Super CheatSheet CCNA2  
  
Switch  
  
Switch – basic config  
  
Switch(config)# **hostname** Switch1  
Switch1(config)# **banner motd #**Enkel toegang voor geautoriseerde gebruikers!! **#**  
(Switch1(config)# enable password pxl) -> niet meer gebruikt  
Switch1(config)# **enable secret** pxl paswoord zetten op mode  
  
Switch1(config)# **service password-encryption** paswoord op console  
Switch1(config)# **line console 0**  
Switch1(config-line)# **password** pxl  
Switch1(config-line)# **login**Switch1(config-line)# **logging synchronous**  
  
Switch1(config)# **line vty 0 15**  paswoord voor telnet  
Switch(config-line)# **password** pxl  
Switch(config-line)# **login**  
Switch1(config-line)# **logging synchronous**  
  
Switch1(config)# **no ip domain-lookups**  beveiligen voor DNS lookup  
  
Instellen Management VLAN (meestal 99)  
  
Switch# **conf t**  
Switch(config)# **vlan 99**  
Switch(config-vlan)# **name** management  
Switch(config-vlan)# exit  
Switch(config)# **interface vlan 99**  
Switch(config-if)# **ip address** 172.17.99.2 255.255.0.0 ip zelf kiezen  
Switch(config-if)# **no shutdown**  aanzetten poort  
Switch(config-if)# end  
  
Op poort waar management computer is aangesloten:  
Switch# **conf t**  
Switch(config)# **interface fastethernet 0/1** naam van de poort  
Switch(config-if)# **switchport mode access**Switch(config-if)# **switchport access vlan 99**  
Switch(config-if)# end

Instellen standaard route:  
Switch# **conf t**  
Switch(config)# **ip default-gateway** 172.17.99.1  
  
Opslaan configuratie:  
Switch# **copy running-config start-up config**  
  
controleren of alles correct is verlopen:  
Switch# **show ip interface brief**  
  
controleren vlans:  
Switch# **show vlan**  
  
opvragen MAC adres tabel:  
Switch# **show mac-address-table**  
  
opvragen dynamisch geleerde MAC adres tabel:  
Switch# **show mac-address-table dynamic**  
  
verwijderen geleerde MAC adressen:  
Switch# **clear mac-address-table dynamic**  
  
instellen statisch mac adres op een poort:  
Switch(config)# **mac-address-table static** 0003.e498.c978 **vlan** 99 **interface** fa 0/1

Of beveiligen door vastzetten van een mac adres:  
Switch(config)# **no mac-address-table static** 0003.e498.c978 **vlan** 99 **interface** fa 0/1  
Switch(config)# **interface** fastethernet 0/1  
Switch(config-if)# **switchport mode access**Switch(config-if)# **switchport port-security**  
Switch(config-if)# **switchport port-security mac-address** 0003.e498.c978  
  
Geleerde en statische mac addressen laten opnemen in running-config:  
Switch(config-if)# **switchport mode access**  
Switch(config-if)# **switchport port-security mac-address sticky**  
  
Aantal MAC adressen per pport beperken:  
Switch(config-if)# **switchport mode access**  
Switch(config-if)# **switchport port-security maximum** 20  
  
Switch resetten:  
Switch> enable  
Switch# show flash  
Switch# delete vlan.dat  
Switch# erase startup-config  
Switch# reload  
  
Configureren van Switchpoorten  
  
verbinding: full, half of auto  
snelheid: 10 , 100 of auto  
auto-mdix: medium, dependent, interface, crossover  
  
Switch# **config t**  
Switch(config)# **interface** fastethernet 0/1  
Switch(config-if)# **duplex auto**  
Switch(config-if)# **speed auto**  
Switch(cofnig-if)# **mdix auto**  
Switch(cofnig-if)# **end**  
  
controleren auto-mdix aanstaat:  
Switch# show controllers ethernet-controller fa 0/1 phy | include Auto-MDIX  
  
Switch Security (SSH) + (Port Security)  
  
**SHH instellen** (switch moet unieke naam hebebn in het netwerk):  
Switch# **config t**  
Switch(config)# **Hostname** S1  
S1(config)# **name** student  
S1(config)# **ip domain-name** cisco.com  
S1(config)# **crypto key generate rsa**The name for the keys will be : S1.cisco.com  
How many bits in the modulus [512]: **1024**  
% generating 1024 bit RSA keys, keys will be non-exportabme..  
  
S1(config)# **username** admin **secret** pxl gebruiker en pw aanmaken  
S1(config)# **line vty 0 15**  
S1(config-line)# **transport input ssh**  
S1(config-line)# **login local**S1(config-line)# end

Password uitschaken = **na line vty 0 15 het commando no password (huidig password)**  
  
Kiezen voor SSH versie 2:  
S1(config)# **ip ssh version 2**

DHCP snooping voorkomen:  
echte DHCP server op trusted poort en alle andere pporten untrusted  
S1(config)# **ip dhcp snooping**  
S1(config)# **ip dhcp snooping vlan** 10,20  
S1(config)# **interface fastetehernet** 0/1  
S1(config-if)# **ip dhcp snooping trust**  
S1(config)# **interface fastethernet** 0/2  
S1(config-if-# **ip dhcp snooping limit rate 5**

**PORT SECURITY**  
  
Instellen poortbeveiliging met STICKY MAC adressen:  
S1(config)# **interface fastethernet** 0/1  
S1(config-if)# **switchport mode access (moet niet altijd)**  
S1(config-if)# **switchport port-security**S1(config-if)# **switchport port-security maximum 50**  
S1(config-if)# **switchport port-security mac-address sticky**

Packets droppen bij violation van unknown source maar ports niet disabled:  
**switchport port-security violation restrict**

Ongebruikte switchpoorten afzetten:  
S1(config)# **interface range fastethernet** 0/3-24  
SA(config-if-range)# shutdown  
  
Opvragen van poortbeveiliging:  
S1# **show port-security interface** fa 0/1  
  
Opvragen adressen behorende tot een poortbeveiligingsgroep:  
S1# **show port-security address**  
  
VLAN

Om te kunnen telnetten in een switch moet de switch een ip adress hebben dit doe je door een vlan te maken, de vlan een ip te geven en dan een interface aan de vlan toe te voegen.  
  
Aanmaken en configureren  
  
Switch# **config t**  
Switch(config)# **vlan** 10 nr van de vlan  
Switch(cofnig-vlan)# **name** student naam van de vlan  
Switch(config-vlan)# exit  
  
Databank van de vlan’s  
Switch# **show vlan brief**  
  
Vlan toevoegen aan een poort (tagged):  
Indien de vlan nog niet bestaat wordt ze aangemaakt.  
interface modus: access, dynamic of trunk  
Switch# **config t**Switch(config)# **interface fastethernet** 0/1  
Switch(config-if)# **switchport mode access**  
Switch(config-if)# **switchport access vlan** 10  
Switch(config-if)# end

Troubleshooting: checken op trunk ports op een switch!! Voor doorgeven vlans tussen switches!!  
Switch(config)# **show interface trunk**  
  
Info per poort opvragen:   
Switch# **show interface fa** 0/1 **switchport**  
Vlan volledig VERWIJDEREN van een switch:  
Switch(config)# **no vlan** 20  
  
Alle Vlan’s verwijderen en switch factory reset geven:  
Switch# erase flash:vlan.dat  
Switch# erase startup-config  
Switch# reload  
  
VLAN Trunks  
  
Poorten die meerdere VLAN’s moeten doorlaten moeten in TRUNK staan!!  
  
Switch(config)# **interface fa** 0/4  
Switch(config-if)# **switchport mode trunk**  
  
Instellen NATIVE VLAN (om pakketen door te sturen die niet tot een vlan behoren):  
Switch(config)# **interface fa** 0/4  
Switch(config-if)# **switchport trunk native vlan 99**  
Beperking van de Vlans die tot een trunk behoren:  
Switch(config)# **interface fa** 0/4  
Switch(config-if)# **switchport trunk allowed vlan** 10,20  
Switch(config-if)# **switchport trunk allowed vlan add** 99  
  
Dynamic Trunk protocol  
  
4 modi: access, trunk, dynamic desirable en dynamic auto  
  
Vastzetten op ‘access’:  
Switch(config-if)# **switchport mode access**  
  
Vastzetten op ‘trunk’:  
Switch(config-if)# **switchport mode trunk**  
  
‘Dynamic auto’ wordt ‘Trunk’ wanneer andere zijde ‘trunk ‘ of ‘dynamix desirable’ is  
Switch(config-if)# **switchport mode dynamic auto**  
  
‘Dynamic desirable’ wordt altijd ‘trunk’ tenzij de andere kant ‘access’ is:  
Switch(config-if)# **switchport mode dynamic desirable**  
  
Troubleshooten van VLAN en TRUNK  
  
commando’s:  
Switch# **show vlan**  
Switch# **show mac-address table**  
Switch# **show interfaces switchport**  
Switch# **show interfaces trunk**  
  
Router  
  
Router – Basic settings  
  
router# **conf t**  
router(config)# **hostname** R1  
  
hostname weghalen  
R1# **no hostname**  
R1(config)# **banner login “**Router van het departement**”**  
R1(config)# **banner motd “**Verboden toegang onbevoegd personeel!**”**  
(R1(config)# enable password pxl )

R1(config)# **enable secret** pxl  
R1(config)# **line console 0**  
R1(config-line)# **password pxl**R1(config-line)# **login**  
R1(config-line)# **logging synchronous**  
  
R1(config)# **line vty 0 15**  
R1(config-line)# **password** pxl  
R1(config-line)# **login**  
R1(config-line)# **logging synchronous**  
R1(config-line)# exit  
R1(config)# **service password-encryption**  
  
Ethernet Interfaces instellen  
  
R1# **conf t**  
R1(config)# **interface FastEthernet** 0/1   
R1(config-if)# **ip address** 192.168.1.3 255.255.255.0  
R1(config-if)# **no shutdown**  
R1(config-if)# **description** connectie met het administratie netwerk  
  
Seriele Interfaces instellen  
  
R1# **conf t**  
R1(config)# **interface serial** 0/0/0  
R1(config-if)# **ip address** 200.200.1.3 255.255.255.0  
R1(config-if)# **clock rate** 1000000  
R1(config-if)# **no shutdown**  
R1(config-if) **description** connectie met ISP router  
  
Clock rate: Seriele kabels zijn voorzien van een DCE en DTE kant. Aan de zijde van de DCE kant moet je de klok instellen!!   
Deze wordt dan overgenomen door de DTE kant.  
Dit staat aangeduid op de kabel maar kan ook in IOS gezien worden:  
R1# **show controllers Serial** 0/0/0  
interface serial0/0/0  
Hardware is PowerQUICC MPC860  
**DCE** V.35 **clockrate 1000000**  
  
Loopback Interface instellen:

Elke router heeft een vast router ID nodig (virtuele interface)  
Deze staat altijd ‘up’.  
  
R1(config)# **interface loopback 0**R1(config-if)# **ip address** 172.0.0.1 255.255.255.255  
  
R2(config)# interface loopback 0   
R2(config-if)# ip address 172.0.0.2 255.255.255.255  
  
InterVLAN Routing  
  
ROUTER-ON-A-STICK  
  
Toekennen van bv 3 VLAN’s aan 1 routerpoort:  
  
R1# **conf t**  
R1(config)# **interface** g0/0.10  
R1(cofnig-if)# **encapsulation dot1q 10**  
R1(cong-if)# **ip address** 192.168.10.1 255.255.255.0  
  
R1(config)# **interface** g0/0.20  
R1(cofnig-if)# **encapsulation dot1q 20 (if natvie vlan put ‘native’ after vlan number)**  
R1(cong-if)# ip address 192.168.20.1 255.255.255.0  
  
R1(config)# interface g0/0.99  
R1(cofnig-if)# encapsulation dot1q 99  
R1(cong-if)# ip address 192.168.99.1 255.255.255.0  
  
R1(config-if)# **interface** g0/0  
R1(config-if)# **no shutdown**  
R1(config-if)# exit

Router Catalyst 2960  
  
Deze kan beperkt als L3 Switch functioneren.  
  
Tonen default template van Cisco switch Database Manager  
switch# **show sdm prefer**  
  
Tonen mogelijke templates Cisco switch Database Manager  
switch# **show sdm ?**  
  
Wijzigen template  
switch(config)# **sdm prefer lanbase-routing**  
  
Toekennen van meerdere SVI’s aan de switch en Ipv4 routing aanzetten  
switch(config)# **interface** g0/0  
switch(config-if)# **switchport mode access**  
switch(config-if)# **switchport access VLAN 10**  
switch(config-if)# exit  
switch(config)# **interface vlan** 10  
switch(config-if)# **ip address** 192.168.10.1 255.255.255.0  
switch(config)# **interface vlan** 20   
switch(config-if)# **ip address** 192.168.20.1 255.255.255.0  
switch(config-if)# **no shutdown**  
switch(config)# **ip routing**  
  
Statische routes toevoegen  
  
**Hierbij moet men kijken welke routes al gekend zijn omdat het buren zijn en dan telkens de andere gaan bij aanvullen per router.**  
  
switch(config)# **ip route** 192.10.0 255.255.255.0 **g**0/1  
switch(config)# **ip route** **0.0.0.0 0.0.0.0** 192.168.1.1

Static Routing  
  
R1# **show ip route** route tabel opvragen  
  
R1# **debug ip routing** systeemmeldingen tijdens aanmaken/verwijderen routes  
  
R1# **no debug ip routing** enkel debugging op routing afzetten  
R1# **no debug all** alle debugging afzetten  
  
met next hop:  
R1(config)# **ip route** 10.10.10.0 255.255.255.0 192.168.0.1 toevoegen  
R1(config)# **no ip route** 10.10.10.0 255.255.255.0 192.168.0.1 verwijderen

Met next administrative distance = **ip route (ip) (subnet) (output interface or ip) (admin distance)**

**ipv6 route ::/0 2001:DB8:A:2::1 = ipv6**  
  
met exit interface:  
R1(config)# **ip route** 10.10.10.0 255.255.255.0 serial 0/0 toevoegen  
R1(config)# **no ip route** 10.10.10.0 255.255.255.0 serial 0/0 verwijderen  
  
toevoegen default gateway (QUAD ZERO ROUTE):  
R1(cofnig)# **ip route 0.0.0.0 0.0.0.0** 192.168.0.1 (or interface number)

**troubleshooting:**

checken connected routes: **show ip route connected**

checken van static routes: **show ip route static**

ip van een interface bekijken: **show ip interface brief**  
  
testen van routes door tracert commando in cmd!!  
  
Dynamic Routing  
  
RIPv1  
---🡪 classful routing protocol dus **zonder subnet masks**

**Hierbij moet men in tegenstelling tot statisch de lokaal verbonden netwerken opgesomd per router!!**

R1(config)# **router rip** aanzetten RIP  
  
Rip staat standaard op versie 1 maar kan ook gereset worden van é naar 1:  
R1(config-router)# **no version** zet terug op standaard (1)  
R1(config-router)# **version 1** zet op versie 1  
  
Na het aanzetten van RIP de netwerken meegeven die met RIP gestuurd moeten worden:  
R1(config-router)# **network** 192.168.1.0  
R1(config-router)# **network** 192.168.2.0

(alle verbonden netwerken moeten worden toegevoegd aan rip niet enkel router naar router, de passive interfaces zijn wel de netwerken die niet naar een router gaan  
  
**Troubleshooting!!**  
R1# **show ip protocols**  
R1# **show ip rip database**  
R1# **debug ip rip** debug tijdens rip config  
  
Interfaces opgeven die niet meedoen aan RIP (netwerken waar geen routers meeluisteren):  
R1(config)# **router rip**  
R1(config-router)# **passive-interface Fastethernet** 0/0  
  
QUAD ZERO ROUTE op de ROUTER DIE MET DE BUITENWERELD IS VERBONDEN!!  
R1(config)# **ip route 0.0.0.0 0.0.0.0 Serial** 0/0  
R1(config)# **router rip**  
R1(config-router)# **default-information originate**  
  
Routes die geleerd zijn door RIP van andere routers staan aangeduid met een ‘**R**’ en hebben een **administratieve kost van 120**.  
  
Voor troubleshooten:  
Bij fouten zoeken moet het eerst de routetabellen bekeken worden.  
Wordt daar niks gevonden dan kan men het Rip protocol en de Rip database bekijken  
Ook de debugging aanzetten in Rip levert veel op.  
  
Ripv2 (paar standaard dingen overnemen van V1)  
-----> classless protocol dus **met subnet masks**  
R1(config)# **router rip**  
R1(config-router)# **version 2**R1(config-router)# **no auto-summary**  
  
Automatisch laten wissen van de statische routes die al aanwezig zijn op de router:  
R1(config-router)# **redistribuate static**  
Altijd nakijken in ‘show running config’ dat de setting ‘ip classless’ staat.  
Indien niet dan :  
R1(config)# **ip classless**  
  
!! Routing summary nemen van de netwerken en **die in RIPv2 zetten zonder subnetmask** !!  
bv  
R1(config-router)# **network** 192.168.1.0  
  
QUAD ZERO ROUTE op de ROUTER DIE MET DE BUITENWERELD IS VERBONDEN!!  
R1(config)# **ip route 0.0.0.0 0.0.0.0 Serial** 0/0  
R1(config)# **router rip**  
R1(config)# **default-information originate**

Single-Area OSPF  
  
Open Shortest Path First (OSPF)  
  
Bij het aanzetten van OSPF moet een id gekozen worden tussen 1 en 65536.   
Dit mag voor alle routers hetzelfde zijn maar hoeft niet.  
  
R1(config)# **router ospf 1**

Router id meegeven in de vorm van een ip adres.  
dit moet uniek zijn.  
  
R1(config-router)# **router-id 172.0.0.1**

R2(config-router)# **router-id 172.0.0.2**  
  
Indien er problemen zijn met veranderde router-id’s kan je het ospf process resetten met:  
R1# **clear ip ospf process**  
  
Toevoegen van netwerken:  
syntax : network network-address widcard-mask area area-id  
R1(config)# **router ospf** 10  
R1(config-router)# **network** 192.168.1.0 0.0.0.255 **area 0**  
R1(config-router)# **network** 192.168.2.0 0.0.0.255 **area 0**  
  
!! wildcard mask is omgekeerde van subnetmask: dus **255.255.255.0 wordt 0.0.0.255** !!  
!! area id moet gelijk zijn voor alle routers die met ospf moeten communiceren !!  
  
Passieve interfaces uitsluiten die niet meedoen aan OSPF:  
R1(config)# **router ospf** 10  
R1(config-router)# **passive-interface GigabitEthernet 0/0**  
**Altijd op het einde QUAD ZERO ROUTE op de ROUTER DIE MET DE BUITENWERELD IS VERBONDEN!!**R1(config)# **ip route 0.0.0.0 0.0.0.0 Serial** 0/0  
R1(config)# **router ospf** 10  
R1(config)# **default-information originate**  
  
De bandbreedte kan per interface ingesteld worden om een verschil te maken tss snelle en trage routes:  
R1(config)# **interface** serial 0/0  
R1(config-if)# **bandwith** 64  
  
**!! OSPF werkt met kost !!**  
!! Kost wordt berekend op basis van bandbreedte !!  
!! de kost van 10Mbit is 10 en van 100Mbit bandbreedte is altijd = 1 !!  
!! snellere lijne dan 100Mbit hebben ook altijd kost = 1 !!  
!! Hoe lager de bandbreedte hoe groter de kost !!  
  
Men kan ook rechtstreeks de kost ingeven ipv de bandbreedte:  
R1(config)# **interface serial** 0/0  
R1(config-if)# **no bandwidth** 64  
R1(config-if)# **ip ospf cost** 1562  
  
Bv  
R1(config)# **interface serial** 0/0  
R1(config-if)# **clock rate 1000000**  
R1(config-if)# **bandwidth 1000**  
R1(config-if)# exit  
R1(config)# interface Serial 0/1  
R1(config-if)# bandwidth 1000  
R1(config-if)# exit  
R2(config)# interface serial 0/0  
R2(config-if)# clock rate **64000**R2(config-if)# bandwidth **64**  
R2(config-if)# exit  
R2(config)# interface serial 0/1  
R2(config-if)# bandwidth 1000  
R2(config-if)# exit  
  
  
Extra:  
Kostberekeing aanpassen kan door het basisgetal dat gedeeld wordt door de bandbreedte aan te passen. Dit is standaard 10\_8.  
R1(config-router)# **auto-cost reference-bandwidth** 10000  
dit zal het getal verzetten naar 10\_10.  
Wil je het terug resetten naar 10\_8 dan moet volgend commando:  
R1(config-router)# **auto-cost reference-bandwidth** 100  
  
Andere OSPF commando’s:  
R1# **show ip ospf neighbor**  
R1# **show ip protocols**  
R1# **show ip ospf**  
R1# **show ip ospf interface brief**  
  
Access Control Lists (ACL)  
  
Standard ACLs  
  
ACL altijd zo dicht mogelijk bij de bestemming!! Dichtste router bij de bestemming, dichtste interface bij de bestemming  
  
syntax : router(config)# access-list access-list-number {permit|deny|remark} source [source wildcard] [log]  
  
Standaard ACLs gaan altijd van **1 tot 99** of van **1300 tot 1999**.  
  
R1(config)# **access-list** 10 **permit** 192.168.30.0 0.0.0.255 alles van dat netwerk doorlaten  
R1(config)# access-list 10 permit 192.168.30.1 0.0.0.0 alles van die host doorlaten  
R1(config)# access-list 10 permit host 192.168.30.1 zelfde als vorige mr geen wildcard  
  
R1(config)# **access-list deny any**  alles stoppen  
R1(config)# **access-list permit any** alles doorlaten  
  
**!! de lijst wordt altijd SEQUENTIEEL afgaan van boven naar onder. Onderaan staat altijd ‘deny any’ !! !! volgorde is HEEL belangrijk !!  
  
ACL ALTIJD KOPPELEN aan een INTERFACE:**R1(config)# interface serial 0/0/0  
R1(config-if)# ip **access-group** 3 **out**  
**ALTIJD MEEGEVEN OF HET INKOMENDE OF UITGAANDE TRAFIEK IS**  
  
Ipv nummers kan met ook met namen werken:  
R1(config)# **ip access-list standard** NO\_ACCESS  
R1(config-std-nacl)# **deny host** 192.168.10.10  
R1(config-std-nacl)# **permit any**  
R1(config-std-nacl)# exit  
R1(config)# interface g0/0  
R1(config-if)# **ip access-group** NO\_ACCESS **out**  
  
Nuttige commando’s:  
R1# **show access-lists**  
R1# **clear access-lists counters**  
  
Een Standaard ACL is ZEER GESCHIKT voor VTY lijnen te beveiligen:  
R1(config)# line vty 0 4  
R1(config-line)# login local  
R1(config-line)# transport input ssh  
R1(config-line)# access-class 21 in  
R1(config-line)# exit  
R1(config)# access-list 21 permit 192.168.10.0 0.0.0.255  
R1(config)# access list 21 deny any  
  
Extended ACL (niet gevraagd op examen)  
  
Nummers zijn **100 tot 199** of **2000 tot 2699**.  
Extended ACL ALTIJD ZO DICHT MOGELIJK TEGEN DE BRON!!  
Rest zie samenvatting.  
  
DHCP  
  
4 Stappen

---------------------

1. Broadcast client

2. “Ik ben een DHCP server, hier hebt ge u lease”

3. Client: “Ik wil de lease van de bepaalde DHCP-server (want er zijn meerdere DHCP servers)”

4. “Accepted”

Default Gateway, statische IP address en Broadcast en Netwerk add mogen niet in de DHCP Pool dus "excluden"

R(config)# **ip dhcp pool** Bram

# **network** 192.168.0.0 255.255.255.0

# **default-router** 192.168.0.1

# **dns** 8.8.8.8

# exit

--> terug naar global conf

# **ip dhcp excluded-address** 192.168.0.1

# ip dhcp excluded-address 192.168.0.1 192.168.0.10 --> Een range excluden

De broadcasten blijven binnen één router. Indien er nog een router is achter de eerste, raakt de broadcast er niet.

Daarom moeten we relay toepassen.

Relay

**interface** fa0/0.10

# **ip helper-add** 172.16.0.1 => IP van poort

Als je router thuis een dynamtic adrress moet krijgen van Telenet of Belgacom (uit de DHCP pool van belgacom of telenet)

s0/0/0

# ip add dhcp

Network Address Translation (NAT)  
  
Public

--------------

A. 10.\*.\*.\*

B. 172.16.\*.\*

172.31.\*.\*

C. 192.168.\*.\*

NAT

=> Source IP(192.168.1.3) wordt aangepast naar Publiek adres (150.150.150.2)

We moeten ook poorten gaan gebruiken om ervoor te zorgen dat meerdere devices op het internet kunnen via publiek adress.

192.168.1.3:1080

----------------------------------------------------------------------------

inside local inside global outside global (vb. website)

192.168.1.3:1080 150.150.150.2:1080 100.100.100.254:80

2 soorten:

-Static

Servers

-Dynamic

Pool creeren met public ip addressen

Overloaded NAT --> PAT (portbased address translation) (vooral bij dynamic)

PAT: meerdere verbndingen op één poort

50.50.50.50:80 -> ip + port = socket

Port tussen:

>1024 - 65k

Door meerdere poorten kunnen ook +- 64k gebruikers van internet worden voorzien.

---------------------------------------------------

Commando's

Met POOL

#**POOL\_1** 150.150.150.3 150.150.150.10

#**access-list 1 permit** 192.168.1.0 0.0.0.255

#**ip nat inside source list** 1 **pool** POOL\_1

Zonder POOL

#**ip nat inside source list** 1 **interface** s0/0/0 **overload**

#**access-list** 1 **permit** 192.168.1.0 0.0.0.255

------------

#**access-list 1 permit** 192.168.1.0 0.0.0.255

#**access-list 1 permit** 192.168.2.0 0.0.0.255

#**ip nat inside source list** 1 **interface** s0/0/0

#**int ser** 0/0/0 buiten poort naar ISP

#**ip nat outside**

#**int g**0/0.10

#**ip nat inside** binnenpoort vlan 10

#**int g**0/0.20 binnenpoort vlan 20

#**ip nat inside**

#exit

Overzicht:

#**ip nat translation**