Föreläsning R&S

2014-01-21

Kap. 2 & 3

STP — STP för att hindra loopar
Skapa redundans

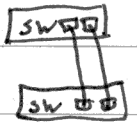
VLAN — VLAN → Virtuella LAN

SW — Switchar

CAM
- CAM — Mac-adress-tabell
- Tajmar ut - Aging time

MAC
- En hacker kan fylla minnet med massa MAC-adresser
- Finns inte MAC - Floodas på alla portar utom sändaren.
  CPU - reggade för switchen (till andra switchar)

PO
- PO1 = Port aggregation / Link aggregation



Domains
- Broadcast domän → Container broadcast på logiska nät.
- Collision domain → Det område där paket kan krocka

STP (Spanning Tree Protokoll) är ett protokoll för att förhindra loopar att inträffa. I och med detta kan man medvetet koppla samman switchar där loopar normalt skulle uppstått för redundans men STP hindrar loopen.

VLAN (Virtuella LAN) delar upp ett nät i flera olika logiska nät.

MAC-adressminnet i en switch kallas för CAM som står för Content Addressable Memory.

Duplex

Halv duplex → En åt gången
Full duplex → Båda åt gången
Gigabit → Bara full duplex

Layer 3

Layer 3 Switching

- Multilayer switching
- Bara första paketet som routas, sedan går den över till switching
  - Src och dst IP cachas

CDP

Cisco utv. protokoll med varandra, vanligt tex för telefoner
Känsligt för attacker

S&F

Store and forward orsakar lite latency, tex så bra i SAN.

Cut-through

Cut-through

- Fast-forward → Granskar inget
- Fragment free → Granskar 64 bytes (inga kollisioner)

Normalt ethernet är 1500, kan ökas till 9600 bytes och kallas då jumbo frames. Även användbart i virtuella miljöer.

- 10/100 mbit kan köra både halv och full duplex medan gigabit alltid kör med full duplex.
- En layer 3 switch är en enhet som routar det första paketet, precis som en vanlig router, men efterföljande paket switchas istället för att få mindre latency och högre throughput.
- Det finns två olika "modes" för switchar, Store and forward och Cut-through (som i sin tur har fast-forward och fragment-free). S & F lagrar paketen och granskar den innan vidaresändning vilket cut-through inte gör.

Redundans

Sätt i switchade nät (redundans)

- Skapas genom att loopa switchar och STP hindrar loopen.

STP

RSTP

STP

- Ny standard RSTP 802.1w
- STP (gamla) har lång konvergenstid och uppstart
- Mix STP & RSTP

Fallback

← Fallback till STP

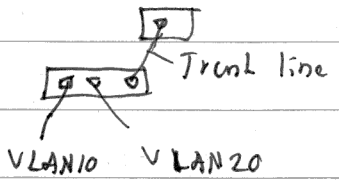
PVST

- En instans per VLAN

PVST Per VLAN Spanning tree

RSTP

- RSTP
  - Kräver trunkning mellan SW
    - Trunkning → Flera VLAN ID på samma kabel.



Rapid PVST

- Rapid PVST

- Redundans i switchar skapas genom att loopa dem och låta STP hindra loopen. När en linje går ner öppnar en ny vägs upp automatiskt. STP standarden benämns 802.1D. STP har lång uppstarts och konvergeringstid.
- RSTP heter den nya standarden för STP och har nummer 802.1w. RSTP är snabbare!

RSTP kräver trunkning mellan switcharna

En trunk tillåter flera VLAN-ID att använda/passera samma kabel. PVST = Per VLAN Spanning Tree.

BPDU

BPDU

Bridge Protocol Data Unit
- 2 sek mellanrum

Portinfo

Hjälper porta/sw

BPDU
paket

Två typer
- Kontig BPDU
- Topologi förändrings BPDU
  - Räcker att en host startas så skickas det

Port states

Port States

Disabled	(admin down)
Blocking	Blockerad för all trafik utom BPDU lär ej MAC
Listening	Samma som blocked, kan även skicka BPDU
Learning	Blockerad men ta emot/skicka BPDU, lär MAC
Forwarding	Normal trafik

BPDU är paketen som STP använder för att kommunicera. Det finns två olika typer av BPDU-paket, nämligen konfigurations BPDU och topologi förändrings BPDU. Ett topology change BPDU skickas ut så fort någting ändras på nätverket, det räcker att en host startas upp för att generera ett topology change.

BID

Root bryggan blir den med lägst BID Brygg ID

BID = prio + MAC

↓

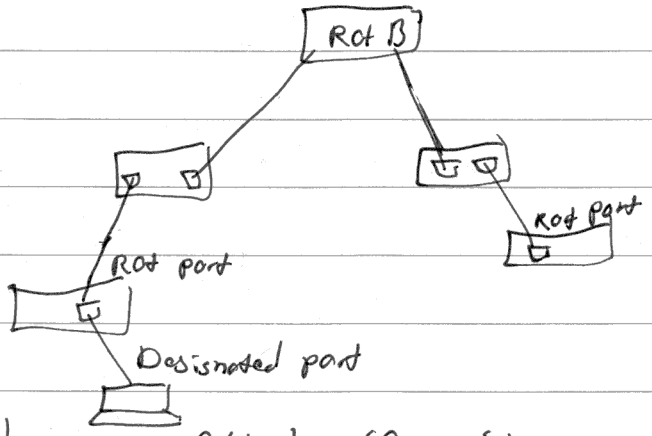
Default 32768

↓

~~Sänk~~ Sänk ifall man vill styra BID och root själv, ex 4096 (0 är inte alltid ok)

Root port

- Root bryggan



Root bryggan oftast core-sw

Port på sw närmast root bridge är root port

Cost path

Kostnad

- Kortast väg
- Hastighet

I BPDU finns info om ven som är root brygga

I STP blir root bryggan den switch/brygga med lägst BID (Bridge ID). BID bestäms genom Prioiteten + MAC addr. Vill man själv kunna styra vem som ska bli root brygga så sänker man Prio numret i den switch man vill ha som root. Oftast är det lägsta giltiga prionr 4096, alltså inte 0. Root port kallas den/de portar som går upp mot root bryggan och designated port kallas den/de portar som går ner mot hostar / access switchar osv.

Designated
Minst en port i varje sw blir designated
DP portens riktning för trafik är downstream
Kan finnas flera DP
- Men bara en per segment

Cisco STP
Ciscos egna STP förbättringar

Port Fast
- STP PortFast
  - Hoppa över STPs steg
  - Bra för access portar/sw
  - Får porten en BPDU återgår den till STP-läge

Uplink Fast
- Uplink Fast
  - För val av root portar snabbare
  - Öppnar inom 2-3 sek.

Backbone Fast
- Backbone Fast
  - På backbone sw

BPDU Guard
- PortFast BPDU Guard
  - Hostar ska inte skicka BPDU
    Ex skydd mot rouge sw eller hacker
    - Porten stängs

Root porten är i riktning mot root bryggan och designated är i riktning mot utrustning, access switchar etc, alltså downstream. Det finns alltid minst en port som är designated. I princip alla portar som går ut i nätet är designated. Cisco har gjort en del egna förbättringar till STP protokollet som är propitära för cisco. Dessa är PortFast (för access switchar), Uplink Fast och Backbone Fast för backbones. BPDU Guard är ett skydd som skyddar mot BPDU paket. Dvs Om porten får en BPDU stängs porten (hostar ska inte sk. BPDU)

BPDU Filter
- Port Fast BPDU filter
  - Filtrerar endast bort BPDU, stänger ej ~~på root port~~

Root Guard
- STP Root Guard
  - Stänger porten om BPDU med bättre cost

Loop Guard
- STP Loop Guard
  - Känner av om det inte kommer några BPDU
    - På root portar

VLAN

VLAN

Delar upp ett fysiska nät i logiska.
Man är inte låst till fysiska platser
Säkerhet mellan avdelningarna
- tex skyddar ekonomin från verkstaden etc

Contains broadcast trafik
Kan minska behovet av routrar
Mer kontig att tänka på

BPDU skyddar också mot BPDU-paket men till skillnad från Guarden så filtrerar BPDU Filter bara bort paketen istället för att bara stänga ner porten tvärt.
Root Guarden stänger porten om den får en BPDU med bättre path cost.
Loop Guard känner av om det inte kommer några BPDU, dvs ifall STP är "trasigt" och då loopar kan bildas, då stängs porten. Bra att ha på root portar.
VLAN delar upp ett fysiskt nät i logiska.

ID

VLAN ID som stöds
1-1000, 1025-4096
VLAN 1001-1024 är reserverade
1002 FDDI
1003 Token ring
1004 FDDI-Net
1006 Trnet

VLAN 1

VLAN 1 är default, här når alla alla och allt.
VLAN 1 = all trafik som inte är taggad släpps fram

NIC

Servers NIC måste stödja VLAN

Best practice

Best practice
- Använd inte VLAN 1 tillsammans med andra VLAN-ID, se upp för andra märken dock
  - Stäng av
- Ersätt VLAN 1 med annat "native" VLAN-ID
- Helst ytterligare ett VLAN för managment

VLAN ID som går att tilldela är 1-1000 och 1025-4096. VLAN:en mellan 1001-1024 är reserverade.
VLAN 1 är default VLAN:et, här når alla allt.
VLAN 1 är default native VLAN vilket innebär att här är all trafik som är otaggad. VLAN 1 är också default managment nät.
Tänk på att servers NIC också måste stödja VLAN.
Det bästa är om man kan ersätta VLAN 1 med ~~andra~~ ett native VLAN och ytterligare ett VLAN för managment.

Statiskt VLAN

Statisk VLAN konfig
- switchport access vlan 10
- Säkrast mot hacking
  - Låst per port

VLAN databas

Cisco switchar har en separat databas för VLAN.
Bara att skriva vlan 10 för att skapa vlan 10
- show vlan för att visa

Ta bort VLAN
no switchport access vlan

VTP

VTP (Virtual Trunking Protocol)
Kommunicerar VLAN mellan switcharna

Krav

Dessa krävs för VTP
- Domän
- VTP stöd (alla sw)
- Endast VLAN 2-1002
- Ställa in mode

Transparent fristående men skickar vidare till andra sw
Känslig mot hacker attacker

- En statisk VLAN konfiguration är det säkraste då porten är låst på ett specifikt VLAN.
- Cisco switchar har en separat databas för VLAN, den ligger alltså i den "vanliga config-filen".
- VTP kommunicerar VLAN mellan switcharna. För att VTP ska fungera krävs att följande har ställts in:
  - Domän
  - Alla sw måste ha VTP stöd
  - VLAN 2-1002
  - Ett mode har valts serv/klient/tra

Trunk

Skapa trunk
- Paket med olika VLAN-ID över samma kabel

Protokoll

Två protokoll
- ISL → Ciscos egna
- 802.1Q → STANDARD, kör på denna!

Tagg

VLAN-taggade paket är 4 byte större (802.1Q)
- Kan skapa problem i äldre utrustning

DTP

DTP → Dynamic Trunking Protocol
Trunklina kan skapas antingen statisk eller dynamisk med DTP då.
Enkelt att sätta upp stefisk
Två sista portarna som trunklina ifall många finns

VLAN taggning i slutnoder
- Funkar med virtuella interface i win/Linux.

- En trunklina är en linje mellan sw där flera olika VLAN ID kan passera. Till detta finns två protokoll, ISL och 802.1Q som är det som bör användas då ISL inte finns i alla switchar och dessutom är ett propiterärt protokoll för Cisco.
- VLAN-taggade paket är 4 byte större, i äldre utrustning kan detta skapa problem.
- DTP = Dynamic Trunking Protocol. Skapar en trunk automatiskt.

Native

Native VLAN

Switchport trunk native vlan 10

Filtrera

Filtrera bort VLAN

Switchport trunk pruning vlan 31-1001
allowed vlan 2-30

Privata

Privata VLAN

- Nod som inte ska nå andra
- Till för gäster, typ bibliotek etc

Gå över routrar

VLAN kan gå över routrar och därmed över internet

Skapa virt NIC

encaps dot1q

ip adress på de virt NIC

KONFA EJ IP PÅ FYSISKA NIC:EN TILL DE VIRT! Annars kan taggen försvinna

- Ett native VLAN kan skapas med `switchport trunk native vlan 10' t.ex.
- Det går att filtrera bort VLAN med pruning som man inte vill ska få passera. Detta görs med `trunk pruning vlan xx-xx'. Man kan även tillåta ranges med VLAN innanför pruning ranges med allowed.
- Privata VLAN brukar man skapa till besökare och gäster. Dessa VLAN ska då inte få nå känsliga delar i nätet.