2022

Cisco Reader

ROUTING EN REDUDANTIE

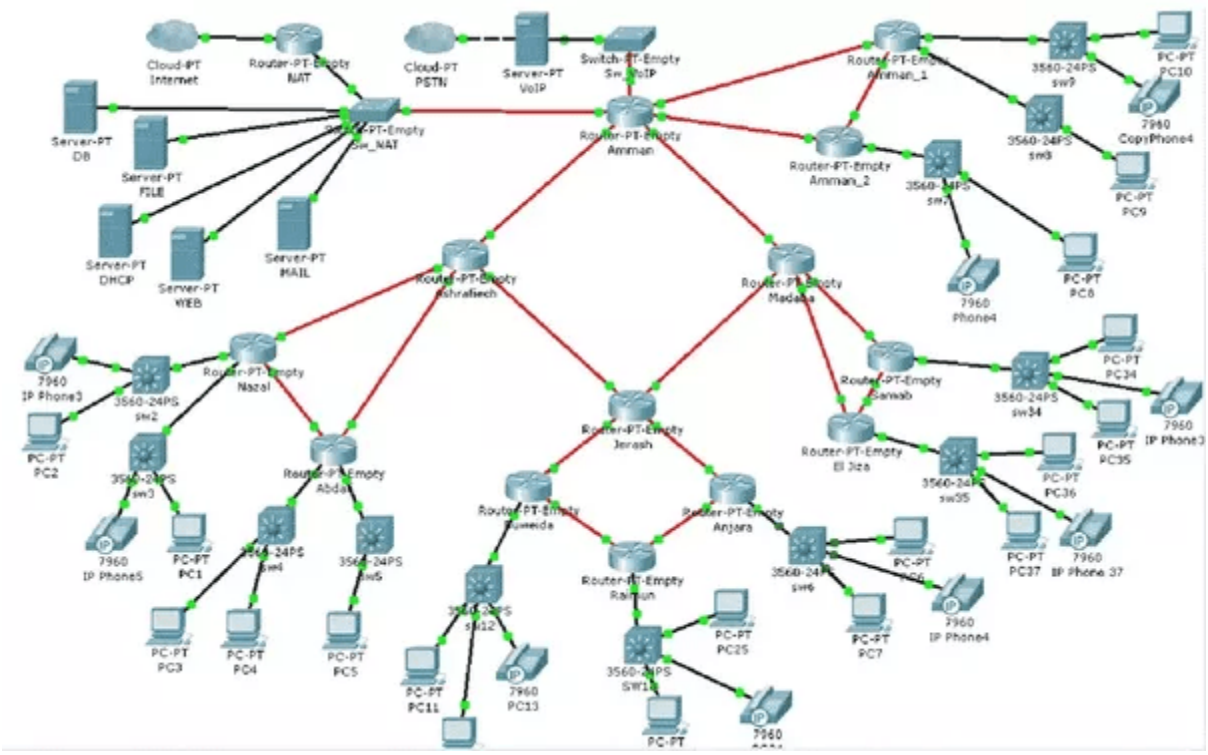
DOOR MARK VAN ETTEN

Inhoudsopgave

Cisco Reader

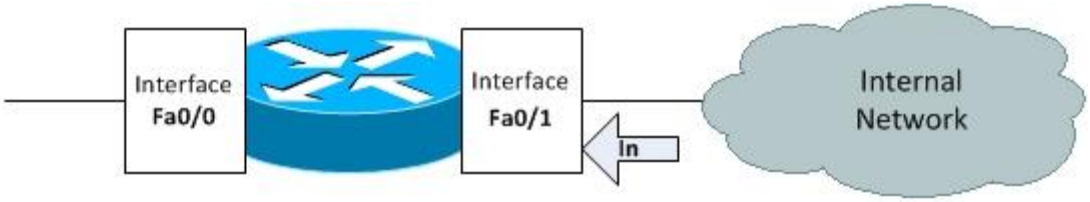
Deze Reader geeft een overzicht van de mogelijkheden van Computer Netwerken. (Leerjaar 2 en 3)

Voorbeeld van een computernetwerk in Packet Tracer



Extended Access-List

Access-list (ACL) is een set regels die is gedefinieerd voor het regelen van het netwerkverkeer en het verminderen van netwerkaanvallen. ACL's worden gebruikt om verkeer te filteren op basis van de set regels die zijn gedefinieerd voor het in- of uitgaan van het netwerk.




```
ip access-list standard Corp
!
remark deny Operations network
deny 172.18.0.0 0.0.255.255 log
!
remark Give access to CEO's host
permit 172.18.3.24 0.0.0.0
```

Blokkeren van poorten

Voorbeeld

Hoe een poort blokkeren van 172.16.40.0 naar 172.16.50.0 op poort 21

```
R1# config terminal
R1(config)# access-list 110
       deny tcp 172.16.40.0 0.0.0.255 172.16.50.0 0.0.0.255 eq 21
       permit any any
R1(config)# interface xx
            ip access-group 110 in/out
```

Blokkeren van netwerken

Hoe een netwerk blokkeren van 172.16.40.0 naar 172.16.50.0

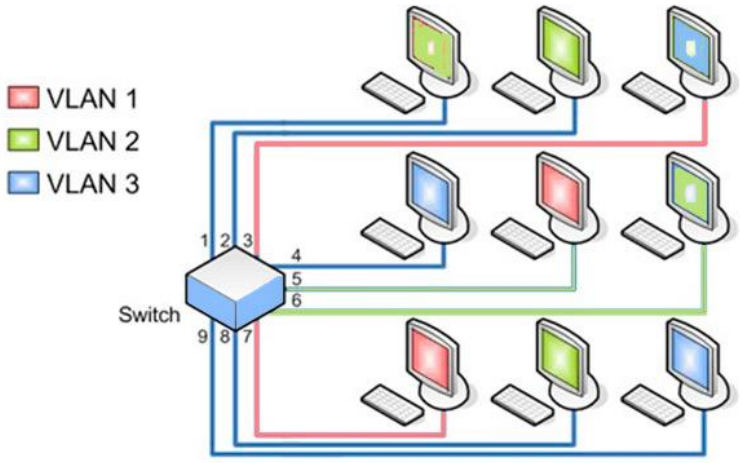
Voorbeeld

```
R1# config terminal
R1(config)# access-list 110
              deny ip 172.16.40.0 0.0.0.255 172.16.50.0 0.0.0.255
       permit any any
R1(config)#interface xx
       ip  access-group 110 in/out
```

De extended Access-List zo dicht mogelijk bij de bron van het verkeer toepassen.

VLANS

Virtual LAN (VLAN) is een concept waarbij we de apparaten logisch kunnen indelen op laag 2 (datalinklaag). Je kan het zien alsof je meerdere switches hebt die het netwerk scheiden.



VLAN ranges

- VLAN 0 en 4095: Kun je niet gebruiken. Deze zijn gereserveerd.
- VLAN 1:Is het default vlan
- VLAN 2-1001: Een normaal vlan van 2 tot en met 1001 kun je gebruiken.

Configuratie

We kunnen eenvoudig VLAN's maken door simpelweg het vlan-id toe te wijzen. Zo maak je bijvoorbeeld vlan 2 aan :

Stap 1

!!!!Niet vergeten!!!!!!

```
#switch1(config)#vlan 2
```

Alternatief op oudere routers/switches (niet in configure terminal uitvoeren)

```
Router#vlan database
Router(vlan)#vlan 10 name 10
```

Stap 2

Vervolgens moet je je vlan koppelen aan de interface van een switch of router

```
Switch(config)#int fa0/0
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access Vlan 2
```

Troubleshoot : VLANx is down

1) Wanneer je een VLANx met een ip-adres hebt en deze de status down heeft. Doe dan het volgende : Breng VLAN1 down met het commando shutdown. Breng daarna VLANx online met no shutdown.

2) En vergeet niet om eerst gewoon een VLAN aan te maken met het commando vlan x.

x is vlannummer.

Trunkports

Als je een vlan aanmaakt en deze met andere vlans wil laten uitwisselen dan moet
het ip-pakket wel weten in welke VLAN deze zat. Het ip-pakket krijgt dan extrainformatie over de vlan. Deze informatie komt in het 802.1Q header.

Om te zorgen dat dit format wordt ondersteund gebruik je dot1q encapsulation. Deze stel je in op de switchport die met een andere switch moet communiceren.

```
switch#interface x/x
switch#switchport mode trunk

optioneel commando, niet altijd beschikbaar op switches
switch#switchport trunk encapsulation dot1q
```

Optioneel kun je de switchport beveiligen met allowed.
Hiermee geef je aan welke vlans over de trunk mogen gaan. (xx vervang je met het VLAN-nummer)

```
switch#switchport trunk allowed vlan xx,xx
```

Inter-vlan routing

Met een layer 3 switch (een multilayer switch) kun je je een switch ook als router gebruiken. Deze constructie noemen ze ook wel 'inter-vlan' routing. Met een layer 3 switch kun je van netwerk x naar y packets versturen.

Om te werken met inter-vlan, zorg dat de layer 3 switch ip-routing enabled is. En je vlan interface een ip-adres heeft.

Commando's

```
#SW1(config) ip routing
#SW1(config) interface vlan 10
#SW1(config-if)ip address 10.1.10.1 255.255.255.0
```

VTP

VTP Client mode Sends/forwards VTP advertisements and Synchronizes VLAN configuration information with other switches.

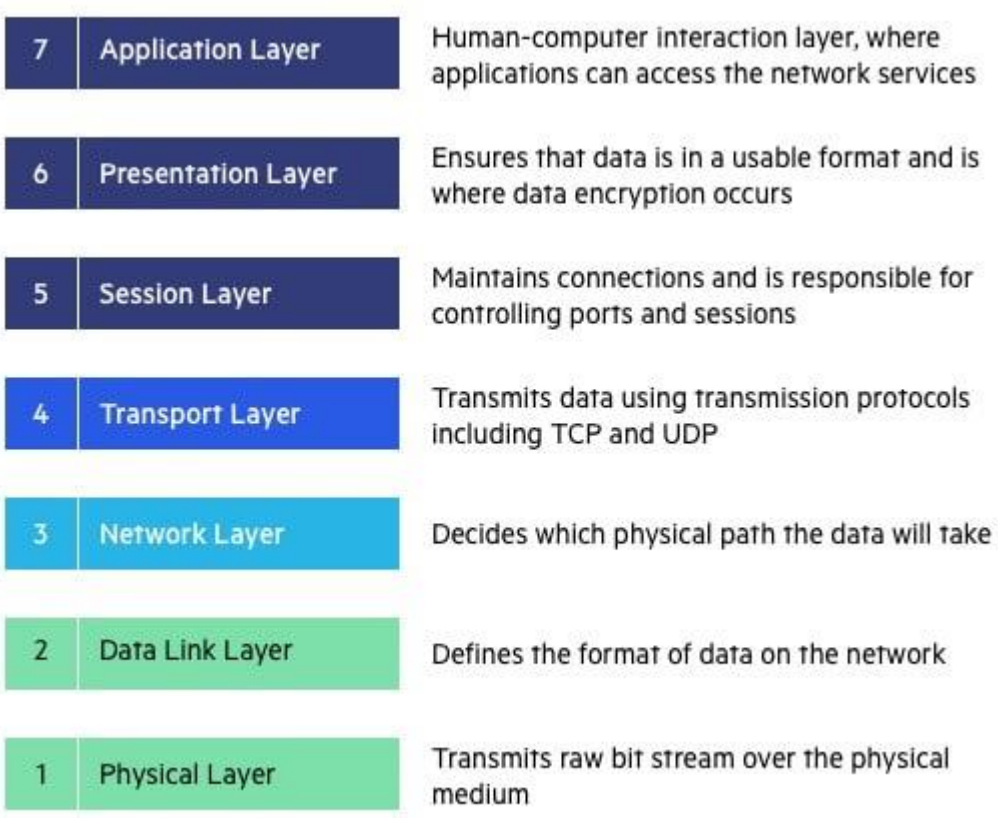
```
switch(config)#vtp domain horizon
switch(config)#vtp password cisco
switch(config)#vtp mode client
switch(config)#end
```

To verify the VTP mode use:

```
switch#show vtp status
VTP Version : 1
Configuration Revision : 0
Maximum VLANs supported locally : 1005
VTP Operating Mode : Client
VTP Domain Name :
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
switch#
```

OSI-Model

Het Open Systems Interconnection Model (kortweg OSI-model) werd door de *International Organization for Standardization* (ISO) ontworpen als **referentiemodel voor een open communicatie** tussen verschillende technische systemen. Handig voorbij het troubleshooten van netwerken.

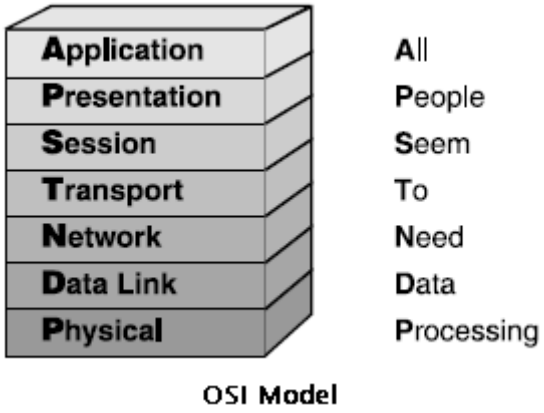


Mnemoniek : **A**ll **P**eople **S**eems **T**o **N**eed **D**ata **P**rocessing

Bottom-up troubleshoot methode

De bottom-up benadering begint bij de onderste laag van het OSI-model (laag 1) en werkt zich door de verschillende lagen omhoog totdat laag 7 is bereikt. Deze aanpak werkt goed als het probleem waarschijnlijk fysiek van aard is (d.w.z. een slechte kabel of een losse draad). Zodra een fysiek probleem is opgelost, zal je zoekopdracht daar waarschijnlijk eindigen (tenzij er meerdere problemen zijn).

Deze benadering vereist echter een intensieve blik op elke laag naarmate je verder komt in het OSI-model. Je moet bijvoorbeeld elke interface en kabel controleren voordat je met zekerheid kunt zeggen dat de fysieke laag niet het probleem is. Het kan extreem tijdrovend zijn, maar is vaak de favoriete aanpak wanneer de oorzaak van een probleem onbekend is.



OSI Model

Handige tip

Ping en Tracert zijn handige hulpmiddelen bij het onderzoeken van verbindingsproblemen. Als een ping mislukt, geeft dit meestal aan dat het probleem zich in de lagere lagen (1-3) voordoet, dus de bottom-up benadering zou de meest effectieve methode zijn om in deze scenario's te gebruiken.

HSRP

Het Hot Standby Router Protocol (HSRP) is een netwerk redundantie protocol van Cisco voor het realiseren van een redundant netwerk.

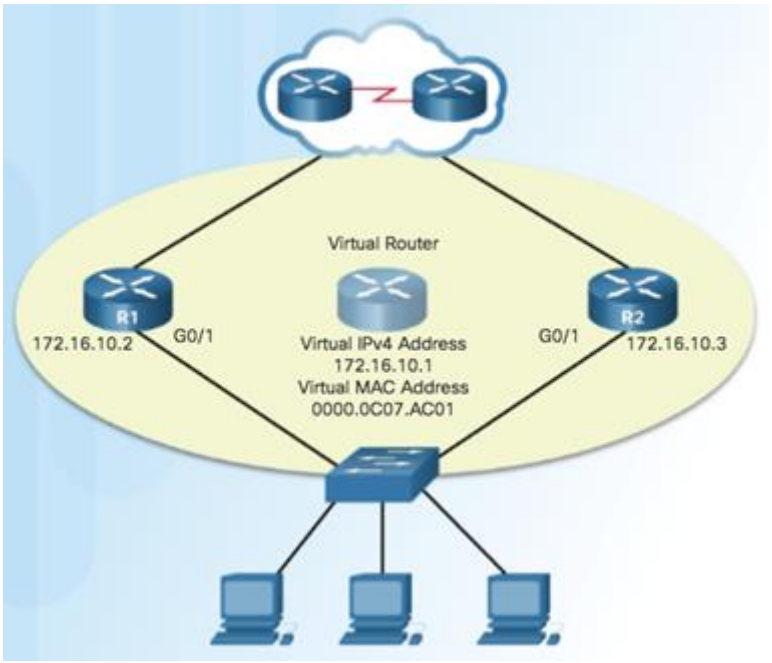
Met een redundantie protocol wordt automatische failover constructie tussen twee of meerdere routers mogelijk. Met dit protocol is de router als single point of failure (***SPOF***) onmogelijk. Het redundantie protocol gaat werken wanneer Één of meerdere interfaces op een router, of de gehele router, uitvalt.

Er zijn verschillende router redundantie protocollen; hier de belangrijkste:

VRRP staat voor Virtual Router Redundancy Protocol. Het is een open protocol; dat betekent dat deze op andere netwerkapparaten, ongeacht het merk, beschikbaar is.

Virtual Router

Voor deze protocollen wordt gebruikt gemaakt van een Virtual (Router) IP. Via deze virtuele router wordt de default gateway op ingesteld.



Preempt

Een Preempt is een stetting die je kan gebruiken om de 'oorspronkelijke' active router weer actief te maken.

Voorbeeld:
Router A is active en preempt.
Router B is standby.

Wanneer Router A down gaat neemt Router B het over.
Wanneer Router A weer online is gaat Router B naar standby.
Zonder *Preempt* gebeurt dit niet en blijft Router B active.

Configureren van HSPR

```
R1(config)# interface g0/1
R1(config-if)# ip address 172.16.10.2 255.255.255.0
R1(config-if)# standby version 2
R1(config-if)# standby 1 ip 172.16.10.1
R1(config-if)# standby 1 priority 150
R1(config-if)# standby 1 preempt
R1(config-if)# no shutdown
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
R2(config)# interface g0/1
R2(config-if)# ip address 172.16.10.3 255.255.255.0
R2(config-if)# standby version 2
R2(config-if)# standby 1 ip 172.16.10.1
R2(config-if)# no shutdown
```

Testen HSPR :

Let op de onderdelen die in het oranje staan.

```
R2# show standby
GigabitEthernet0/1 - Group 1 (version 2)
  State is Standby
    5 state changes, last state change 01:03:59
  Virtual IP address is 172.16.10.1
  Active virtual MAC address is 0000.0c9f.f001
    Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.944 secs
  Preemption disabled
  Active router is 172.16.10.2, priority 150 (expires in 8.160 sec)
    MAC address is fc99.4775.c3e1
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Gi0/1-1" (default)
R2#
```

Debug messages

```
R2# debug standby packets
*Dec  2 15:20:12.347: HSRP: Gi0/1 Grp 1 Hello  in  172.16.10.2
  Active pri 150 vIP 172.16.10.1

*Dec  2 15:20:12.643: HSRP: Gi0/1 Grp 1 Hello  out 172.16.10.3
  Standby pri 100 vIP 172.16.10.1
```

Letop! Deze kan veel meldingen genereren. Met dit commando zet je de debug message uit :

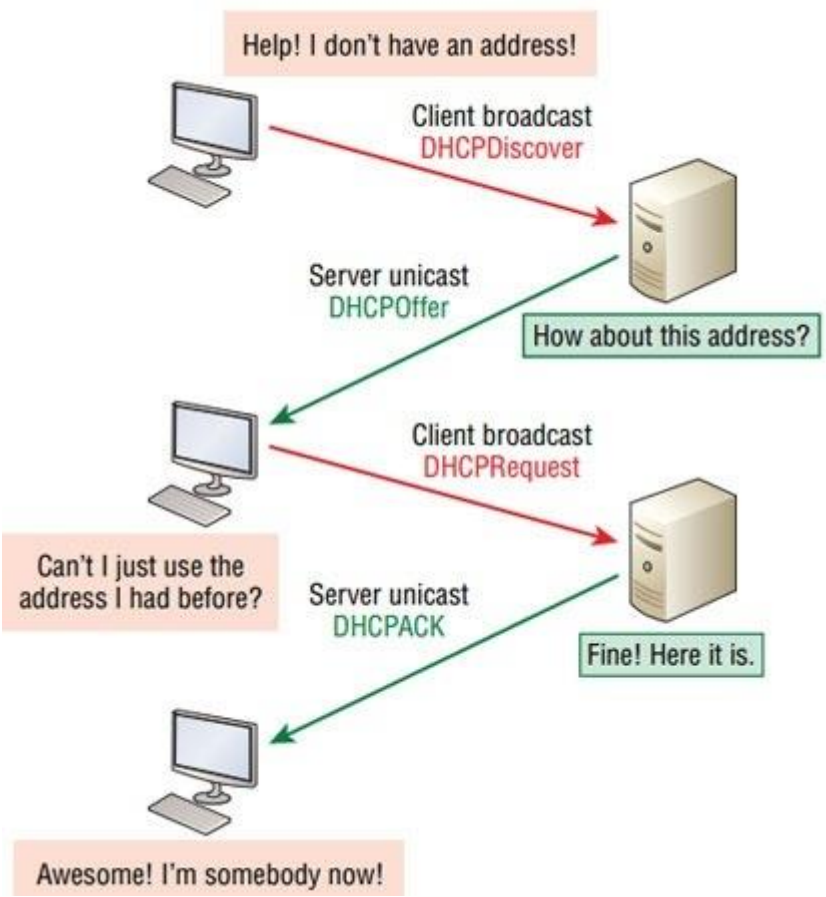
no debug all

DHCP

Dynamic Host Configuration Protocol (DHCP) is een computerprotocol dat beschrijft hoe een computer dynamisch zijn netwerkinstelling (zijn ip-adres) van een DHCP-server kan verkrijgen. Het DHCP-protocol is gebaseerd op het Internet Protocol IP en werkt met UDP-pakketten.

Werking van DHCP

Opmerking : Een broadcast message gaat niet verder dan de router.
De router houdt broadcast messages tegen.
Met het commando: **ip helper-address** kun je berichten voor een DHCP doorsturen. Dit noemen ze een ***Relay-Agent*** Handig voor als je DHCP server op een ander netwerk zit.



Instellen van een relay-agent

Het configureren hiervan gebeurt op de interface die het broadcast packet binnen krijgt. Op een Multilayer Switch is dit het VLAN.

```
SW-CORE(config-if)#int vlan 30
SW-CORE(config-if)#ip helper-address 172.16.40.10
```

Wat is een Relay-Agent

In grotere netwerkomgevingen met vele subnetten en verschillende IP-reeksen is het niet efficiënt om één DHCP-server per LAN/subnet op te zetten en te onderhouden. Voor dergelijke netwerken zal men er daarom de voorkeur aan geven om te werken met een of meer centrale DHCP-servers die IP-adressen kunnen toewijzen voor verschillende LANs/subnetten. Dit betekent echter dat DHCP-verkeer tussen de verschillende LANs en de DHCP-server mogelijk moet zijn, waarbij er toestellen op hogere lagen dan de datalinklaag, zoals routers, moeten worden gepasseerd. Om dit toe te laten kan men werken met *DHCP-relay-agents*.

Hoe stel je het in?

DHCP Snooping

DHCP Snooping en snuffelen is de letterlijke vertaling. En het is één van de belangrijkste default security settings in je netwerk. Hiermee zorg je ervoor dat er maar één DHCP in je netwerk kan zijn.

Waarom DHCP snooping?

Waarom is dat belangrijk? Ooit gehoord van DHCP Starvation Attack? Met deze attack kunnen hackers ervoor zorgen dat nieuwe devices *geen* ip-adres ophalen. Dat is voor de gebruiker vervelend. En jij als netwerkbeheerder hebt een dagtaak hebt om de oorzaak te achterhalen.

Begrippen DHCP snooping

- snooping trust
- snooping event
- snooping limit rate
- snooping packet

Configuring DHCP snooping

Het configureren van DHCP-snooping op een switch heeft de volgende stappen.

- DHCP-snooping is standaard uitgeschakeld op switches. Om deze functie te gebruiken, moeten we deze eerst inschakelen.

- DHCP-snooping werkt per VLAN-basis. Zodra DHCP-snooping is ingeschakeld, moeten we het VLAN opgeven waarop we dit willen toepassen. Je kunt Één VLAN of meerdere VLAN's specificeren. Om Één VLAN te configureren, voer je Één VLAN-nummer in. Om een €‹€‹reeks VLAN's te configureren, voert u een begin- en een eind-VLAN-nummer of een streepje en het bereik van VLAN's in.

- DHCP-snooping behandelt alle poorten van het opgegeven VLAN als de trusted (vertrouwde) poorten. Een untrusted poort is een poort die geen DHCP-packets (berichten) accepteert. Met andere woorden, als een apparaat is aangesloten op een untrusted poort, kan het IP-configuratie verkrijgen van de DHCP-server, maar het kan geen IP-configuratie aanbieden. Het wordt Één richtingsverkeer.

- Als er een DHCP-server op de poort is aangesloten, moeten we die poort configureren als de trusted (vertrouwde) poort. Een vertrouwde poort is een poort die DHCP-serverberichten accepteert. Met andere woorden, een DHCP-server kan alleen IP-configuratie bieden als deze is aangesloten op een vertrouwde poort.

DHCP-Snooping commands

De volgende tabel bevat de opdrachten die worden gebruikt om DHCP-snooping op Cisco-switches te configureren en te verifiëren.

Command	Description
Switch(config)# ip dhcp snooping	To enable DHCP snooping globally.
Switch(config)# ip dhcp snooping vlan number [number]	To enable DHCP snooping on the specified VLAN.
Switch(config-if)# ip dhcp snooping trust	To configure the interface as a trusted interface.
Switch(config-if)# ip dhcp snooping limit rate [rate]	To limit the number of DHCP packets that the interface can receive in a second.
Switch# show ip dhcp snooping	To view DHCP snooping configuration and status
Switch# debug ip dhcp snooping event	To debug DHCP snooping events.
Switch# debug ip dhcp snooping packet	To view DHCP messages and packets.

DHCP snooping voorbeeld

Stel dat op je switch de DHCP server op Interface fa/04 is aangesloten. Dit is dus je trusted poort. Gebruik dan de volgende commando's

```
Switch(config)#interface fa0/4
Switch(config-if)#ip dhcp snooping trust
```

Rate-Limit

Met het commando limit rate kun je aangeven hoeveel DHCP berichten over je netwerk gaan. Hiermee voorkom je een DHCP Starvation Attack. Als er meer dan zoveel DHCP aanvragen per seconden worden verstuurd dan kan de DHCP pool leegraken. Je kan daarom met het volgende command de limit aangeven. Deze limit kun je plaatsen op een *trusted* als een *untrusted* poort.

```
ip dhcp snooping limit rate [number]
```

DHCP Snooping controleren

De configuratie kun je bekijken met : Show ip DHCP snooping

Debuggen

Met de volgende commando's kun je debug messages bekijken

```
debug ip dhcp snooping event
```
en
```
debug ip dhcp snooping packet
```

VPN

Een VPN is een verbinding die gemaakt wordt via het internet tussen twee LAN's (Local Area Network) of tussen een pc op het internet en een LAN. Er wordt als het ware een tunnel door het internet gecreëerd waardoor veilig informatie verzonden kan worden.

Wat zijn de voordelen?

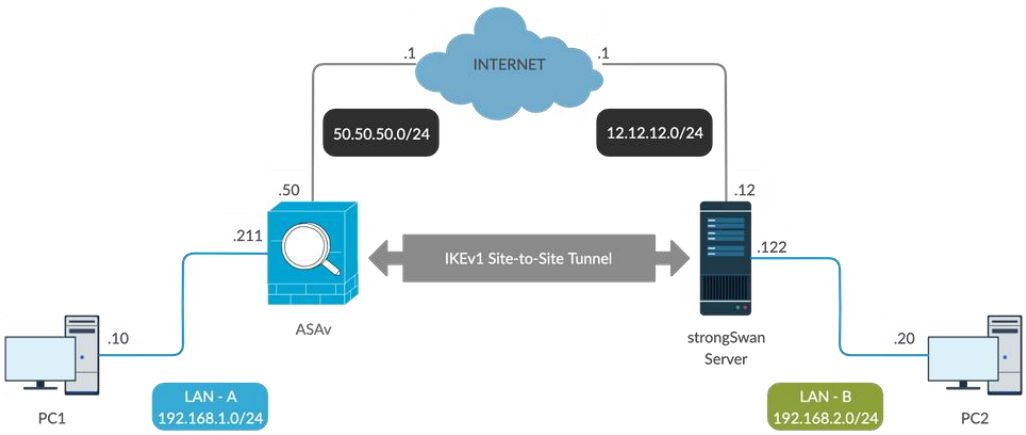
1) **Kosten besparen** Je kan makkelijk een beveiligde verbinding opzetten vanuit huis over een internetverbinding zoals Ziggo.

2) **Scalability** Je kan makkelijk de infrastructuur uitbreiden.

3) **Security** VPN tunnels zijn veilig omdat data wordt versleuteld met een sterke codering.

Welke type vpn's zijn er?

- **Dynamic Multipoint VPN (DMVPN)** Meerdere routers zijn met elkaar verbonden
- **Remote Accces VPN** Bijvoorbeeld voor thuiswerkers
- **Site-to-Site VPN** Tunnel tussen een sites (twee of meer bedrijven).



GRE

Generic Routing Encapsulation (GRE) is een non-secure, site-to-site VPN tunneling protocol. Het is gemaakt door Cisco. GRE kan ip-verkeer tussen meerdere sites versturen.

Figuur 1Gre

Tu0 = Tunnel (meestal een public-ip)
L0 = Local Interface IP

Hoe een GRE verbinding configureren?

In zes stappen een GRE tunnel instellen.

Stap 1. Maak een tunnel interface **interface tunnel** *number* command.

Stap 2. Maak een IP address voor de tunnel interface. (private address)

Stap3. Geef de tunnel source adres. De kant die verbonden is met het internet

Stap 4. Geef de destination adres. De router waarmee je verbinding wilt maken.

Stap 5. (Optional) Specify GRE tunnel mode as the tunnel interface mode.

Stap 6. Stel een OSPF netwerk in. En publiceer je private netwerken.

Voorbeeld uitwerking:

Zie ook Figuur 1Gre

RouterA (R1)

```
R1(config)# interface Tunnel0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# tunnel source [interface]
R1(config-if)# tunnel destination 10.10.10.1
R1(config-if)# tunnel mode gre ip
R1(config-if)# exit
R1(config)# router ospf 1
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

RouterB (R2)

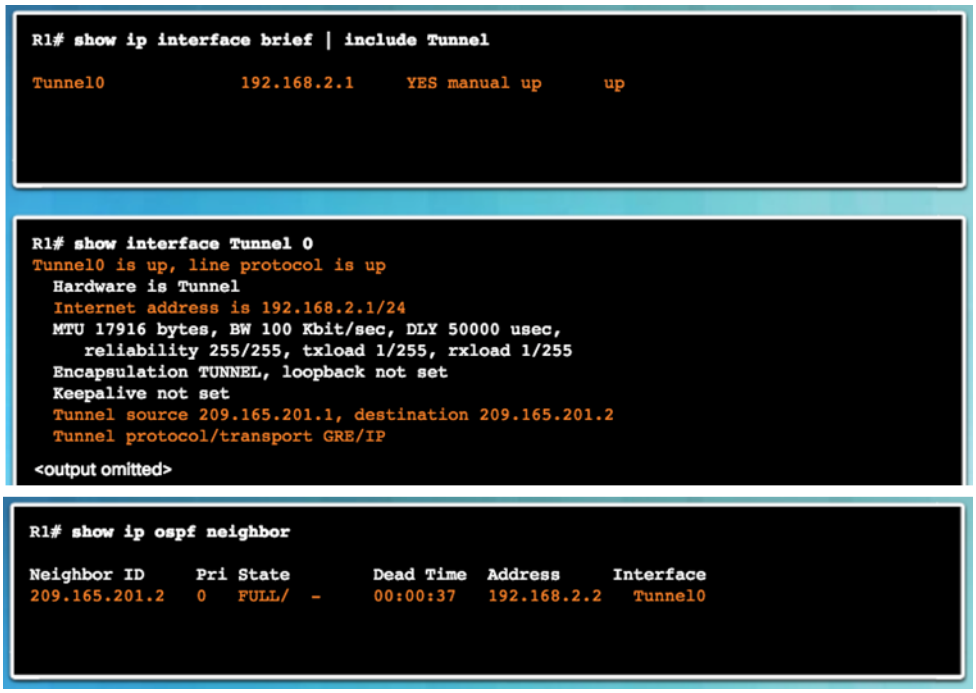
```
R2(config)# interface Tunnel0
R2(config-if)# ip address 192.168.1.2 255.255.255.0
R2(config-if)# tunnel source [interface]
R2(config-if)# tunnel destination 10.10.10.2
R2(config-if)# tunnel mode gre ip
R2(config-if)# exit
R2(config)# router ospf 1
R2(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

Troubleshooting GRE

1. Controleer of de tunnel ip-adressen kloppen. Het kan zijn dat het subnetmask niet klopt. Gebruik dan **`show ip interface brief`** command.

2. Er is geen route opgenomen met OSPF. Gebruik **`show ip route`** or **`show ip ospf neighbor`** om te zien of de private networks zijn opgenomen.

3. Controleer of de tunnel-modes gelijk zijn. Als de tunnel van R1 anders is als die van R2 dan kunnen ze elkaar niet begrijpen.

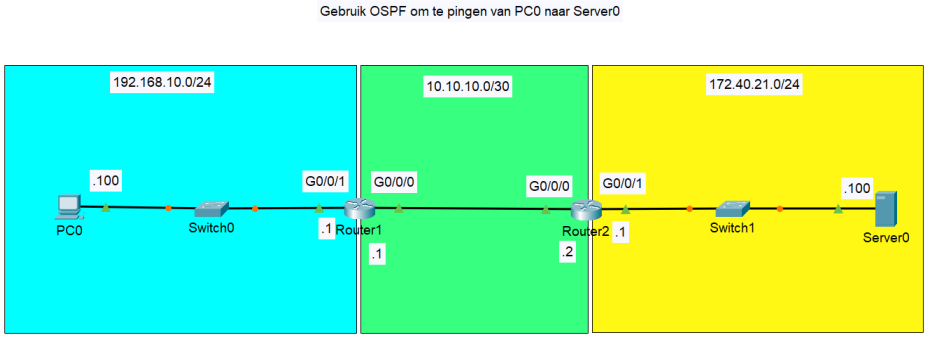


OSPF

Open Shortest Path First (OSPF) is een open en dynamisch routeringsprotocol dat routers in staat stelt om automatisch de snelste route te vinden. Je vindt protocol ook in Google Maps voor het bepalen voor de korste route van huis naar werk.

OSPF is een link-state protocol. Dat wil zeggen dat bij wijzigingen in bijvoorbeeld de bekabeling of een router die uit gaat, de routers daarna een nieuwe snelle route berekenen.

OSPF stuurt Link-State Advertisement (LSA) om elkaar op de hoogte te houden van de snelste route.



Voordat je begint

Met het commando **show ip route** kun je de route tabel uitlezen. Hier kun je zien welke routes er al bekend zijn op de router.
Een C route is direct verbonden.
Een L route is het lokale IP-adres.
Een *dynamische route* krijgt bijvoorbeeld **R**, **O** of **D**

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.10.10.0/30 is directly connected, GigabitEthernet0/0/0
L       10.10.10.1/32 is directly connected, GigabitEthernet0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0/1
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0/1

Router#
```

Instellen van OSPF

Commands op Router 1

```
router ospf 1

network 10.10.10.0 0.0.0.3 area 0

network 192.168.10.0 0.0.0.255 area 0

router-id 10.10.10.1
```

Commands op Router 2

```
router ospf 1

network 10.10.10.0 0.0.0.3 area 0

network 172.40.21.0 0.0.0.255 area 0

router-id 10.10.10.2
```

Voor het router-id kun je het IP-adres gebruiken van de router.

Testen

Met het commando kun je zien of OSPF werkt:

```
show ip ospf neighbor
```

controleer in het resultaat dat er FULL/BDR staat. Dat betekent dat er een OSPF link is.

```
R3#show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface
192.168.23.2 1 FULL/BDR 00:00:36 192.168.23.2 FastEthernet0/0
```

Check ook of er een route is aangemaakt. Deze herken je dan aan de letter “O”

```
show ip route
```

Back-uppen en Updates

Backuppen gaat vaak via TFTP (Trivial File Transfer Protocol). Het is een eenvoudig type bestandsoverdracht protocol dat wordt gebruikt voor het overdragen van configuraties of kleine bestanden. Het protocol is op UDP gebaseerd.

Informatie over het TFTP Protocol

Port : UDP 69
Max filesize : 4GB
Verzenden in octects (binair of ascii)

Hoe back-uppen?

Je kan je running of startup-config naar een TFTP of FTP server uploaden. Je gebruikt dan de volgende commando's:

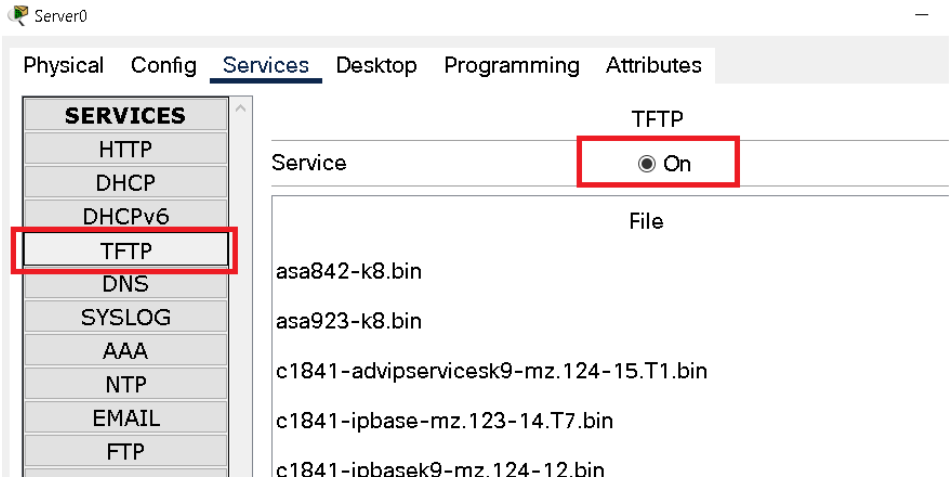
```
CE_2#copy running-config tftp:

Address or name of remote host []? 64.104.207.171
Destination filename [ce_2-confg]? backup_cfg_for_my_router
!!
1030 bytes copied in 2.489 secs (395 bytes/sec)
CE_2#
```

```
Router#copy tftp: running-config

Address or name of remote host []? 64.104.207.171
Source filename []? backup_cfg_for_my_router
Destination filename [running-config]?
Accessing tftp://10.66.64.10/backup_cfg_for_my_router...
Loading backup_cfg_for_router from 64.104.207.171 (via
FastEthernet0/0): !
```

Bestanden via TFTP komen dan op je server



Updaten van een IOS File

Cisco update kun je downloaden van de website. Je moet hiervoor wel een geldig account hebben. Na de aanschaf van een router/switch van Cisco krijg je ook toegang tot deze website om updates te downloaden.
Voordat je gaat updaten: Zorg voor een backup van de bestaande .bin file. Dit is je bestaande OS. Je kan net als een configfile je .bin file uploaden naar een TFTP server.

Voorbeeld Cisco update .bin file.

c2800nm-adventerprisek9-mz.151-4.M10.bin

Naamgeving update file : type-OS-features-versie.bin

Check eerst of je op je flash voldoende ruimte hebt.

Het updaten van een Cisco IOS file gaat via het volgende commando:

```
R1#copy flash: tftp:
Source filename []? c2800nm-adventerprisek9-mz.151-4.M10.bin
Address or name of remote host []? 192.168.1.200
Destination filename [c2800nm-adventerprisek9-mz.151-4.M10.bin]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
67926080 bytes copied in 312.508 secs (217358 bytes/sec)
```

NTP

NTP staat voor Network Time Protocol, netwerk tijd protocol. Het zorgt ervoor dat de datum en tijd automatisch wordt geüpdatet. Je hebt hiervoor een NTP server nodig. Online vind je veel NTP servers : een bekende is *www.ntp.org*.

```
device#(config) ntp peer ip-address
```

Port-Security

Switch-poortbeveiliging beperkt het aantal geldige MAC-adressen dat op een poort is toegestaan. Wanneer een MAC-adres of een groep MAC-adressen is geconfigureerd om switchpoortbeveiliging in te schakelen, zal de switch pakketten alleen doorsturen naar de apparaten die deze MAC-adressen gebruiken. Elk pakket dat van een ander apparaat komt, wordt door de switch gedropped (weggegooid) zodra het op de switchpoort aankomt.

Wat is het verschil tussen Dynamic en Sticky?

- Dynamic secure MAC addresses na een herstart van de switch zullen de geleerde mac-adressen worden vergeten.

- Sticky secure MAC addresses Geleerde mac-adressen worden opgeslagen in de config. Na een herstart blijft het mac-adres staan.

Welke violation modes zijn er?

- protect Wanneer het maximaal aantal mac-adressen is bereikt dan worden de andere pakketten gedropped. Er komt geen melding in de switch.

- restrict Wanneer het maximaal aantal mac-adressen is bereikt dan worden de andere pakketten gedropped. Er komt een melding in de switch. Je kan dan met SNMP de switch uitlezen.

- shutdown Schakelt de port uit zodra het maxium mac-adressen is bereikt.

Hoe maak je een dynamic-port aan?

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
```

Hoe maak je een sticky-port aan?

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config)if)#switchport port-security maximum 10
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation restrict
```

Hoe kun je zien wat de port-status is?

Command : **show port-security address**

Spanning-Tree Protocol

Wat is STP?

Het **spanning Tree protocol** is een layer twee techniek die netwerk loops ook wel **broadcast storm** genaamd **voorkomt** op je netwerk. Met het Spanning Tree Protocol kan je ook redundantie tussen verschillende switchen gaan opbouwen. En dit is het hoofd doel van het Spanning Tree Protocol.

Hoe werkt STP?

Wanneer een Switch opstart zijn er vier fases waar een Switch doorheen gaat.

– Blocking (20 seconden)
– Listening (15 seconden)
– Learning (15 seconden)
– Forward

In de Listening fase stuurt de switch **BDU** messages. Speciale packeten om te bepalen waar de eventuele loops zitten en wie de root-bridge is.

De Root Bridge wordt geselecteerd op basis van de Bridge ID, The Bridge ID is het MAC-adres van de Switch. De Root-Bridge is dus de switch met het laagste Bridge ID.

Welke commado's kun je gebruiken?

`Switch0#show spanning-tree`	Geeft een overzicht wie de root-brigde is en het bridge-ID.
`Switch0# show spanning-tree interface fa0/1`	Geeft het STP protocol specifiek voor een VLAN of interface.

`Switch(config)#spanning-tree ?`
`  mode  Spanning tree operating mode`
`  portfast  Spanning tree portfast options`
`  vlan  VLAN Switch Spanning Tree`
	In configure mode kun je spanning-tree gebruiken om een ander protocol te kiezen.

Welke verschillende protocollen zijn er?

STP. Spanning Tree-protocol (IEEE 802.1D). Vormt een loopvrije verbinding van switches. Eenvoudig protocol dat standaard op elke switch aanwezig is.

PVSTP. Per-VLAN Spanning Tree-protocol . Het eigen protocol van Cisco waarmee elk VLAN in een netwerk een onafhankelijke spanning tree met een onafhankelijke root kan uitvoeren in plaats van een enkele topologie voor alle VLAN's te forceren.

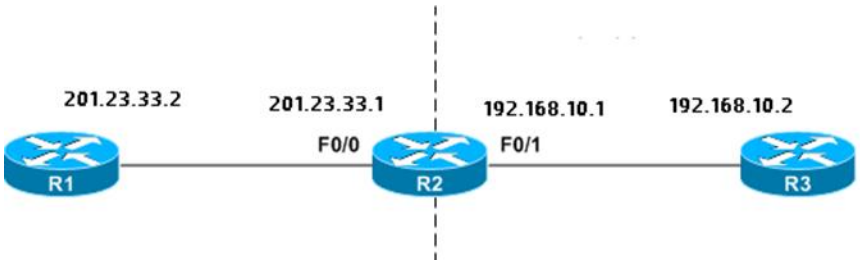
RSTP. Rapid Spanning Tree-protocol (IEEE 802.1w). Een betere versie van het spanning tree-protocol met een snellere convergentietijd (snelle opstarttijd).

EtherChannel. Een Cisco-techniek die de mogelijkheid biedt om meerdere fysieke interfaces te bundelen tot één enkele, logische koppeling met een hogere snelheid. Hiermee kun je twee poorten van 1Gbit bundelen tot een 2Gbit poort. (Liever geen Cisco? Gebruik dan IEEE 802.3ad Link- aggregation)

NAT

Wat is NAT?

NAT staat voor Network Address Translation. Je gebruikt NAT om op internet te kunnen komen. NAT wordt gebruikt om IP-adressen om te zetten van private naar public. NAT zorgt letterlijk voor een vertaling.



Hoe werkt dit?

Voorbeeld: Je laptop thuis heeft een 192.168.10.10 private adres. Een private adres kan niet op internet. Een router met NAT kan dan jouw adres omzetten naar een public adres. Bijvoorbeeld naar 201.23.33.1. Dit adres is public en kan op internet.

NAT Begrippen

Bij NAT komen de volgende begrippen die je echt wel moet kennen. Als je deze begrippen niet begrijpt dan zal NAT lastig te begrijpen zijn. Oefenen is daarom belangrijk. Begrippen die je moet kennen zijn.

- Private adres
- Public adres
- Inside Global
- Inside Local
- Outside Local
- Outside Global
- Dynamic NAT
- NAT Overload (Ook wel PAT genoemd)
- Static NAT

Private adressen

Private adressen zijn adressen die je privé gebruikt. Of in een kantoornetwerk gebruikt. Deze adressen kunnen niet op internet.

Class A	10.0.0.0 - 10.255.255.255
Class B	172.16.0.0 - 172.31.255.255
Class C	192.168.0.0 - 192.168.255.255

Public adressen

Een public adres kan wel het internet op zoals 8.8.8.8 (Google DNS Server).

Met de website https://www.whatismyip.com/ kun je al snel je eigen public adres bekijken.

NAT Types

NAT Static is het Één op Één vertalen van een private naar een public adres. Dat betekent dat Één computer gebruik kan maken van Één public adres. Handig voor je (Web of Minecraft) server.

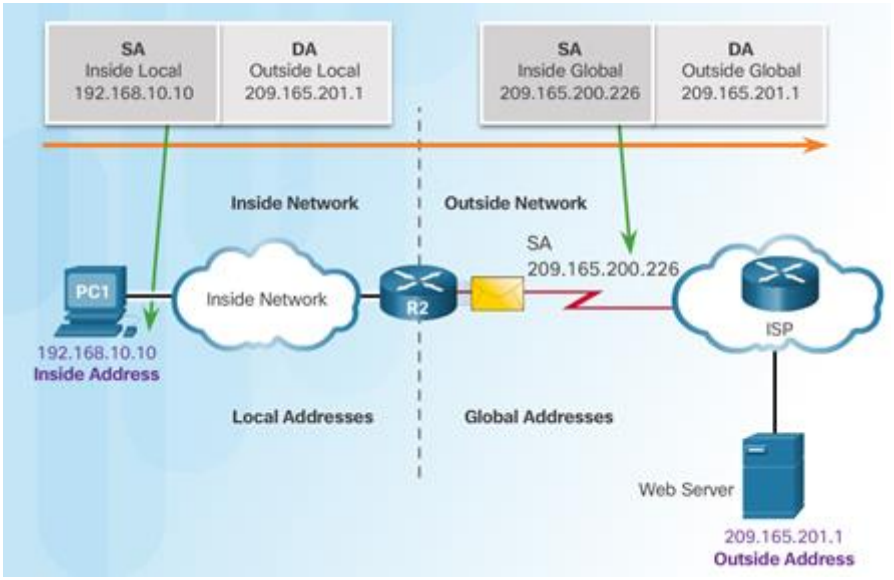
NAT Overload zorgt dat meerdere computers verbinding kunnen maken met het internet. Handig als je een thuis/kantoor netwerk hebt waar meerdere computer het internet op moeten kunnen.

NAT Inside/Outside

Je hebt vier termen : Inside, Outside, Local en Global. Wat betekenen deze termen?

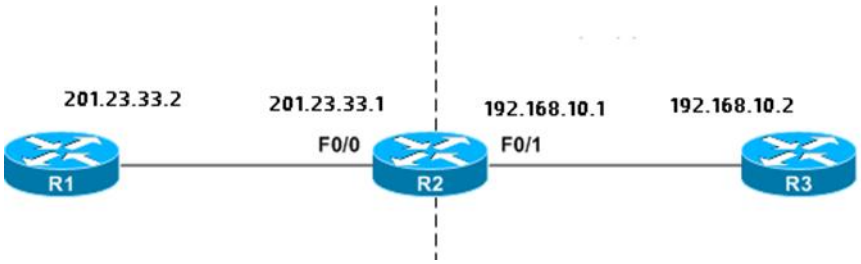
Het zijn begrippen bij het configureren van NAT in een router. Het netwerk met publieke adressen zijn is je Outside netwerk. Adressen met private adressen zijn Inside Netwerk. Adressen in je Inside netwerk hebben dan een Local adres. Adressen in je outside netwerk hebben dan een Global.

Kijk eens goed naar onderstaande afbeelding. Het adres 209.165.200.226 is een Inside Global. Waarom is dat denk je? Het zou toch een outside adres moeten zijn? Maar dit adres hoort bij de router R2. En is het publieke IP van R2.



Oefening NAT

Kijk naar de volgende tekening en noteer de juiste adressen in de tabel.



Inside Local	Inside Global	Outside Local	Outside Global

Configureren NAT Overload

Het configureren van NAT Overload (PAT) op R2 gaat als volgt:

```
interface FastEthernet0/0
   ip address 201.23.33.1 255.255.255.0
   ip nat outside

interface FastEthernet0/1
   ip address 192.168.10.1 255.255.255.0
   ip nat inside

access-list 1 permit 192.168.10.0 0.0.0.255
ip nat inside source list 1 interface FastEthernet0/0 overload
```

Configureren NAT Static

```
interface FastEthernet0/0
   ip nat outside

interface FastEthernet0/1
   ip nat inside
ip nat inside source static 192.168.10.20  201.23.33.1
```

Hierarchical Network Design

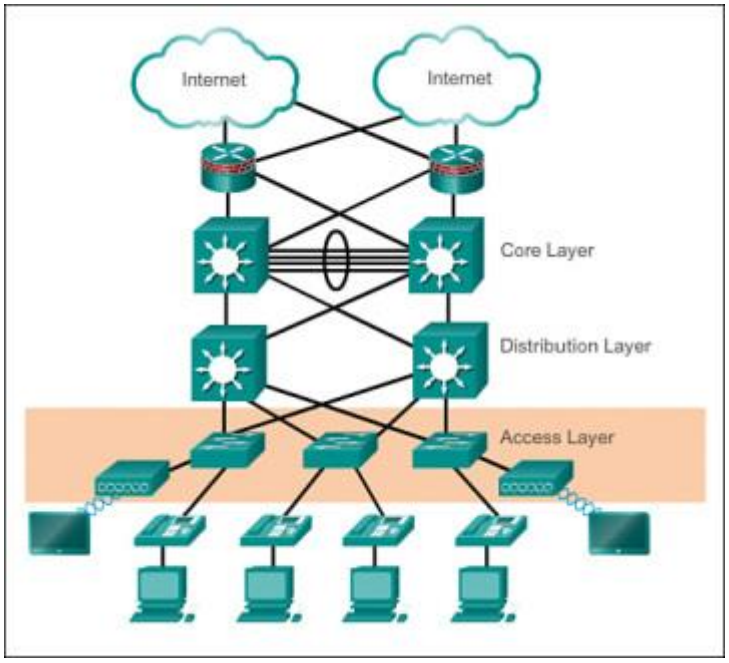
Een typisch hiërarchisch LAN-netwerk voor ondernemingen omvat de volgende **drie** lagen:

Accesslayer

Biedt werkgroep-/gebruikers toegang tot je netwerk.
Vaak komen hier je *werkstations*, *laptops*, *accesspoints* etc. Alles waar gebruikers mee werken.

Belangrijke functies:

- Laag 2 switches
- Hoge beschikbaarheid
- Poortbeveiliging (Port Security)
- QoS
- Power over Ethernet (PoE) en extra VLAN's voor VoIP

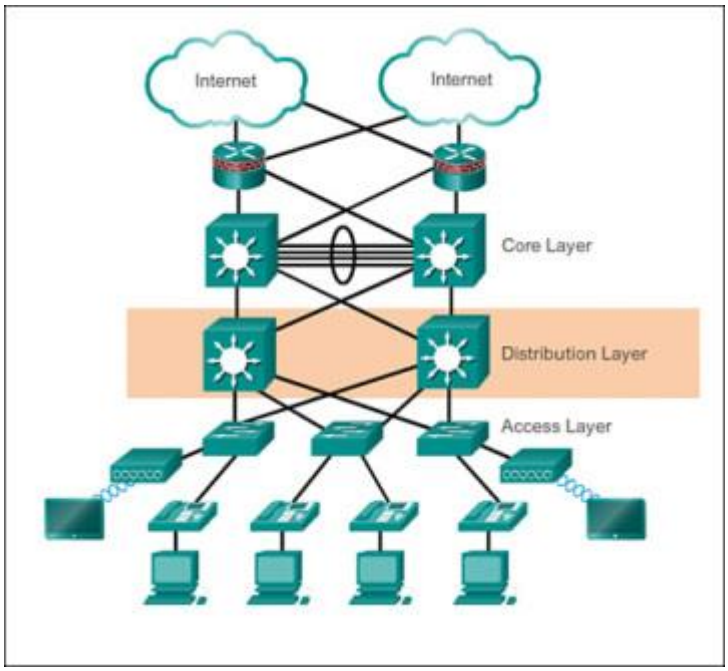


Distributionlayer

Zorgt voor de verdeling van het netwerkverkeer en controleert de grens tussen de access- en corelayer.
Deze laag zorgt ervoor dat verkeer tussen de *acceslayer* en *corelayer* soepel verloopt; het verdeelt het verkeer.

Belangrijke functies:

- Beveiliging in de vorm van access control lists (ACL's) en filtering.
- Routingservices tussen LAN's en VLAN's en tussen routeringsdomeinen (bijv. EIGRP of OSPF).
- Redundantie en load-balancing.

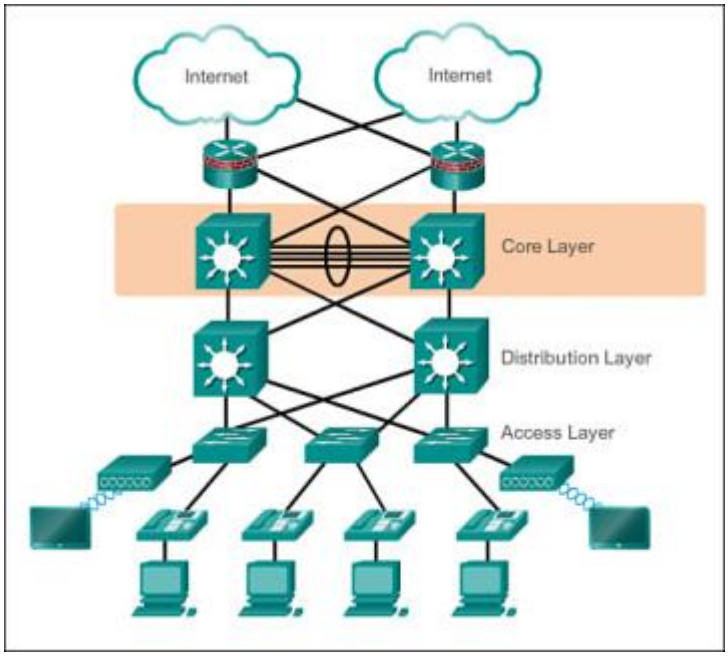


Corelayer

zorgt voor snel transport tussen distributieswitches binnen het bedrijf.
Deze laag is bedoelt voor toegang tot het internet en of de *servers* binnen het netwerk.

Belangrijke functies:

- Snelle netwerkpoorten (Gigabit of hoger)
- Betrouwbaarheid en fouttolerantie (port-channel).
- Geen CPU intensieve controle op ip-pakketen door acl of andere vorm van ip-filtering.



Afbeeldingen van :
https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

Cisco commando's

Elk commando van Cisco kan op een bepaald niveau (Prompt) worden uitgevoerd. Een commando met een letter G betekent dat deze alleen in configure-terminal kan worden uitgevoerd.

Prompt	Afkorting	Omschrijving
Router>	**U**	User EXEC mode, is the first level of access.
Router#	**P**	Privileged EXEC mode. The second level of access, accessible with the "enable" command.
Router(config)#	**G**	Configuration mode. Accessible only via the privileged EXEC mode.
Router(config-if)#	**I**	Interface mode. Level accessible via configuration mode.
Router(config-router)#	**R**	Routing mode. Level within configuration mode.
Router(config-line)#	**L**	Line level (vty, tty, async). Accessed via the configuration mode
Router(config-vlan)#	**V**	Config-vlan, accessible via the global configuration mode.
Switch(vlan)#	**VD**	Vlan database, accessible from the privileged EXEC mode.

Navigatie commando's

Commando	Mode	Omschrijving
enable	U	Moves from User to Privileged mode.
logout	U	Exit User mode.
configure <terminal>	P	Moves from Privileged to Configure mode.
disable	P	Exit user mode.
Interface <interface description>	G	Enter interface configuration mode.
vlan vlan-id	G	Moves to configure vlan mode.
Vlan database	P	Enter vlan database from Privilege mode.
line	G	Enter line from Global configuration mode.
exit end	G, R, L, V	return to previous mode.

Basic Configuration

Meest gebruikte commando's voor eenvoudige installaties.

Commando	Mode	Omschrijving
show version	U,P	Display information about IOS and router.
show interfaces	U,P	Display physical attributes of the router's interfaces.
show ip route	U,P	Display the current state of the routing table.
show access-lists	P	Display current configured ACLs and their contents.
show ip interface brief	P	Displays a summary of the status for each interface.
show running-config	P	Display the current configuration.
show startup-config	P	Display the configuration at startup.
enable	U	Acces Privilege mode
config terminal	P	Access Configuration mode.
interface <int>	G	Enter interface configuration.
ip address <ip address> <mask>	I	Assign an IP address to the specified interface.
shutdown no shutdown	I	Turn off or turn on an interface. Use both to reset.
description <name-string>	I	Set a description to the interface.
show ip interface <type number>	U,P	Displays the usability status of the protocols for the interfaces.
show running-config interface interface <slot/number>	P	Displays the running configuration for a specific interface.
hostname <name>	G	Set a hostname for the Cisco device.
enable secret <password>	G	Set an "enable" secret password.
copy running-config startup-config	P	Saves the current (running) configuration in the startup configuration into the NVRAM. The command saves the configuration so when the device reloads, it loads the latest configuration file.
copy startup-config running-config	P	It saves (overwrites) the startup configuration into the running configuration.

copy from-location to-location	P	It copies a file (or set of files) from a location to another location.
erase nvram	G	Delete the current startup configuration files. The command returns the device to its factory default.
reload	G	Reboot the device. The NVRAM will take the latest configuration.
erase startup-config	G	Erase the NVRAM filesystem. The command achieves the similar outcome as “erase nvram”

Commando	Mode	Omschrijving
cdp run no cdp run	P	The “cdp run” command enables Cisco Discovery Protocol. The “no cdp run” disables it.
show cdp	P	Display global information for CDP.
show cdp neighbors	P	Display all CDP neighbors.
lldp run no lldp run	P	The “lldp run” command enables the LLDP Protocol. The “no lldp run” disables it.
show lldp	P	Displays global information for LLDP
show lldp neighbors	P	Show all LLDP neighbors.
show mac address-table	P	Display all the MAC address entries in a table.
spanning-tree mode rapid-pvst	G	A global configuration command that configures the device for Rapid Per VLAN Spanning Tree protocol.
spanning-tree vlan <1-4094> priority <0-61440>	G	Manually set the bridge priority per vlan.
spanning-tree vlan <1-4094> root primary	G	Make the switch the root of the SP.
no spanning-tree vlan <1-4094>	G	Disable SP on the specific VLAN.
show spanning-tree summary	P	Show a summary of all SP instances and ports.
show spanning-tree detail	P	Show detailed information of each port in the spanning-tree process.
show vlan	P	Lists each VLAN and all interfaces assigned to that VLAN. The output does not include trunks.
show vlan brief	P	Displays vlan information in brief
show interfaces switchport	P	Display configuration settings about all the switch port interfaces.
show interfaces trunk	P	Display information about the operational trunks along with their VLANs.
vlan <1-4094>	G	Enter VLAN configuration mode and create a VLAN with an associated number ID.
name <name>	V	Within the VLAN configuration mode, assign a name to the VLAN
switchport mode access	I	In the interface configuration mode, the command assigns the interface link type as an access link.
switchport access vlan <>	I	Assign this interface to specific VLAN.
interface range < > 	I – range	Access interface range configuration mode from Interface Configuration.

channel-group <number>	I – range	Assign the Etherchannel. Set the interface range to a channel group.
no switchport access vlan <>	I	Remove VLAN assignment from interface. It returns to default VLAN 1
show vtp status	P	Display all vtp status
vtp mode <server | client | transparent>	G	In the global configuration mode, set the device as server, client, or transparent vtp mode.
switchport mode trunk	I	An interface configuration mode. Set the interface link type as a trunk link.
switchport trunk native vlan <>	I	Set native VLAN to a specific number.
switchport trunk allowed vlan <>	I	Allow specific VLANs on this trunk.
switchport trunk encapsulation dot1q	I	Sets the 802.1Q encapsulation on the trunk link.

IP Connectivity

Voor het aanmaken van static routes of dynamic routes zoals met OSPF.

Commando	Mode	Omschrijving
Show ip route	P	Show the routing table.
Show ip route ospf	P	Show routes created by the OSPF protocol.
ip default-gateway <ip_address>	G	Set the default gateway for the router.
ip route <network> <mask> <next hop>	G	Create a new static route
no ip route <network> <mask> <next hop>	G	Remove a specific static route.
ip route 0.0.0.0 0.0.0.0 <nex thop>	G	Configure a default route
router ospf <process ID>	G	Enable OSPF with an ID. The command will open the router configuration mode.
show ip ospf interface	P	Display all the active OSPF interfaces

IP Services NAT DHCP en IP-Helper

Commando's voor NAT, DHCP, and DNS.

Commando	Mode	Omschrijving
ip nat <inside | outside>	I	Specific whether the interface is the inside or outside of NAT.
ip nat inside source <ACL No.> <pool | static IP> <overload>	G	Configure dynamic NAT. It instructs the router to translate all addresses identified by the ACL on the pool. To configure Port Address Translation (PAT) use the "overload" at the end.
ip nat inside source static <local IP> <global IP>	G	Create a static NAT from inside (local IP) to outside (global IP)
ip nat outside source static <ACL No.> <pool | static IP>	G	Create a static NAT from outside (ACL) to inside (IP pool)
ntp peer <ip-address>	G	Configure the time by synchronizing it from an NTP server.
ip dhcp excluded-address <first-ip-address> <last-ip-address>	G	The IP addresses that the DHCP server should not assign to the DHCP client.
ip dhcp pool <name>	G	Enters the DHCP pool configuration mode and creates a new DHCP pool.
network <network ID> <mask>	G – DHCP	Inside the DHCP configuration mode. Define the address pool for the DHCP server.
default-router <IP address>	G – DHCP	Set the default gateway IP address for the DHCP clients.
dns-server <IP address>	G – DHCP	Set the DNS server IP address for the DHCP clients.
ip helper-address <ip address>	I	Turns an interface into a DHCP bridge. The interface redirects DHCP broadcast packets to a specific IP.
show ip dhcp pool	P	Display information about the DHCP pool
show ip dhcp binding	P	Display information about all the current DHCP bindings.

ip dns server	G	Enable DNS service.
ip domain-lookup	G	Enable domain lookup service. DNS client
ip name-server <IP address | domain name>	G	Set a public DNS server.
snmp-server community <community-string> ro	G	Enable SNMP Read-Only public community strings.
snmp-server community <community-string> rw	G	Enable SNMP Read-Only private community strings.
snmp-server host <ip-address> version <community-string>	G	Specific the hosts to receive the SNMP traps
logging <ip address>	G	Determines the Syslog server to send log messages.
logging trap level	G	Limit Syslog messages based on severity level
show logging	P	Shows the state logging (syslog). Shows the errors, events, and host addresses. It also shows SNMP configuration and activity.
terminal monitor	P	Enables debug and system's error messages for the current terminal.
sh ip ssh	P	Verify SSH access into the device.

Security commando's

ACL List en PortSecurity

Commando	Mode	Omschrijving
enable secret <password>	G	Set an "enable" secret password. Enable secret passwords are hashed via the MD5 algorithm.
line vty 0 4	G	A global configuration command to access the virtual terminal configuration. VTY is a virtual port used to access the device via SSH and Telnet. 0 4 to allow five simultaneous virtual connections
line console 0	G	A global configuration command to access the console configuration.
password <password>	L	Once in line mode, set a password for those remote sessions with the "password" command.
Login local		The authentication uses only locally configured credentials.
username <username> privilege <level> secret <password>	G	Require a username with a specific password. Also configure different levels of privilege.
service password-encryption	G	Makes the device encrypt all passwords saved on the configuration file.
crypto key generate rsa	G	Generate a set of RSA key pairs for your device. These keys may be used for remote access via SSH.
access-list	G	Defined a numbered ACL
ip access-list	G	Defined an IPv4 ACL.
access-list access-list-number <deny | permit}> source <source> [log]	G	Create a standard ACL.
access-list access-list-number <deny | permit}> protocol <> source <source [ports]>destination <destination [ports]> [Options]	G	Create an extended ACL.
ip access-class <access-list-name> <in | out>	L	A line configuration command mode. It restricts incoming and outgoing connections to a particular vty line. Use "no" to remove the restriction.

no ip access-group <access-list-name> <in | out>		
show ip access-list	P	Show all IPv4 ACLs
switchport mode access	I	From the interface configuration mode, this command assigns the interface link type as an access link.
switchport port-security	I	enable dynamic port security on the specific interface.
switchport port-security maximum <max value>	I	Specify the maximum number of secure MAC addresses on the specific interface.
switchport port-security mac-address <mac-address | sticky [mac-address]>	I	Force a specific mac-address to the interface. Also use the “sticky” option to make the interface remember the first mac-address connected to the interface.
switchport port-security violation <shutdown | restrict | protect>	I	Define the action to be taken when a violation is detected on the port.
show port security	P	Display the port security configuration on each interface.

Troubleshooting commando's

Wanneer het netwerk niet doet wat je had verwacht, kun je met onderstaande commando's het netwerk onderzoeken.

Commando	Mode	Omschrijving
ping <target IP | hostname> <repeat Count [5]> <source [IP | interface]	P	Diagnose connectivity with extended ping. Check reachability, RRTs, and packet loss.
traceroute <target IP | hostname><source [IP | interface]	P	Use traceroute to diagnose connectivity on a hop by hop basis.
telnet	P	Use Telnet to check for listening ports (1 to 65535) on a remote device.
show interface	P	Use this command to discover the physical attributes; find duplex, link types, and speed mismatches. Both ends must match. Also use this command to find errors.
speed <10 | 100 | 1000 | auto>	I	Set the speed of an interface. Or configure it as auto.
duplex <auto | full | half>	I	Set the interface duplex.
show interface | include fastethernet | input errors	P	This command searches across all interfaces and outputs the ones that include input errors.
show ip interface	P	Use this command to discover the status for all the protocols on that interface.
shutdown no shutdown	I	Interface configuration mode. Restart an interface
show ip route	P	This command is useful for determining the route of ip packets.
show cdp neighbors	P	Discover basic information about neighboring Cisco's routers and switches
show mac address-table	P	Display the contents of the mac-address table.
Show vlan Show vlan brief	P	Find vlan status and interfaces assigned to the vlans.

show vtp status	P	Use this command to discover the current VTP mode of the device.
show interfaces trunk	P	Check the allowed VLANs on both ends of the trunk.
show ip flow top-talkers	P	If Netflow is enabled, this command is very useful to troubleshoot top talkers.