nyinkopplade switchens konfiguration.

Risken att hela vlan-databasen tas bort på det här viset har löst sig i VTPv3.

VTPv3

VTPv3 är den senaste versionen och den mest rekommenderande att använda. VTPv3 har löst problem so

Förändringar i VTPv3:
- Serverroll, det finns två servertyper i VTPv3, primär och sekundär. Enbart den primära servern får modifiera VLAN-databasen. Den sekundära kan ta över rollen som primär vid behov. Det gör att VLAN-databasen ej kan bli rensad som i tidigare VTP-versioner.
- Lösenord, VTP lösenordet kan krypteras så att det inte syns i klartext.
- VTPv3 klarar av hela VLAN-rangen inklusive private VLANs. Pruning funkar dock enbart för normal-range VLANs.
- Off-läge, det går att ställa in så att switchen ej deltar i VTPv3 och kastar samtliga VTP-paket. Det går även att stänga av VTP per trunk.
- VTPv3 är en teknik för att föra över databas-information, ej enbart VLAN-databasen. Exempelvis MST-regioner kan synkar över VTPv3.

Skulle en VTPv3 switch konfigureras som transparent och sedan bytas tillbaka till klient så nollställs ej revisionsnumret såsom det gör i tidigare versioner. Det enda sättet att nollställa revisionsnumret är att konfigurera VTP domännamn eller konfigurera ett VTP lösenord.

En VTPv3 switch som ansluter sig mot en VTPv2 switch går över till VTPv2 på just det interfacet. Mot VTPv1 kan VTPv3 ej göra detta.

Conflict

Om switchar i en VTPv3 domän har olika uppfattning om vilken switch som är primärserver så kallas det för en *conflict*. Switchar i konflikt synkroniserar ej sina VLAN databaser även om alla VTP parametrar matchar. Kontrollera konflikter med kommandot `show vtp devices conflicts`.

VTP-lägen och funktoner

Det finns fyra typer av VTP-lägen en switch kan fungera som:

image.png

Det finns fyra typer av meddlanden som VTPv1 och VTPv2 använder sig av:

Läge	Förklaring
Summary Advertisement	Skickas av VTP server och klientswitchar var femte minut samt vid modifiering av VLAN-databasen. Meddelandet innehåller VTP domännamn, revisionsnummer, identiteten av den som uppdaterade senast, tidsstämpel från senaste uppdatering, MD5 summa över VLAN databasen och VTP lösenord samt antalet Subset Advertisements som följer denna Summary Advertisement.
Subset Advertisement	Skickas av VTP server och klientswitchar efter modifiering av VLAN-databasen. Innehåller hela VLAN databasen. Flera Subset Advertisements kan behövas om VLAN databasen är stor.
Advertisement Request	Skickas av VTP server och klentswitchar för att be sina grannar skicka hela VLAN databasen eller delar av den. Skickas när en VTP klientswitch startas om, när en switch blir klient eller när en server eller klientswitch får en Summary Advertisement med ett revisionsnummer höger än sitt egna.
Join	Skickas av VTP server och klientswitchar periodvis var femte minut om VTP Pruning är aktivt. Join-meddelanden innehåller ett bit-fält för varje VLAN i normal range som indikerar om det är aktivt eller inaktivt - och därmed ska "prune:as".

VTP-meddelanden skickas enbart ut över trunklänkar och accepteras enbart att tas emot över trunklänkar.

VTP processer och revisionsnummer

Varje en gång VLAN-databasen uppdaterade i VTPv1 och VTPv2 så räknar revisionsnumret upp. Som tidigare nämnt fungerade VTPv1 och VTPv2 som så att när de tar emot ett meddelande med högre revisionsnummer än sitt egna så litar de på den uppdatering och uppdaterar VLAN-databasen därefter.

Per default så är Cisco-switchar i VTP server mode men de skickar inga VTP uppdateringar förrän ett domännamn är satt. VTP klienter behöver dock faktiskt inte sätta ett domännamn utan antar att domännamnet som är med i den första VTP-uppdateringen de mottager är det som gäller. De måste dock konfigureras som klienter först.

För att skydda ett nät från otillåtna switchar kan man använda sig av VTP passwords. VTP Summary Advertisements skickar med en MD5 hash som är gjord från VLAN databasen och VTP lösenordet, om det är konfigurerat. Mottagande switch räknar ut sin egen MD5 hash efter mottagen uppdatering och jämför den med hashen från skickande switch.

Konfiguration

VTPv2

```
vtp version 2
vtp domain VTP-NAMN
vtp password PASSWORD
vtp mode server/client/transparent
```

VTPv3

```
vtp version 3
vtp mode client client/off/transparent/off
vtp password PASSWORD hidden


do vtp primary
```

Spanning-Tree Protocol

STP är ett protokoll som används för att ej skapa L2-loopar. STP ska alltid användas i ett bryggat nät. Se mer information här.

Show kommandon

show vtp status	Se information om VTP version, domännamn, VLAN, senaste förändring osv
show vtp password	Se VTP lösenord
show vtp counters	Statistik
show vtp devices	Enbart VTPv3
show vtp interface	Se om VTP är igång på interface

Cisco Resilient Ethernet Protocol (REP)

REP är ett Ciscopropertiärt protokoll för att snabbt konvergera ett L2-nät i ringtopologi. Det är ett alternativ till STP. Konvergensen är väldigt snabb, mellan 50 och 300 millisekunder. En REP domän kallas för segment. Segmentet är en omkretsen början-till-slut mellan två edge-portar. Destinations MAC-adress `0180.c200.0000` används, vilket vanligtvis används för STP. Enbart en port i hela ringen kommer att blockera VLAN för att undvika loopar.

image.png

Bilden till vänster visar ett ring segment där båda edge-portar är på samma switch och bilden till höger visar edge-portar i ett "open segment" där edge-portarna är på olika switchar.

Ett VLAN dedikerat till REP-admin behövs. Sedan specifiseras `rep admin vlan x` i globbalt konfigläge. Verifiering kan ske med `show interface GigabitEthernet0/1 rep { detail }`.

För att REP ska aktiveras på ett interface måste det vara ett NNI (network-to-network interface) och det måste vara en trunkport. REP stöds på länkaggregeringar. Edgeportar ska konfigureras där en är primary och en är secondary.

```
! Edge-portar i ringsegment
interface Port-channel1
 port-type nni
 switchport mode trunk
 rep segment 1 edge primary

interface Port-channel2
 port-type nni
 switchport mode trunk
 rep segment 1 edge

! Portar på övriga switchar
interface Port-channel 1
 port-type nni
 switchport mode trunk
 rep segment 1

Warning: Enabling REP automatically disables STP on this port. It is
recommended to shutdown all interfaces which are not currently in use to
prevent potential bridging loops.
```

Verifieringar sker med `show rep topology segment 1`.

Age-timers, alltså hur länge en switch väntar innan REP-grannskapet anses dött, kan konfigureras med interface kommandot `rep lsl-age-timer x`, där x är millisekunder. Hello-värdet är 3 gånger så

litet som age-timern. Timers ska matcha mellan switchar, annars kan en ostabil miljö skapas.

Debugging kan utföras med `debug rep failure-recovery` och `debug rep prsm`.

Ett val utförs när ringen formas. Varje port har en 64-bitar stor prioritet. De första 4 bitarna innehåller en failed bit och konfigurerbara fält. Följande 12 bitar innehåller portidentifierare och de kvarstående 48 bitarna innehåller switchens MAC-adress. Alternate portval sker npå en blockad port när en "öppen" port måste väljas. Switchar utbyter blocked port advertisements (BPA) med varandra vilket innehåller prioriteter. Prioritet per interface går att se med `show rep topology segment 1 detail`. En port med bättre prioritet blir "open" och en port med sämre blir "alternate". BPAs skickas bara av en alternate port under valet då BPAerna innehåller VLANinformation för blockerade VLAN.

Det går ej att sätta en specifik portprioritet. Det går dock bra att konfigurera ett interface som preferred med `rep segment 1 edge preferred`. Ingen preemption sker, vill man byta roll måste länken flappa. När en länk går ned så togglas "failed" bit som nämndes ovan.

Port IDn nämndes ovan i BPA paketet. De går att se med `show interfaces rep detail`. Genom att använda oss av port IDn kan vi åstakomma VLAN load sharing. Det konfigureras på primary och edge-portarna. Man specifiserar en port i segmentet där vissa VLAN ska blockeras. Ett interface kan specifiseras genom att manuellt ange port IDt, använda neighbor offset number manuellt eller genom perferred-nyckelordet.

För att förändring ska ske när man har justerat för VLAN load balacing måste man manuellt skaka om ringen lite. Det gör man med exec-kommandot `rep preempt segment 1`.

```
! Ändra per port ID
interface Port-channel1
 rep block port id 0011001D4692F700 vlan 13-37

! Numreringsmetod
interface Port-channel1
 rep preempt delay 15
 ! Siffran nedanför är distans till primary edge eller distance tills econdary edge
 rep block port -2 vlan 13-37

! Preferred-metod
interface Port-channel1
 rep block port preferred vlan 13-37

! Verifiering med show rep topology segment 1
```

I den här andra designen, REP open segment, har den fjärde Cisco-switchen (3560) inte möjligheten att köra REP. Den kommer att köra RPVST+.

image.png

Länkarna mot 3560 kommer att konfigureras lite annorlunda, se exempel:

```
 ! Interface mot 3560 som är SEC Edge port
interface GigabitEthernet0/1
 port-type nni
 switchport mode trunk
 rep segment 1 edge no-neighbor preferred
 rep stcn stp

 ! Interface mot 3560 som ej är PRI/SEC Edge port
 interface GigabitEthernet0/1
  port-type nni
  switchport mode trunk
  spanning-tree guard loop
  rep stcn stp
```

För att REP ska informera STP om förändringar i nätet ska `rep stcn stp` läggas till på interfacekonfen.

Ethernet Ring Protection Switching (ERPS)

ERPS är en teknik som fungerar likt REP men som är industristandard. Även känd som ITU G.8032. Ett segment kallas för "ring" och en länk mellan två ring-noder kallas för "ring link". "Ring ports" är portar i ring links. Alternate-porten (blockerad) kallas för ring protection link (RPL). Noden som blockerar en port kallas för RPL owner node. Precis som i RPL kommer bara en port i hela ringen att blockera VLAN föratt undvika loopar.

VLAN Mapping

VLAN Mapping innebär att en switch på en trunkport tar emot paket på ett VLAN och skriver om L2 headern till ett annat VLAN.
Konfigurationen är enkel, ex: `switchport vlan mapping 13 37`. Det första VLANet är mottaget VLAN och det andra är det som det skall skrivas om till.

Revision #1
Created 26 April 2025 11:54:55 by Jehrlander
Updated 26 April 2025 11:55:08 by Jehrlander