



Networks advanced



Switching, Routing, Wireless
and Enterprise Networking

Auteur:

Johan Cleuren

Lectoren:

Johan Cleuren



WOORD VOORAF

Leermaterialen

Cursus

- Online Cisco curriculum op cisco.netacad.com

Website

- <http://blackboard.pxl.be>, Blackboard cursus met aanvullingen, de getoonde presentaties en animaties, opgaven en oplossingen van bepaalde oefeningen.
- <http://pluralsight.com>, online video tutorials.

Achtergrondinformatie

Handboek

- Switching, Routing, and Wireless Essentials v7 Companion Guide (ISBN 978-0-13-663438-6).
- Enterprise Networking, Security, and Automation Companion Guide (CCNAv7) (ISBN-10: 0-13-663432-X, ISBN-13: 978-0-13-663432-4)

Inhoud

WOORD VOORAF	1
HOOFDSTUK 0: HERHALING NETWORKS ESSENTIALS	1
❖ INITIAL CONFIGURATION IN IOS	1
❖ IOS HELP	3
HOOFDSTUK 1: BASIC DEVICE CONFIGURATION.....	7
1.1. CONFIGURE A SWITCH WITH INITIAL SETTINGS.....	7
❖ RECOVERING FROM A SYSTEM CRASH.....	7
❖ INSTELLEN VAN SVI	8
1.2. CONFIGURE SWITCHING PORTS	8
❖ INSTELLEN VAN SNELHEID EN VERBINDING VAN DE POORT	8
❖ VERIFICATIE VAN DE CONFIGURATIE.....	9
1.3. SECURE REMOTE ACCESS	9
❖ BASISBEVEILIGING VAN DE TOEGANG (HERHALING CCNA1).....	9
❖ BEVEILIGDE TOEGANG VIA SSH	10
1.4. BASIC ROUTER CONFIGURATION	10
❖ BASIS ROUTER SETTINGS	10
❖ CONFIGURE ROUTER INTERFACES	12
❖ INSTELLING VAN LOOPBACK INTERFACE	13
1.5. VERIFY DIRECTLY CONNECTED NETWORKS	13
❖ ROUTE OPVRAGEN.....	13
❖ FILTEREN VAN SHOW COMMANDO.....	13
HOOFDSTUK 2: SWITCHING CONCEPTS.....	15
HOOFDSTUK 3: VLANS.....	16
3.1. OVERVIEW VLAN	16
3.2. VLAN'S IN A MULTI-SWITCHED ENVIRONMENT.....	16
3.3. VLAN CONFIGURATION	16
❖ AANMAKEN EN CONFIGURATIE VAN EEN VLAN	16
❖ POORTEN TOEKENNEN AAN EEN VLAN.....	17
❖ VERIFICATIE VAN INSTALLATIE	17
3.4. VLAN TRUNKS	18
3.5. DTP: DYNAMIC TRUNKING PROTOCOL	19
HOOFDSTUK 4: INTER-VLAN ROUTING.....	20
4.1. INTER-VLAN ROUTING OPERATION	20
4.2. ROUTER-ON-A-STICK INTER-VLAN ROUTING	20
❖ ROUTER-ON-A-STICK.....	20
❖ CASE STUDY: ROUTER-ON-A-STICK	20
4.3. INTER-VLAN ROUTING USING LAYER 3 SWITCHES	22
4.4. TROUBLESHOOT INTER-VLAN ROUTING.....	22
❖ TROUBLESHOOTING VLAN'S EN TRUNKS.....	22
HOOFDSTUK 5: STP CONCEPTS	24
5.1. PURPOSE OF SPANNING TREE CONCEPTS	24
5.2. STP OPERATIONS	24
5.3. EVOLUTION OF STP	24
❖ PVST+	24

❖ RAPID PVST+	24
5.4. SPANNING TREE CONFIGURATION.....	24
❖ PVST+ CONFIGURATION	24
❖ RAPID PVST+ CONFIGURATION	25
HOOFDSTUK 6: ETHERCHANNEL	26
6.1. ETHERCHANNEL OPERATION	26
6.2. CONFIGURE ETHERCHANNEL	26
❖ CONFIGURING ETHERCHANNEL	26
❖ TROUBLESHOOTING ETHERCHANNEL.....	26
HOOFDSTUK 7: DHCPV4	27
7.1. DYNAMIC HOST CONFIGURATION PROTOCOL VERSIE 4.....	27
7.2. CONFIGURE A CISCO IOS DHCPV4 SERVER	27
❖ DHCP RELAY.....	27
7.3. CONFIGURE A DHCPV4 CLIENT	28
HOOFDSTUK 8: SLAAC AND DHCPV6	29
8.1. IPV6 GUA ASSIGNMENT	29
8.2. STATELESS ADDRESS AUTOCONFIGURATION (SLAAC).....	29
8.3. DHCPV6	29
8.4. CONFIGURE DHCPV6 SERVER.....	29
❖ CONFIGURATIE VAN STATELESS DHCPV6.....	29
❖ CONFIGURATIE VAN STATELESS DHCPV6-CLIENT	29
❖ CONFIGURATIE VAN STATEFUL DHCPV6.....	29
❖ CONFIGURATIE VAN STATEFUL DHCPV6-CLIENT	29
❖ TROUBLESHOOT VAN DHCPV6.....	30
❖ DHCPV6 RELAY.....	30
HOOFDSTUK 9: FHRP CONCEPTS.....	31
9.1. FIRST HOP REDUNDANCY PROTOCOLS	31
9.2. HSRP.....	31
❖ HSRP CONFIGURATION	31
❖ HSRP TROUBLESHOOTING	31
HOOFDSTUK 10: LAN SECURITY CONCEPTS	32
10.1. ENDPOINT SECURITY	32
10.2. ACCESS CONTROL.....	32
10.3. LAYER 2 SECURITY THREATS	32
10.4. MAC ADDRESS TABLE ATTACK	32
10.5. LAN ATTACKS	32
HOOFDSTUK 11: SWITCH SECURITY CONFIGURATION.....	33
11.1. IMPLEMENT PORT SECURITY	33
❖ ONGEBRUIKTE POORTEN UITZETTEN	33
❖ SWITCH PORT SECURITY	33
11.2. MITIGATE VLAN ATTACKS	33
❖ VLAN HOPPING ATTACK.....	33
11.3. MITIGATE DHCP ATTACKS.....	34
❖ DHCP SNOOPING	34
11.4. MITIGATE ARP ATTACKS	34
❖ CONFIGURATIE VAN DAI (DYNAMIC ARP INSPECTION).....	34

11.5. MITIGATE STP ATTACKS	35
❖ PORTFAST AND BPDU GUARD	35
HOOFDSTUK 12: WLAN CONCEPTS	36
HOOFDSTUK 13: WLAN CONFIGURATION	37
HOOFDSTUK 14: ROUTING CONCEPTS	38
14.1. PATH DETERMINATIONS	38
14.2. PACKET FORWARDING	38
14.3. BASIC ROUTER CONFIGURATION REVIEW	38
14.4. IP ROUTING TABLE	39
❖ ROUTETABELLEN	39
❖ OPVRAGEN VAN STATISCHE STANDAARDROUTE	39
HOOFDSTUK 15: IP STATIC ROUTING	40
15.1. STATIC ROUTES	40
❖ OPVRAGEN VAN DE ROUTETABEL	40
15.2. CONFIGURE IP STATIC ROUTES	40
❖ STATISCHE ROUTES IN IPv4	40
❖ STATISCHE ROUTES MET IPv6	42
15.3. CONFIGURE FLOATING STATIC ROUTES	43
❖ TROUBLESHOOTING VAN IPv4 DEFAULT ROUTES	44
❖ CASE STUDY: STATISCHE ROUTES	45
HOOFDSTUK 16: TROUBLESHOOT STATIC AND DEFAULT ROUTES	48
HOOFDSTUK 17: DYNAMIC ROUTING - RIP	49
17.1. RIP v1: ROUTING INFORMATION PROTOCOL VERSIE 1	49
❖ CASE STUDY: RIP VERSIE 1	50
17.2. RIP v2: ROUTING INFORMATION PROTOCOL VERSIE 2	52
❖ CASE STUDY: RIPv2	53
HOOFDSTUK 18: DYNAMIC ROUTING - OSPF	56
18.1. ROUTER-ID	56
❖ CONFIGURE ROUTER-ID	56
18.2. POINT-TO-POINT OSPF NETWORKS	57
❖ NETWORK COMMAND AND WILDCARD MASK	57
❖ ALTERNATIVE: NETWORK COMMAND AND QUAD-ZERO WILDCARD MASK	57
❖ ALTERNATIVE: IP OSPF COMMAND	57
❖ PASSIVE INTERFACE	57
❖ POINT-TO-POINT NETWORKS	57
18.3. MULTI-ACCESS OSPF NETWORKS	58
❖ OSPF IN MULTIACCESS NETWORKS	58
18.4. MODIFY SINGLE-AREA OSPFv2	58
❖ REFERENCE BANDWIDTH	58
❖ MANUALLY SET OSPF COST	59
❖ HELLO PACKETS INTERVAL	59
18.5. DEFAULT ROUTE PROPAGATION	59
18.6. VERIFYING OSPF	59
❖ CASE STUDY 1: OSPFv2	60
❖ CASE STUDY 2: TUNING OSPFv2	62
18.7. EXTRA: SINGLE-AREA OSPFv3	64
❖ CONFIGURING OSPFv3	64
❖ VERIFYING OSPFv3	64

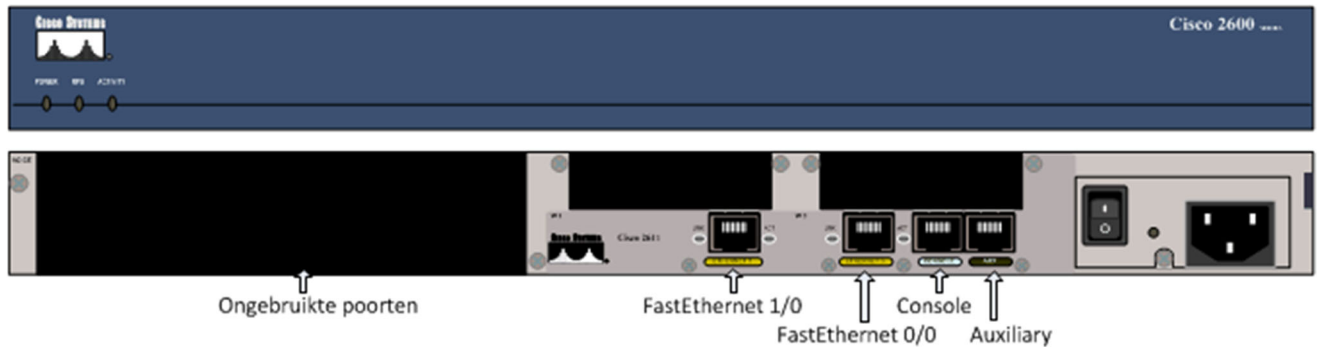
❖ CASE STUDY: OSPFv3	65
HOOFDSTUK 19: ACLS FOR IPV4 CONFIGURATION	68
19.1. CREATE AN ACL.....	68
❖ NUMBERED STANDARD IPV4 ACL.....	68
❖ NAMED STANDARD IPV4 ACL.....	68
❖ APPLY A STANDARD IPV4 ACL.....	69
19.2. MODIFY IPV4 ACLS.....	69
19.3. SECURE VTY-PORTS WITH A STANDARD IPV4 ACL.....	70
19.4. EXTENDED IPV4 ACLS.....	71
❖ NUMBERED EXTENDED ACL	71
❖ NAMED EXTENDED ACL.....	71
❖ VERIFY EXTENDED ACL.....	72
HOOFDSTUK 20: NETWORK ADDRESS TRANSLATION IPV4	73
20.1. NAT CHARACTERISTICS	73
20.2. TYPES OF NAT.....	73
20.3. NAT ADVANTAGES AND DISADVANTAGES	73
20.4. STATIC NAT FOR IPV4	73
❖ CONFIGURING STATIC TRANSLATION OF INSIDE SOURCE ADDRESSES	73
20.5. DYNAMIC NAT.....	74
❖ CONFIGURING DYNAMIC TRANSLATION OF INSIDE SOURCE ADDRESSES.....	74
20.6. PAT.....	74
❖ USING NAT TO ALLOW INTERNAL USERS ACCESS TO THE INTERNET OVER ONE GLOBAL ADDRESS (=PAT).....	74
20.7. PORT FORWARDING USING IOS.....	75

Hoofdstuk 0: Herhaling Networks Essentials

❖ Initial configuration in IOS

De CLI (Command Line Interface) van Cisco-apparatuur kan benaderd worden op drie manieren:

- Console-ingang met een consolekabel
- Telnet of SSH-sessie met UTP-kabel via één van de fastethernetpoorten
- Over HTTP via één van de fastethernetpoorten
- AUX-poort



Figuur 1: De aansluitpoorten van de Cisco 2611XM

▪ Consoletoegang

De consoletoegang wordt ook de CTY-lijn (*Console TeleType*) genoemd. Traditioneel werd HyperTerminal als terminalsoftware meegeleverd met Windows. Sinds Windows Vista is dit niet langer het geval. Je dient andere software te installeren, bijvoorbeeld PuTTY.

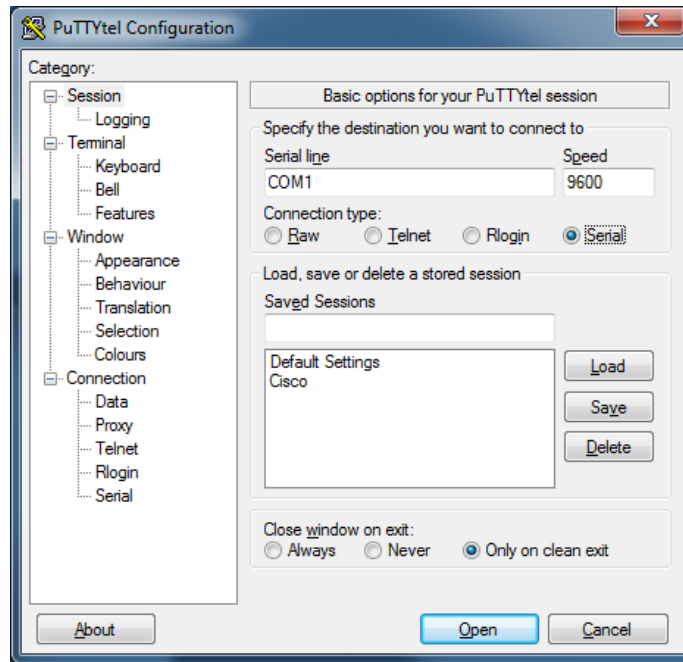
De standaardinstellingen zijn:

- Bitrate: 9600 bits per seconde
- 8 databits
- Geen pariteit
- 1 stopbit
- Geen datatransportbesturing

Om een connectie op te bouwen is het voldoende om een verbinding te maken tussen de seriële poort van de computer en de consolepoort van de router. Hiervoor gebruik je een consolekabel. Daarna kan je PuTTY opstarten.

De consoletoegang is onmisbaar voor de volgende situaties:

- De initiële configuratie van de netwerkapparatuur;
- Paswoordherstel;
- Als het niet mogelijk is om over het netwerk connectie te maken.



Figuur 0-2: PuTTY

▪ Telnet-toegang

Vanaf het moment dat het netwerkapparaat voorzien is van een actieve IP-service kan ook connectie gemaakt worden met een UTP-kabel en dus ook over het netwerk. Voor deze toegang is het dus niet langer noodzakelijk om fysiek in de buurt van de apparatuur te zitten.

Een telnetsessie kan geopend worden met het `telnet`-commando, maar ook met andere software zoals PuTTY. Hiervoor moet de basisbeveiliging van de netwerkapparatuur wel in orde zijn (paswoord op enable en vty-lijnen).

▪ AUX-toegang

De AUX-toegang maakt gebruik van een telefoonconnectie. Hiervoor moet een modem verbonden worden met de AUX-poort (Auxiliary) van de netwerkapparatuur. Deze toegang kan zowel lokaal als vanop afstand (remote) gebruikt worden.

▪ http-toegang

Sommige netwerkapparatuur is voorzien over grafische user interface (GUI) die web based is en dus met een webbrowser over http kan benaderd worden. De toegang over http is niet standaardmatig mogelijk. Met de volgende commando's kan je de http-toegang aanzetten.

```
Router(config)# ip http authentication enable
Router(config)# ip http server
```

Binnen IOS zijn vier verschillende modes voorzien:

- User executive mode
 - Laat enkel toe de basisinstellingen te bekijken (*view-only mode*). Komt overeen met een gastaccount.
- Privileged executive mode
 - Laat toe alles te bekijken en te wijzigen en komt dus overeen met een beheerdersaccount.
- Global configuration mode
 - Algemene instellingen van het gehele netwerkapparaat.

- Specific configuration mode
 - Specifieke instellingen voor een bepaald onderdeel van het netwerkapparaat.

De User executive mode wordt gekenmerkt door de 'groter dan' cursor, de privileged mode door het hekje. Met het `enable` en `disable` commando kan je van User naar Privileged mode gaan en omgekeerd.

```
Router>enable
Router#disable
Router>
```

Vanuit de privileged mode geeft het commando `configure terminal` je toegang tot de globale configuratie. Met `exit` of `Ctrl-Z` kan je een mode terug gaan.

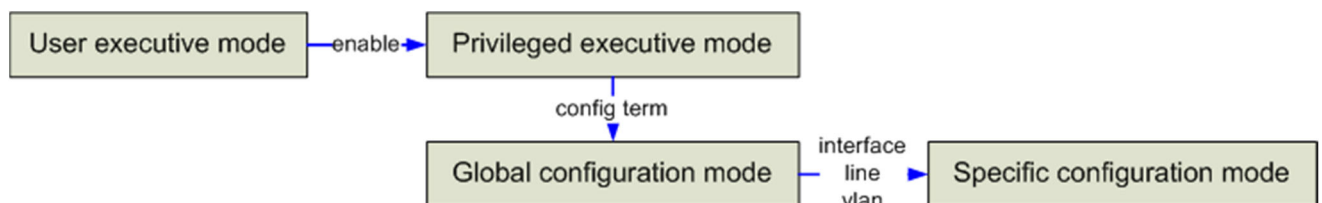
```
Router#configure terminal
Router(config)#exit
Router#
```

Vanuit globale configuratiemodus kan je naar de specifieke configuratie, bijvoorbeeld die van een interface, een lijninterface, een VLAN, enzovoort.

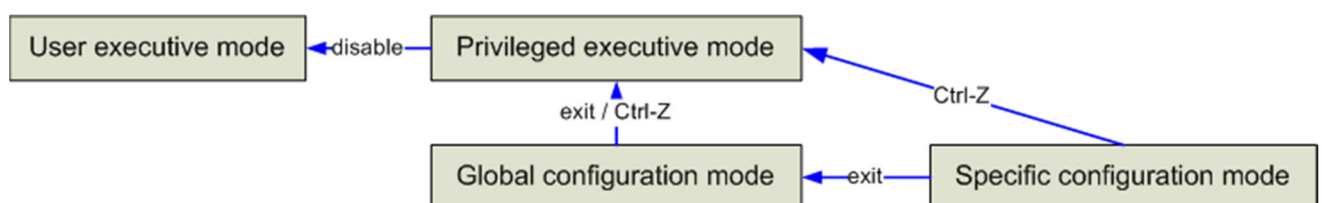
```
Router(config)#interface fa 0/1
Router(config-if)#
```

Vanuit hogere configuratiemodi kan je ook in één stap terugkeren met `end`.

```
Router(config-if)#end
Router#
```



Figuur 2: IOS-structuur van boven naar beneden



Figuur 3: IOS-structuur van beneden naar boven

❖ IOS help

Er zijn drie vormen hulp mogelijk:

- Contextgevoelig
- Syntaxcontrole
- Sneltoetsen

▪ Contextgevoelige hulp

Met het vraagteken kan een lijst bekomen worden met alle mogelijke commando's binnen de huidige modus.

In User Exec-mode geeft dit de mogelijke commando's op dat niveau.

```
Switch>?
Exec commands:
  access-enable  Create a temporary Access-List entry
  clear          Reset functions
  connect        Open a terminal connection
  disable        Turn off privileged commands
  disconnect     Disconnect an existing network connection
  enable         Turn on privileged commands
  exit           Exit from the EXEC
  help           Description of the interactive help system
  lock           Lock the terminal
  login          Log in as a particular user
  logout         Exit from the EXEC
...
```

In Privileged Exec-mode zijn andere commando's beschikbaar.

```
Switch#?
Exec commands:
  access-enable  Create a temporary Access-List entry
  access-template Create a temporary Access-List entry
  archive        manage archive files
  cd             Change current directory
  clear          Reset functions
  clock          Manage the system clock
  cluster        cluster exec mode commands
  configure      Enter configuration mode
  connect        Open a terminal connection
  copy           Copy from one file to another
  debug          Debugging functions (see also 'undebug')
  delete         Delete a file
  dir            List files on a filesystem
  disable        Turn off privileged commands
...
```

In de configuratiemodes levert het vraagteken weer een andere lijst van beschikbare commando's op.

Het vraagteken kan ook gebruikt worden om de mogelijke parameters van een commando's te bekomen.

```
Switch#ping ?
WORD Ping destination address or hostname
ip    IP echo
tag   Tag encapsulated IP echo
<cr>
```

▪ Syntaxcontrole

De commando's binnen IOS mogen afgekort worden. De commando's worden van links naar rechts gelezen. Als deze letters het begin zijn van één enkel commando dan wordt dit uitgevoerd. In het andere geval zijn er meerdere letters nodig.

```
Switch#c?
cd      clear clock cluster configure
connect copy

Switch#cl?
clear clock cluster

Switch#clo?
clock
```

In het geval dat `clock` wordt ingegeven, is dat voor de netwerkkapparatuur dus eenduidig het clock-commando en wordt dit uitgevoerd.

```
Switch#clock set 05:06:07 8 SEP 2010
```

Deze afkortingsmogelijkheid vermindert het typewerk soms aanzienlijk.

```
Switch#conf term
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

Indien commando's fout of onvolledig worden ingegeven wordt de positie van de fout aangegeven door het ^-teken. Het ?-teken kan dat gebruikt worden om contextgevoelige hints te tonen.

```
Switch#clock set 05:06:07 8 9 10
```

```
% Invalid input detected at '^' marker.
```

```
Switch#clock set 05:06:07 8 ?  
MONTH Month of the year
```

▪ Sneltoetsen

Tab	Vervolledigt een gedeeltelijk ingegeven commando
Delete	Verwijdert karakter rechts van de cursor
Backspace	Verwijdert karakter links van de cursor
Up Arrow	Geeft vorig commando bij het scrollen door de commando's
Down Arrow	Geeft volgend commando bij het scrollen door de commando's
Ctrl+P	Idem aan up arrow
Ctrl+N	Idem aan down arrow
Ctrl+A	Cursor naar het begin van de lijn
Ctrl+E	Cursor naar het eind van de lijn
Ctrl+F	Een karakter naar voor
Ctrl+B	Een karakter naar achter
Esc+F	Een woord naar voor
Esc+B	Een woord naar achter
Ctrl+R	Herhaalt vorig commando
Ctrl+U	Wist een lijn
Ctrl+W	Wist een woord
Ctrl+Z	Een niveau terug

▪ Informatie opvragen binnen IOS

Op de verschillende niveau kan telkens informatie opgevraagd worden over de instellingen die daar gebeurd zijn. Hiervoor is wel wat inzicht in de geheugenstructuur van Cisco-apparatuur nodig.

Op elk niveau kan het show-commando gebruikt worden.

RAM (IOS)			NVRAM	FLASH	
Programma's	Huidige configuratie bestand	Tabellen en buffers	Reserve configuratie bestand	Besturings systeem	Interfaces
processes protocols	running-config	memory stacks buffers	startup-config	flash	interface
version					

In het IOS-deel kan je de IOS-versie opvragen.

```
router#show version
```

In het interface-deel kan je bijvoorbeeld een overzicht van de interfaces opvragen.

```
router#show interfaces serial 0/1
router#show ip interface brief
```

De huidige configuratie is opgeslagen in het RAM. Aangezien RAM vluchtig is gaat deze informatie verloren als de apparatuur uitgezet worden. Deze dient dus opgeslagen te worden in het NVRAM. Dit is geen vluchtig (Non Volatile RAM) geheugen dat gebruikt wordt tijdens het bootproces om de configuratiebestanden uit te lezen. De bestandsnamen zijn running-config en startup-config. Het kopieercommando mag natuurlijk pas gebeuren als je zeker bent dat de configuratie juist gebeurd is.

```
router#show running-config
router#copy running-config startup-config
router#show startup-config
```

Hoofdstuk 1: Basic Device Configuration

1.1. Configure a Switch with Initial Settings

❖ Recovering from a System Crash

Bepalen welke image geladen wordt bij het opstarten doe je met `boot system`.

```
Switch# configure terminal
Switch(config)# boot system flash:/c2960-lanbase-mz.122-25.FX.bin
```

Met `show boot` kan je meer info verkrijgen over de opstartprocedure.

```
Switch#show boot
BOOT path-list      :
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break        : no
Manual Boot         : no
HELPER path-list    :
Auto upgrade        : yes
NVRAM/Config file   :
buffer size:        65536
Switch#
```

Het bootproces:

```
switch: set
BOOT=flash:/c2960-lanbasek9-mz.122-55.SE7/c2960-lanbasek9-mz.122-55.SE7.bin
(output omitted)
switch: flash_init
Initializing Flash...
flashfs[0]: 2 files, 1 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 32514048
flashfs[0]: Bytes used: 11838464
flashfs[0]: Bytes available: 20675584
flashfs[0]: flashfs fsck took 10 seconds.
...done Initializing Flash.
```

Met `dir flash:` vraag je de bestandenlijst uit het flashgeheugen op.

```
switch: dir flash:
Directory of flash:/
  2  -rwx 11834846          c2960-lanbasek9-mz.150-2.SE8.bin
  3  -rwx  2072            multiple-fs
```

Configuratie van boot image

```
switch: BOOT=flash:c2960-lanbasek9-mz.150-2.SE8.bin
switch: set
BOOT=flash:c2960-lanbasek9-mz.150-2.SE8.bin
(output omitted)
switch: boot
```

❖ Instellen van SVI

Voor het management-VLAN (meestal 99) dien je een ip-adres toe te kennen aan de virtuele poort (SVI: switch virtual interface) om via telnet de configuratie te kunnen doen. Hiervoor is het nodig een interface te creëren voor dat VLAN.

```
Switch# configure terminal
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
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch#
```

De gewijzigde configuratie kan dan naar de startup-configuratie gekopieerd worden.

```
Switch# copy running-config startup-config
```

Het instellen van de standaardrouter kan met volgend commando.

```
Switch# configure terminal
Switch(config)# ip default-gateway 172.17.99.1
```

Om te controleren of alles correct is verlopen kan je de info van de ip-interfaces opvragen.

```
Switch#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	unassigned	YES	manual	up	up
FastEthernet0/2	unassigned	YES	manual	down	down
FastEthernet0/3	unassigned	YES	manual	down	down
...					
FastEthernet0/24	unassigned	YES	manual	down	down
GigabitEthernet1/1	unassigned	YES	manual	down	down
GigabitEthernet1/2	unassigned	YES	manual	down	down
Vlan1	unassigned	YES	manual	administratively down	down
Vlan99	172.17.99.2	YES	manual	up	down

1.2. Configure Switching Ports

❖ Instellen van snelheid en verbinding van de poort

Je kan de duplex-verbinding (full, half of auto), de snelheid (10, 100 of auto) instellen en auto-mdix (medium-dependent-interface-crossover) instellen zodat je overall straight-through kabel kan gebruiken.

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# duplex auto
Switch(config-if)# speed auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

Je kan controleren of auto-mdix aanstaat op een poort.

```
Switch# show controllers ethernet-controller fa 0/1 phy | include Auto-MDIX
```

❖ Verificatie van de configuratie

Er zijn verschillende commando's om de instellingen van de switch te verifiëren.

```
Switch# show interfaces
Switch# show startup-config
Switch# show running-config
Switch# show flash
Switch# show version
Switch# show history
Switch# show ip
Switch# show mac-address-table
```

1.3. Secure Remote Access

❖ Basisbeveiliging van de toegang (herhaling CCNA1)

Ken een andere naam toe aan de switch en stel een message of the day in.

```
Switch(config)# hostname Switch1
Switch1(config)#banner motd #Enkel toegang voor geautoriseerde gebruikers#
```

Je kan een niet-versleuteld of versleuteld paswoord zetten op het enable-commando. Zonder dit paswoord kan je niet naar de privileged Exec mode en dus geen wijzigingen aan de instellingen aanbrengen.

```
Switch1(config)# enable password px1
```

Het bovenstaand ingesteld paswoord met enable password wordt opgeslagen in ASCII en is gewoon leesbaar in de configuratiefiles. Indien je liever hebt dat dit paswoord versleuteld wordt doorgestuurd en opgeslagen dan kan dit met enable secret.

```
Switch1(config)# enable secret px1
```

Je kan ook een paswoord zetten op de console lijn en de telnettoegang.

```
Switch1(config)#service password-encryption
Switch1(config)#line console 0
Switch1(config-line)#password px1
Switch1(config-line)#login
```

Een tweede mogelijkheid van toegang is over de vty-lijnen (*Virtual Teletype Terminal*) met een telnetsessie. Alle apparatuur ondersteunt 5 lijnen, genummerd van 0 tot 4. Dit aantal kan tot 16 gaan (vty 0 tot 15). De configuratie is gelijkaardig aan die van de consolelijn.

```
Switch1(config)#line vty 0 15
Switch1(config-line)#password px1
Switch1(config-line)#login
```

Om ervoor te zorgen dat je geen meldingen (unsolicited messages) halverwege je commando verkrijgt kan je op de console- en vty-lijnen de synchrone logging aanzetten.

```
Switch1(config)#line vty 0 15
Switch1(config-line)#logging synchronous
```

Om te beveiligen tegen ongewenste DNS-lookups:

```
Switch1(config)#no ip domain-lookups
```

❖ Beveiligde toegang via SSH

Een betere beveiliging dan telnet is SSH. Hiervoor moet de switch wel een unieke naam in het netwerk hebben. Daarna moet je sleutels aanmaken.

```
Switch# configure terminal
Switch(config)# Hostname S1

S1(config)#ip domain-name cisco.com
S1(config)#crypto key generate rsa
The name for the keys will be: S1.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

In een volgende stap maak je een gebruiker aan en stel je in dat alle vty-lijnen enkel nog ssh-connecties mogen aanvaarden en er met een lokale gebruiker moet ingelogd worden.

```
S1(config)#username admin password px1
*mrt 1 0:1:6.676: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#line vty 0 15
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#end
S1#
```

Je kan ook voor versie2 van ssh kiezen.

```
S1(config)#ip ssh version 2
```

En controleren

```
S1#show ip ssh
S1#show ssh
```

1.4. Basic Router Configuration

❖ Basis Router Settings

▪ Instelling van hostname

De apparatuur zal standaardmatig de naam switch of router dragen. In een netwerk met vele apparaten is dat allesbehalve handig. Daarom wordt het aangeraden alles te hernoemen met het `hostname`-commando.

```
router#configure terminal
router(config)#hostname R1
```

Je kan een instelling steeds wijzigen door het `no`-commando.

```
R1#configure terminal
R1#no hostname
Router(config)#
```


Je kan een niet-versleuteld of versleuteld paswoord zetten op het `enable`-commando. Zonder dit paswoord kan je niet naar de privileged Exec mode en dus geen wijzigingen aan de instellingen aanbrengen.

```
Router(config)# enable password pxl
```

Het bovenstaand ingesteld paswoord met `enable password` wordt opgeslagen in ASCII en is gewoon leesbaar in de configuratiefiles. Indien je liever hebt dat dit paswoord versleuteld wordt doorgestuurd en opgeslagen dan kan dit met `enable secret`.

```
Router(config)# enable secret pxl
```

▪ Beveiliging van toegang op afstand

Je kan ook een paswoord zetten op de console lijn en de telnettoegang. Eerst kies je het configuratieniveau van de lijningangen. Daarna kan je met het `password`-commando een paswoord instellen en met het `login`-commando ervoor zorgen dat authenticatie aangezet wordt.

```
Router(config)#line console 0
Router(config-line)#password pxl
Router(config-line)#login
```

Een tweede mogelijkheid van toegang is over de vty-lijnen (*Virtual Teletype Terminal*) met een telnetsessie. Alle apparatuur ondersteunt 5 lijnen, genummerd van 0 tot 4. Dit aantal kan tot 16 gaan (vty 0 tot 15). De configuratie is gelijkaardig aan die van de consolelijn.

```
Router(config)#line vty 0 15
Router(config-line)#password pxl
Router(config-line)#login
Router(config-line)#exit
Router(config)#service password-encryption
```

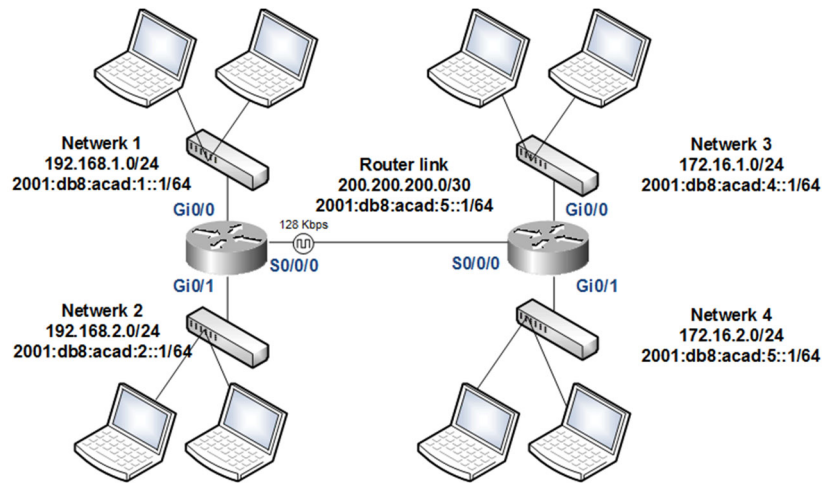
Om ervoor te zorgen dat je geen meldingen (unsolicited messages) halverwege je commando verkrijgt kan je op de console- en vty-lijnen de synchrone logging aanzetten.

```
Router(config)#line vty 0 15
Router(config-line)#logging synchronous
```

Alleen een hostnaam is vaak niet duidelijk genoeg, het kan handig zijn ook een melding mee te geven. Vaak worden deze meldingen gebruikt om juridische redenen. De meest gebruikte banners zijn de login-banner en de motd-banner (message of the day).

De melding moet binnen niet getoonde karakters zitten, vaak worden quotes ("melding") of hekjes (#melding #) gebruikt.

```
R1(config)#banner login "Router van het departement PXL-it"
R1(config)#banner motd "Alle acties worden gelogd!"
```



Figuur 4: Voorbeeldnetwerk

❖ Configure Router Interfaces

De Ethernetpoorten (100Mbit, 1Gbit) van routers dienen een IP-adres te krijgen en moeten aanzet worden met het `no shutdown`-commando. Je kan ook een beschrijving aan een poort toekennen.

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# description Link to LAN 1
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/1
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# description Link to LAN 2
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ip address 200.200.200.1 255.255.255.252
R1(config-if)# ipv6 address 2001:db8:acad:5::225/64
R1(config-if)# description Link to R2
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
```

▪ Instelling van seriële interfaces

De seriële poorten worden op dezelfde wijze geconfigureerd.

```
R1(config)#interface serial 0/0/0
R1(config-if)#description Connectie naar R2
R1(config-if)#ip address 200.200.200.2 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
```

Seriële kabels zijn voorzien van een DCE- en een DTE-kant. Aan de zijde van DCE (Data Circuit-terminating Equipment) moet je de klok instellen. Deze klok wordt overgenomen door de DTE-kant (Data Terminal Equipment). De aanduiding is aangegeven op het kabeleinde, maar kan ook opgevraagd worden in IOS.

```
R1#show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 128000
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
```

❖ Instelling van loopback interface

Om ervoor te zorgen dat elke router een vast router-id heeft, worden loopbackadressen (virtuele interfaces) gebruikt. Een loopback staat immers altijd "up". Dit is ook nuttig voor testing.

```
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
```

1.5. Verify Directly Connected Networks

Na het instellen van de interfaces controleer je best of alles juist is gebeurd.

```
R1#show ip interface brief
Interface                IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0       192.168.1.1     YES manual  up                    up
GigabitEthernet0/1       192.168.2.1     YES manual  up                    up
Serial0/0/0              200.200.200.2   YES manual  up                    up
Serial0/0/1              unassigned      YES unset   administratively down  down
Loopback0                172.0.0.1       YES manual  up                    up
Vlan1                    unassigned      YES unset   administratively down  down
R1#
```

Gefilterd:

```
R1#show ip interface brief | exclude unassigned
Interface                IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0       192.168.1.1     YES manual  up                    up
GigabitEthernet0/1       192.168.2.1     YES manual  up                    up
Serial0/0/0              200.200.200.2   YES manual  up                    up
Loopback0                172.0.0.1       YES manual  up                    up
R1#
```

Of voor IPv6:

```
R1#show ipv6 interface brief
```

Per interface:

```
show ipv6 interface gigabitethernet 0/0/0
```

❖ Route opvragen

Routetabel opvragen.

```
R1# show ip route
```

❖ Filteren van show commando

Je kan slechts een gedeelte van de output laten genereren te filteren, bijvoorbeeld op section.

```
R1# show running-config | section line vty
line vty 0 4
 password 7 110A1016141D
 login
 transport input all
```

Filteren op begin:

```
R1#show running-config | begin Serial0/0/0
interface Serial0/0/0
description Connectie naar ISP
ip address 200.200.200.2 255.255.255.252
clock rate 128000
!
interface Serial0/0/1
no ip address
```

ipv6 route

▪ Commando geschiedenis

Je kan de laatst gebruikte commando's opvragen.

```
R1# terminal history size 200
R1#
R1#show history
show ip interface brief
show running-config | begin Serial0/0/0
terminal history size 200
show history
```

Hoofdstuk 2: Switching Concepts

Hoofdstuk 3: VLANs

3.1. Overview VLAN

3.2. VLAN's in a Multi-Switched Environment

3.3. VLAN Configuration

❖ Aanmaken en configuratie van een VLAN

▪ Aanmaken van een VLAN

Bij het aanmaken van een VLAN moet er een ID meegegeven worden. Je kan ook een naam meegeven.

```
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name lector
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name student
Switch(config-vlan)# exit
Switch(config)# vlan 30
Switch(config-vlan)# name gast
Switch(config-vlan)# exit
```

Je kan de databank van vlan's opvragen. Indien er nog geen toewijzingen gebeurd zijn, zitten alle poorten nog in het standaard VLAN 1. Dit default VLAN kan niet gewist worden.

```
Switch# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
10	lector	active	
20	student	active	
30	gast	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Met het no-commando kan je een vlan verwijderen

```
Switch(config)# no vlan 20
```

Alle vlan's wissen en de switch opstarten in zijn fabrieksinstelling, doe je door de databank en de opstartconfiguratie te wissen.

```
Switch# erase flash:vlan.dat
Switch# erase startup-config
Switch# reload
```

❖ Poorten toekennen aan een VLAN

Een 'tagged' switchpoort is een poort waaraan een VLAN is toegekend. Je dient ook de modus (access, dynamic of trunk) van de interface mee te geven. Als het toegekende VLAN nog niet bestaat, wordt het aangemaakt.

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# end
```

Je kan de info per poort opvragen.

```
Switch# show interfaces fa 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Pector) ...
```

Met het no switchport-commando kan je een poort terug uit een vlan verwijderen. De poort komt dan terug in het default VLAN1.

```
Switch#configure terminal
Switch(config)#interface fa0/1
Switch(config-if)#no switchport access vlan 10
Switch(config-if)#end
```

Configureren van een data and voice VLAN

```
S3(config)# vlan 20
S3(config-vlan)# name student
S3(config-vlan)# exit
S3(config)# vlan 150
S3(config-vlan)# name VOICE
S3(config-vlan)# exit
S3(config)# interface fa0/18
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 20
S3(config-if)# mls qos trust cos
S3(config-if)# switchport voice vlan 150
S3(config-if)# end
S3#
```

❖ Verificatie van installatie

Bij het opvragen van de VLAN-configuratie, kan je verder specificeren.

```
Switch# show vlan name student
```

VLAN Name	Status	Ports
20 student	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
20	enet	100020	1500	-	-	-	-	-	0	0

```
Switch# show vlan id 10
VLAN Name                Status    Ports
-----
10    lector                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                   Fa0/5

VLAN Type  SAID      MTU    Parent RingNo BridgeNo  Stp    BrdgMode Trans1 Trans2
-----
20    enet  100020   1500    -       -       -       -       -         0      0
```

Een samenvatting kan je opvragen met de parameter summary (werkt niet in Packet Tracer).

```
Switch# show vlan summary
```

De informatie van de SVI (hier VLAN 99) vraag je op via show interfaces vlan {id}. Oudere switchen kunnen maar één SVI hebben, vanaf de 2960 zijn er meerdere SVI's mogelijk.

```
Switch#show interfaces vlan 99
Vlan99 is up, line protocol is up
  Hardware is CPU Interface, address is 0001.4240.4601 (bia 0001.4240.4601)
  Internet address is 172.17.99.2/16
  MTU 1500 bytes, BW 100000 kbit, DLY 1000000 usec,
  ...
```

3.4. VLAN trunks

Voor poorten die meerdere VLAN's moeten doorschakelen dient trunking aangezet te worden.

```
Switch(config)# interface G0/0
Switch(config-if)# switchport mode trunk
```

Instellen van een native VLAN (het VLAN om pakketten op uit te sturen die niet tot een VLAN behoren).

```
Switch(config)# interface g0/1
Switch(config-if)# switchport trunk native vlan 99
```

Beperking van de VLAN's die toegelaten worden op de trunk. In onderstaand voorbeeld kunnen de VLAN's 10, 20 en 99 op de trunkverbinding.

```
Switch(config)# interface g0/1
Switch(config-if)# switchport trunk allowed vlan 10,20, 99
```

Je kan ook per VLAN toevoegen of verwijderen

```
Switch(config-if)# switchport trunk allowed vlan add 99
Switch(config-if)# switchport trunk allowed vlan remove 99
```

Met het no switchport-commando kan je een poort terug uit een vlan verwijderen. De poort komt dan terug in het default VLAN1.

```
Switch#configure terminal
Switch(config)#interface G0/1
Switch(config-if)#no switchport trunk allowed vlan
Switch(config-if)#no switchport trunk native vlan
Switch(config-if)#end
```

Met show interfaces trunk krijg je een overzicht van de getrunkte poorten.

```
Switch#show interface trunk
```


Port Gig0/1	Mode on	Encapsulation 802.1q	Status trunking	Native vlan 99
Port Gig0/1	Vlans allowed on trunk 10,20,30,99			
Port Gig0/1	Vlans allowed and active in management domain 10,20,30,99			
Port Gig0/1	Vlans in spanning tree forwarding state and not pruned 10,20,30,99			

Je kan meer gedetailleerde informatie opvragen over de trunkpoorten.

```
Switch#show interfaces g0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Management)
...
```

3.5. DTP: Dynamic Trunking Protocol

Er zijn vier modi: access, trunk, dynamic desirable en dynamic auto. De access mode staat vast in accessmodus.

```
Switch(config-if)# switchport mode access
```

De trunk mode staat vast in trunkmodus.

```
Switch(config-if)# switchport mode trunk
```

Dynamic auto zal wijzigen naar trunk als de andere zijde trunk of dynamic desirable is.

```
Switch(config-if)# switchport mode dynamic auto
```

Dynamic desirable zal altijd wijzigen naar trunk, behalve als de andere zijde access is.

```
Switch(config-if)# switchport mode dynamic desirable
```

Je kan DTP ook afzetten.

```
Switch(config-if)# switchport nonegotiate
```

Opvragen van de DTP-status kan met

```
Switch# show dtp interface F0/1
```

Of met

```
Switch# show interface F0/1 switchport
```

```
: 10 (lector)
```

Hoofdstuk 4: Inter-VLAN Routing

4.1. Inter-VLAN Routing Operation

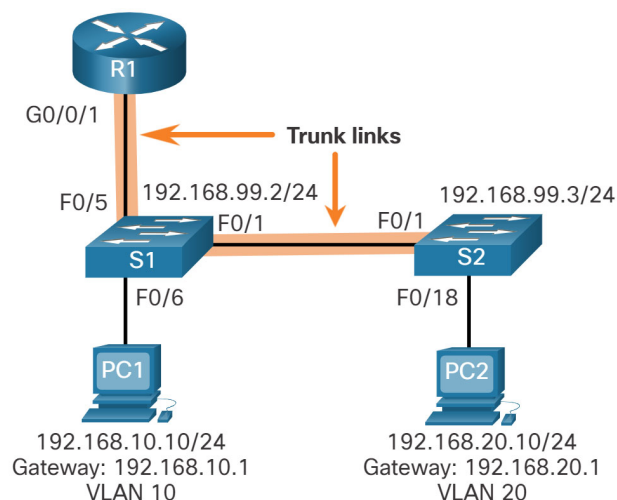
4.2. Router-on-a-Stick Inter-VLAN Routing

❖ Router-on-a-stick

Het toekennen van bijvoorbeeld drie VLAN's (10,20,99 aan één enkele routerpoort)

```
routerB#configure terminal
routerB(config)#interface g0/0.10
routerB(config-if)#encapsulation dot1q 10
routerB(config-if)#ip address 192.168.10.1 255.255.255.0
routerB(config)#interface g0/0.20
routerB(config-if)#encapsulation dot1q 20
routerB(config-if)#ip address 192.168.20.1 255.255.255.0
routerB(config)#interface g0/0.99
routerB(config-if)#encapsulation dot1q 99
routerB(config-if)#ip address 192.168.99.1 255.255.255.0
routerB(config-if)#interface g0/0
routerB(config-if)#no shutdown
routerB(config-if)#exit
routerB(config)#
```

❖ Case study: Router-on-a-Stick



▪ Installatie van Switch1

Aanmaken van de VLAN's

```
S1(config)# vlan 10
S1(config-vlan)# name LAN10
S1(config-vlan)# exit
S1(config)# vlan 20
S1(config-vlan)# name LAN20
S1(config-vlan)# exit
S1(config)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)#
```

Aanmaken van de management SVI en configuratie van default gateway

```
S1(config)# interface vlan 99
S1(config-if)# ip add 192.168.99.2 255.255.255.0
```

```
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.99.1
S1(config)#
```

Toekennen van de poorten

```
S1(config)# interface fa0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# no shut
S1(config-if)# exit
S1(config)#
```

Configuratie van de trunkpoorten

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode trunk
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# interface fa0/5
S1(config-if)# switchport mode trunk
S1(config-if)# no shut
S1(config-if)# end
```

Hetzelfde voor Switch 2

```
S2(config)# vlan 10
S2(config-vlan)# name LAN10
S2(config-vlan)# exit
S2(config)# vlan 20
S2(config-vlan)# name LAN20
S2(config-vlan)# exit
S2(config)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# exit
S2(config)#
S2(config)# interface vlan 99
S2(config-if)# ip add 192.168.99.3 255.255.255.0
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.99.1
S2(config)# interface fa0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# interface fa0/1
S2(config-if)# switchport mode trunk
S2(config-if)# no shut
S2(config-if)# exit
S2(config-if)# end
```

Configuratie van Router-on-a-Stick op R1

```
R1(config)# interface G0/0/1.10
R1(config-subif)# description Default Gateway for VLAN 10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip add 192.168.10.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.20
R1(config-subif)# description Default Gateway for VLAN 20
R1(config-subif)# encapsulation dot1q 20
R1(config-subif)# ip add 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
```

```

R1(config)# interface G0/0/1.99
R1(config-subif)# description Default Gateway for VLAN 99
R1(config-subif)# encapsulation dot1q 99
R1(config-subif)# ip add 192.168.99.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1
R1(config-if)# description Trunk link to S1
R1(config-if)# no shut
R1(config-if)# end

```

4.3. Inter-VLAN routing using Layer 3 Switches

▪ Layer 3 Switch inter-VLAN Routing

Toekennen van meerdere SVI's aan de switch en het enablen van IPv4 Routing

```

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

```

Routeren enablen

```

Switch(config)#ip routing
Switch(config)#

```

4.4. Troubleshoot inter-VLAN Routing

❖ Troubleshooting VLAN's en trunks

De commando's

```

Switch# show vlan
Switch# show vlan brief
Switch# show mac-address table
Switch# show interfaces switchport
Switch# show interfaces trunk

```

▪ Missend VLAN

Als er een probleem is met een poort, vraag eerst de MAC-adrestabel op.

```

Switch#show mac-address-table
          Mac Address Table
-----
Vlan      Mac Address      Type      Ports
----      -
10        0001.962a.982c   DYNAMIC   Fa0/1
Switch#

```

Controleer daarna die specifieke poort en bekijk Access Mode VLAN. Als dit VLAN niet bestaat staat daar "Inactive"

```
Switch#show interface fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
```

▪ Switch trunk issues

Controleer welke interfaces als trunk geconfigureerd zijn

```
Switch# show interfaces trunk
```

▪ MAC-adrestabel

Opvragen van de MAC-adrestabel.

```
Switch# show mac-address-table
      Mac Address Table
-----
Vlan    Mac Address      Type        Ports
----    -
  99    0003.e498.c978   DYNAMIC     Fa0/1
```

Je kan hierbij filteren op dynamisch geleerde MAC-adressen.

```
Switch# show mac-address-table dynamic
      Mac Address Table
-----
Vlan    Mac Address      Type        Ports
----    -
  99    0003.e498.c978   DYNAMIC     Fa0/1
```

De geleerde MAC-adressen kan je ook uit het geheugen verwijderen.

```
Switch# clear mac-address-table dynamic
Switch# show mac-address-table dynamic
      Mac Address Table
-----
Vlan    Mac Address      Type        Ports
----    -
```

Access Mode VLAN

Hoofdstuk 5: STP concepts

5.1. Purpose of Spanning Tree Concepts

5.2. STP Operations

5.3. Evolution of STP

❖ PVST+

❖ Rapid PVST+

5.4. Spanning Tree Configuration

❖ PVST+ Configuration

Het opvragen van de spanning tree configuratie

```
Switch# show spanning-tree
```

Bridge-id aanpassen om de root bridge manueel te kiezen, kan door de prioriteit op een kleiner veelvoud van 4096 (of een veelvoud hiervan) te zetten en kleiner te houden dan de prioriteit van de andere switchen.

```
Switch(config)# spanning-tree VLAN xx priority 4096
```

Bridge-id aanpassen om de root bridge dynamisch te kiezen.

```
Switch(config)# spanning-tree VLAN xx root primary
```

Bridge-id aanpassen om de back-up root bridge dynamisch te kiezen.

```
Switch(config)# spanning-tree VLAN xx root secondary
```

Het opvragen van de actieve interfaces in spanning tree configuratie.

```
Switch# show spanning-tree active
```

Het opvragen van de spanning tree configuratie per VLAN.

```
Switch# show spanning-tree vlan xx
```

❖ **Rapid PVST+ Configuration**

Alle configuratiecommando's zijn hetzelfde als bij PVST+.

Het wijzigen van PVST+ (default op Cisco 2960), naar RPVST+

```
Switch(config)# spanning-tree mode rapid-pvst
```

Het herstarten van het spanning tree proces.

```
Switch(config)# clear spanning-tree detected-protocols
```

Het identificeren van de interswitch links als point-to-point (dit is enkel nodig als er nog hubs in het netwerk aanwezig zijn).

```
Switch(config-if)# spanning-tree link-type point-to-point
```

Hoofdstuk 6: EtherChannel

6.1. EtherChannel Operation

6.2. Configure Etherchannel

❖ Configuring EtherChannel

De configuratie van EtherChannel met LACP. Zorg er altijd voor dat de interfaces op dezelfde parameters staan.

```
Switch(config)# interface range FastEthernet 0/1-2
Switch(config-if-range)# shutdown
Switch(config-if-range)# duplex auto
Switch(config-if-range)# speed 100
Switch(config-if-range)# channel-group 1 mode active
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

Na het aanmaken van de linkaggregatie kan de interface geconfigureerd worden.

```
Switch(config)# interface port-channel 1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10, 20, 30
```

De configuratie van EtherChannel met PAgP.

```
Switch(config)# interface range FastEthernet 0/1-2
Switch(config-if-range)# channel-group 1 mode desirable
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

❖ Troubleshooting EtherChannel

Opvragen van linkaggregatie interface.

```
Switch# show interfaces port-channel
```

Opvragen van de EtherChannel info van meerdere port-channels.

```
Switch# show etherchannel summary
```

Of van één specifieke port-channel

```
Switch# show etherchannel port-channel
```

Of van één specifieke interface van een port-channel

```
Switch# show interface f0/1 etherchannel
```


Hoofdstuk 7: DHCPv4

7.1. Dynamic Host Configuration Protocol versie 4

7.2. Configure a Cisco IOS DHCPv4 Server

Binnen een bereik dat een DHCP-server moet uitdelen zijn vaak adressen al vast toegekend aan routerpoorten of servers. Deze adressen mogen niet langer uitgedeeld worden.

```
Router(config)# ip dhcp excluded-address 172.16.1.1
Router(config)# ip dhcp excluded-address 172.16.1.254
```

Dit kan ook dadelijk een bereik aan adressen zijn.

```
Router(config)# ip dhcp excluded-address 172.16.1.1 172.16.1.9
```

Daarna kan de DHCP-pool aangemaakt worden en worden geconfigureerd met netwerknummer, standaardrouter, dns-server, ...

```
Router(config)# ip dhcp pool LAN-POOL-1
Router(dhcp-config)#network 172.16.1.0 255.255.255.0
Router(dhcp-config)#default-router 172.16.1.1
Router(dhcp-config)#dns-server 172.16.1.254
Router(dhcp-config)#domain-name pxl.be
```

▪ Troubleshooting

Controleer of de service wel aan staat. Onderstaand commando zou geen resultaat mogen hebben.

```
Router# show running-config | include no service dhcp
```

Indien DHCP niet aanstaat

```
Router# service dhcp
```

Controleer de DHCP-binding of statistieken

```
Router# show ip dhcp binding
Router# show ip dhcp server statistics
```

Je kan ook de debugging aanzetten.

```
Router# debug ip dhcp server events
```

❖ DHCP relay

Aangezien DHCP gebruik maakt van broadcastframes worden deze geblokkeerd door elke L3-apparaat, zoals routers. Wil je toch DHCP-request toelaten over de router heen, dan dient een ip-helperadres ingesteld te worden.

```
Router(config)# interface g0/0
Router(config-if)#ip helper-address 172.16.1.1
```

7.3. Configure a DHCPv4 Client

Een routerpoort kan ook ingesteld worden om dynamisch een IP-adres te bekomen.

```
Router(config)# interface g0/0  
Router(config-if)# ip address dhcp
```

Hoofdstuk 8: SLAAC and DHCPv6

8.1. IPv6 GUA Assignment

8.2. Stateless Address Autoconfiguration (SLAAC)

8.3. DHCPv6

8.4. Configure DHCPv6 Server

❖ Configuratie van Stateless DHCPv6

Eerst dien je IPv6 routing aan te zetten, en daarna maak je identiek aan DHCPv4 maak je een pool aan met als zijn parameters.

```
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 dhcp pool LAN-IPV6-1
Router(config-dhcpv6)#address prefix 2001:db8:cafee:1::/64 lifetime infinite
Router(config-dhcpv6)#dns-server 2001:db8:cafee:aaaa::5
Router(config-dhcpv6)#domain-name pxl.be
```

Daarna koppel je het aan een interface en zet je de configuratievlag van 0 naar 1.

```
Router(config)# interface g0/1
Router(config-if)# ipv6 address 2001:db8:café:1::1/64
Router(config-if)# ipv6 dhcp server LAN-IPV6-1
Router(config-if)# ipv6 nd other-config-flag
```

❖ Configuratie van Stateless DHCPv6-client

Een routerpoort kan ook ingesteld worden om dynamisch een IPv6-adres te bekomen.

```
Router(config)# ipv6 unicast-routing
Router(config)# interface g0/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address autoconfig
```

❖ Configuratie van Stateful DHCPv6

Het is erg gelijkend op stateless DHCPv6. Eerst dien je IPv6 routing aan te zetten. Identiek aan stateless DHCPv6 maak je een pool aan met als zijn parameters. Hier dien je wel een adressenbereik mee te geven.

```
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 dhcp pool LAN-IPV6-1
Router(config-dhcpv6)#address prefix 2001:db8:cafee:1::/64 lifetime infinite
Router(config-dhcpv6)#dns-server 2001:db8:cafee:aaaa::5
Router(config-dhcpv6)#domain-name pxl.be
```

Daarna koppel je het aan een interface en zet je de managed vlag van 0 naar 1.

```
Router(config)# interface g0/1
Router(config-if)# ipv6 address 2001:db8:café:1::1/64
Router(config-if)# ipv6 dhcp server LAN-IPV6-1
Router(config-if)# ipv6 nd managed-config-flag
Router(config-if)# ipv6 nd prefix default no-autoconfig
```

❖ Configuratie van Stateful DHCPv6-client

Een routerpoort kan ook ingesteld worden om dynamisch een IPv6-adres te bekomen.

```
Router(config)# ipv6 unicast-routing
Router(config)# interface g0/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address dhcp
```

❖ Troubleshoot van DHCPv6

Controleer de instellingen.

```
Router# show ipv6 dhcp pool
Router# show ipv6 dhcp binding
Router# show ipv6 interface g0/0
Router# debug ipv6 dhcp detail
```

❖ DHCPv6 relay

Ook bij DHCPv6 is het soms nodig een relay agent in te stellen.

```
Router(config)# interface g0/0
Router(config-if)#ipv6 dhcp relay destination 2001:db8:cafe:1::6
```

Controleer de instellingen.

```
Router# show ipv6 dhcp interface
Router# show ipv6 dhcp binding
```

Hoofdstuk 9: FHRP Concepts

9.1. First Hop Redundancy Protocols

9.2. HSRP

❖ HSRP configuration

De configuratie van HSRP op Router1, met een virtueel IP-adres van 192.168.1.1 en met preempt zodat een herverkiezing op basis van prioriteit wordt afgedwongen.

```
Router1(config)# interface GigabitEthernet 0/1
Router1(config-if)# ip address 192.168.1.10 255.255.255.0
Router1(config-if)# standby version 2
Router1(config-if)# standby 1 ip 192.168.1.1
Router1(config-if)# standby 1 priority 110
Router1(config-if)# standby 1 preempt
Router1(config-if)# no shutdown
```

De configuratie van HSRP op Router2, ook met een virtueel IP-adres van 192.168.1.1, maar met lagere prioriteit.

```
Router2(config)# interface GigabitEthernet 0/1
Router2(config-if)# ip address 192.168.1.11 255.255.255.0
Router2(config-if)# standby version 2
Router2(config-if)# standby 1 ip 192.168.1.1
Router2(config-if)# standby 1 priority 90
Router2(config-if)# no shutdown
```

❖ HSRP troubleshooting

De configuratie van HSRP opvragen.

```
Router# show standby
```

Een kortere versie opvragen.

```
Router# show standby brief
```

Debug aanzetten, kan met errors, events, packets en terse.

```
Router# debug standby packets
Router# debug standby terse
Router# debug standby errors
Router# debug standby events
```

Hoofdstuk 10: LAN Security Concepts

10.1. Endpoint Security

10.2. Access Control

Beveiligen van de toegang is over de vty-lijnen (*Virtual Teletype Terminal*) met een telnetsessie. Alle apparatuur ondersteunt 5 lijnen, genummerd van 0 tot 4. Dit aantal kan tot 16 gaan (vty 0 tot 15). De configuratie is gelijkaardig aan die van de consolelijn.

```
Switch1(config)#line vty 0 15
Switch1(config-line)#password px1
Switch1(config-line)#login
```

Een betere beveiliging dan telnet is SSH. Hiervoor moet de switch wel een unieke naam in het netwerk hebben. Daarna moet je sleutels aanmaken.

```
Switch# configure terminal
Switch(config)# hostname S1

S1(config)#ip domain-name cisco.com
S1(config)#crypto key generate rsa
The name for the keys will be: S1.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

In een volgende stap maak je een gebruiker aan en stel je in dat alle vty-lijnen enkel nog ssh-connecties mogen aanvaarden en er met een lokale gebruiker moet ingelogd worden.

```
S1(config)#username admin password px1
*mrt 1 0:1:6.676:  %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#ssh version 2
S1(config)#line vty 0 15
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#end
S1#
```

10.3. Layer 2 Security Threats

10.4. MAC Address Table Attack

10.5. LAN Attacks

Hoofdstuk 11: Switch security Configuration

11.1. Implement Port Security

❖ Ongebruikte poorten uitzetten

Ongebruikte switchpoorten kunnen om veiligheidsredenen afgezet worden.

```
S1(config)#interface range fastethernet 0/3-24
S1(config-if-range)#shutdown
```

❖ Switch port security

Instellen van poortbeveiliging met sticky mac-adressen.

```
S1(config)#interface fastethernet 0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 50
S1(config-if)#switchport port-security mac-address sticky
```

Fine-tuning van port security

```
S1(config)#interface fastethernet 0/1
S1(config-if)#switchport port-security aging time
S1(config-if)#switchport port-security violation restrict
S1(config-if)#switchport port-security violation protect
S1(config-if)#switchport port-security violation shutdown
```

Het opnieuw enablen van een poort na violation doe je door de poort af te zetten en terug aan te zetten.

```
S1(config)#interface FastEthernet 0/1
S1(config)#shutdown
S1(config)#no shutdown
```

Het opvragen van de poortbeveiliging.

```
S1#show port-security interface fa 0/1
Port Security           : Enabled
Port Status             : Secure-down
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 50
Total MAC Addresses     : 0
Configured MAC Addresses : 0
Sticky MAC Addresses    : 0
Last Source Address:vlan : 0000.0000.0000:0
Security Violation Count : 0
```

Het opvragen van de adressen behorende tot een poortbeveiliging.

```
S1#show port-security address
```

11.2. Mitigate VLAN Attacks

❖ VLAN Hopping Attack

Een VLAN hopping attack tegenhouden

```
S1(config)# interface range fa0/1 - 16
S1(config-if-range)# switchport mode access
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/17 - 20
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1000
S1(config-if-range)# shutdown
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/21 - 24
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport nonegotiate
S1(config-if-range)# switchport trunk native vlan 999
S1(config-if-range)# end
```

11.3. Mitigate DHCP Attacks

❖ DHCP Snooping

Configuratie van DHCP snooping

```
S1(config)# ip dhcp snooping
S1(config)# interface f0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)# interface range f0/5 - 24
S1(config-if-range)# ip dhcp snooping limit rate 6
S1(config-if-range)# exit
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)# end
```

Controle:

```
S1# show ip dhcp snooping
```

11.4. Mitigate ARP Attacks

❖ Configuratie van DAI (Dynamic ARP Inspection)

Configuratie:

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10
S1(config)# ip arp inspection vlan 10
S1(config)# interface fa0/24
S1(config-if)# ip dhcp snooping trust
S1(config-if)# ip arp inspection trust
```

Configuratie om pakketten te onderzoeken en te droppen

```
S1(config)# ip arp inspection validate ?
dst-mac validate destination MAC address
ip validate IP addresses
src-mac validate source MAC address
S1(config)# ip arp inspection validate src-mac
S1(config)# ip arp inspection validate dst-mac
S1(config)# ip arp inspection validate ip
S1(config)# do show run | include validate
ip arp inspection validate ip
S1(config)# ip arp inspection validate src-mac dst-mac ip
S1(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
S1(config)#
```


11.5. Mitigate STP Attacks

❖ PortFast and BPDU Guard

Het configureren van PortFast op alle niet-trunking poorten (in global config mode)

```
Switch(config)# spanning-tree portfast
Switch(config)# spanning-tree portfast default
```

Het configureren van PortFast op één bepaalde access-poort (in interface config mode)

```
Switch(config)# int f0/1
Switch(config-if)# spanning-tree portfast
```

Het configureren van BPDU Guard op alle niet-trunking poorten (in global config mode)

```
Switch(config)# spanning-tree portfast bpduguard default
```

Het configureren van BPDU Guard op één bepaalde access-poort (in interface config mode)

```
Switch(config)# int f0/1
Switch(config-if)# spanning-tree bpduguard enable
```

Hoofdstuk 12: WLAN Concepts

Hoofdstuk 13: WLAN Configuration

Hoofdstuk 14: Routing concepts

14.1. Path Determinations

14.2. Packet Forwarding

14.3. Basic Router Configuration review

Herhaling van reeds behandelde IOS-commando's

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# logging synchronous
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)# banner motd #
Enter TEXT message. End with a new line and the #
*****
WARNING: Unauthorized access is prohibited!
*****
#
R1(config)# ipv6 unicast-routing
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ip address 10.0.1.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# ipv6 address fe80::1:a link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# description Link to LAN 2
R1(config-if)# ip address 10.0.2.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# ipv6 address fe80::1:b link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/1
R1(config-if)# description Link to R2
R1(config-if)# ip address 10.0.3.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# ipv6 address fe80::1:c link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

14.4. IP Routing Table

❖ Routetabellen

De routetabel opvragen doe je met het commando “show ip route”. Het resultaat toont minstens de connected en de local routes en de andere gekende netwerken.

```
R1#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

```
172.0.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.0.0.0/24 is directly connected, Loopback0
L    172.0.0.1/32 is directly connected, Loopback0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
L    192.168.1.1/32 is directly connected, GigabitEthernet0/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.2.0/24 is directly connected, GigabitEthernet0/1
L    192.168.2.1/32 is directly connected, GigabitEthernet0/1
200.200.200.0/24 is variably subnetted, 2 subnets, 2 masks
C    200.200.200.0/30 is directly connected, Serial0/0/0
L    200.200.200.2/32 is directly connected, Serial0/0/0
R1#
```

❖ Opvragen van statische standaardroute

Opvragen van de routetabel

```
R1# show ip route static
R1# show ipv6 route static
```

Connectiviteit testen.

```
R1#ping 172.16.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

```
escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:2::2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/11 ms
R1#
```

Hoofdstuk 15: IP Static Routing

15.1. Static Routes

❖ Opvragen van de routetabel

Het belangrijkste aspect van het configureren van een router is het bekomen van foutloze en volledige routetabellen. Je kan de routetabel opvragen met onderstaand commando.

```
Router# show ip route
```

15.2. Configure IP Static Routes

❖ Statische routes in IPv4

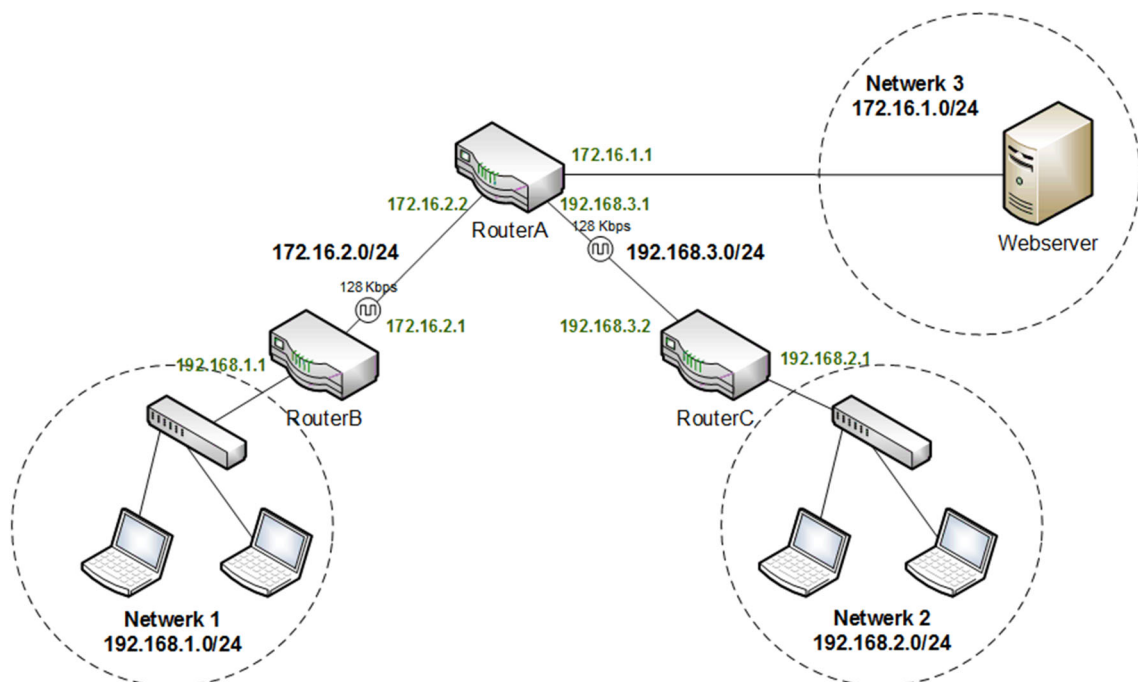
▪ Configureren van IPv4 statische routes

Toevoegen van statische routes met een next-hop adres

```
Router(config)#ip route network-address subnet-mask {ip-address | exit-intf}
```

Verwijderen van statische routes met een exit interface

```
Router(config)# no ip route network-address subnet-mask {ip-address | exit-intf}
```



Figuur 5: Voorbeeldnetwerk statische routes

▪ Configureren van IPv4 statische routes met next-hop adres

Het toevoegen van statische routes met een next-hop adres is aangewezen bij multiple access verbindingen, zoals bij het gebruik van UTP-bekabeling.

```
RouterB(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.2
RouterB(config)#ip route 192.168.2.0 255.255.255.0 172.16.2.2
RouterB(config)#ip route 192.168.3.0 255.255.255.0 172.16.2.2
```

▪ Configureren van IPv4 statische routes met exit interface

Het toevoegen van statische routes met een exit interface is aangewezen voor point-to-point connecties, zoals seriële verbindingen.

```
RouterB(config)#ip route 172.16.1.0 255.255.255.0 Serial 0/0
RouterB(config)#ip route 192.168.2.0 255.255.255.0 Serial 0/0
RouterB(config)#ip route 192.168.3.0 255.255.255.0 Serial 0/0
```

▪ Configureren van fully specified IPv4 statische routes

Bij multi-access bekabeling kan ook alles gespecificeerd worden, dus zowel de exit interface als het next-hop adres. Stel dat in het bovenstaand voorbeeldnetwerk de seriële kabels vervangen worden door UTP-kabels op de gigabitconnectoren.

```
RouterB(config)#ip route 172.16.1.0 255.255.255.0 G0/0 172.16.2.2
RouterB(config)#ip route 192.168.2.0 255.255.255.0 G0/0 172.16.2.2
RouterB(config)#ip route 192.168.3.0 255.255.255.0 G0/0 172.16.2.2
```

Je kan details van de routetabel opvragen met onderstaand commando.

```
Router# show ip route static | begin Gateway
```

▪ Configureren van IPv4 default routes

Toevoegen van een default gateway

```
Router(config)# ip route 0.0.0.0 0.0.0.0 { ip-address | exit-intf }
```

Voor RouterB en RouterC kunnen alle toegevoegde statische routes vervangen worden door een default route (quad zero) aangezien het hier gaat op doodlopende netwerken (stub network).

```
RouterB(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2
RouterC(config)#ip route 0.0.0.0 0.0.0.0 192.168.3.1
```

Om alle systeemmeldingen te zien tijdens het aanmaken en verwijderen van routes kan je de debug-optie aan te zetten.

```
Router# debug ip routing
```

De debug-optie afzetten doe je met het no-commando.

```
Router# no debug ip routing      (enkel debugging op routing afzetten)
Router# no debug all             (alle debugging afzetten)
```

❖ Statische routes met IPv6

▪ Configureren van IPv6 statische routes

Voor het invoeren van IPv6-routes gebruik je de volgende syntax.

```
Router(config)#ipv6 route ipv6-prefix/prefix-length {ipv6-address | exit-intf}
```

▪ Configureren van IPv6 statische routes met next-hop adres

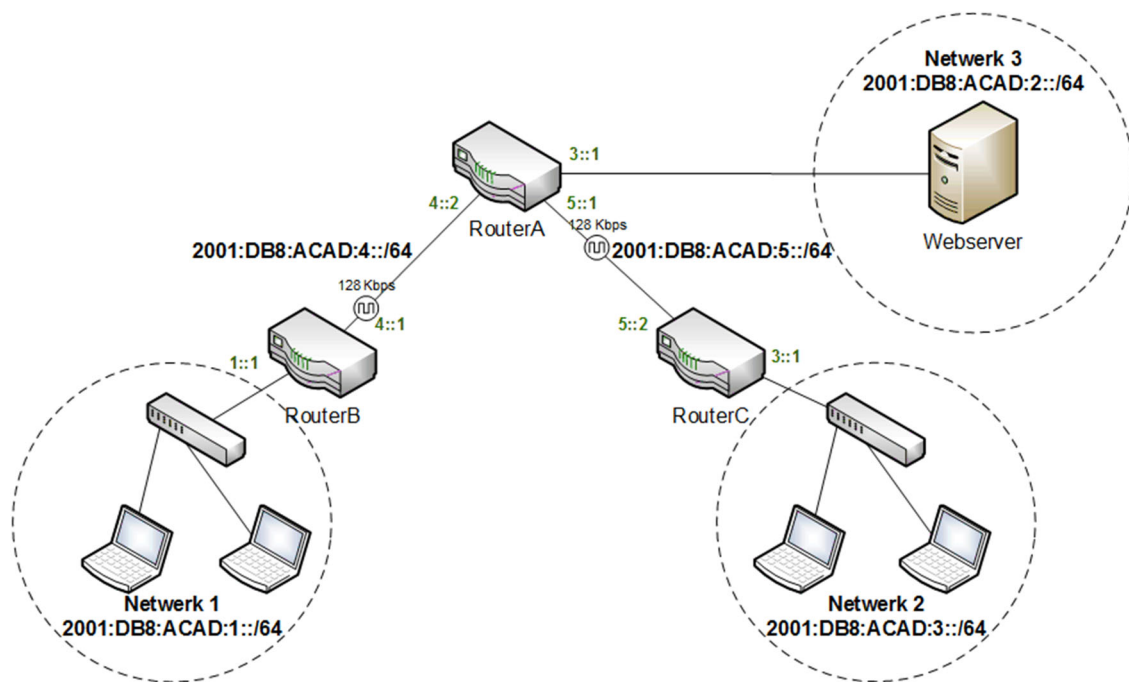
Het toevoegen van statische routes met een next-hop adres is aangewezen bij multiple access verbindingen, zoals bij het gebruik van UTP-bekabeling.

```
RouterB(config)#ipv6 route 2001:DB8:ACAD:3::/64 2001:DB8:ACAD:4::2
RouterB(config)#ipv6 route 2001:DB8:ACAD:4::/64 2001:DB8:ACAD:4::2
RouterB(config)#ipv6 route 2001:DB8:ACAD:4::/64 2001:DB8:ACAD:4::2
```

▪ Configureren van IPv6 statische routes met exit interface

Het toevoegen van statische routes met een exit interface is aangewezen voor point-to-point connecties, zoals seriële verbindingen.

```
RouterB(config)#ipv6 route 2001:DB8:ACAD:3::/64 serial 0/0
RouterB(config)#ipv6 route 2001:DB8:ACAD:4::/64 serial 0/0
RouterB(config)#ipv6 route 2001:DB8:ACAD:4::/64 serial 0/0
```



Figuur 6: IPv6 voorbeeldnetwerk met statische routes

▪ Configureren van fully specified IPv6 statische routes

In het geval dat een link local adres wordt gebruikt als next-hop moet de exit-interface eveneens vermeld worden zelfs ingeval van een point-to-point verbinding.

```
RouterB(config)#ipv6 route 2001:DB8:ACAD:3::/64 serial 0/0 fe80::2
RouterB(config)#ipv6 route 2001:DB8:ACAD:4::/64 serial 0/0 fe80::2
RouterB(config)#ipv6 route 2001:DB8:ACAD:4::/64 serial 0/0 fe80::2
```


Je kan details van de IPv6-routetabel opvragen met onderstaand commando.

```
Router# show ipv6 route static
```

▪ Configureren van IPv6 default routes

Toevoegen van een IPv6 standaardroute.

```
Router(config)# ipv6 route ::/0 { ipv6-address | exit-intf }
```

Voor RouterB en RouterC kunnen alle toegevoegde statische routes vervangen worden door een default route (quad zero) aangezien het hier gaat op doodlopende netwerken (stub network).

```
RouterB(config)#ipv6 route ::/0 2001:DB8:ACAD:4::2
```

```
RouterC(config)#ipv6 route ::/0 2001:DB8:ACAD:5::1
```

15.3. Configure Floating Static Routes

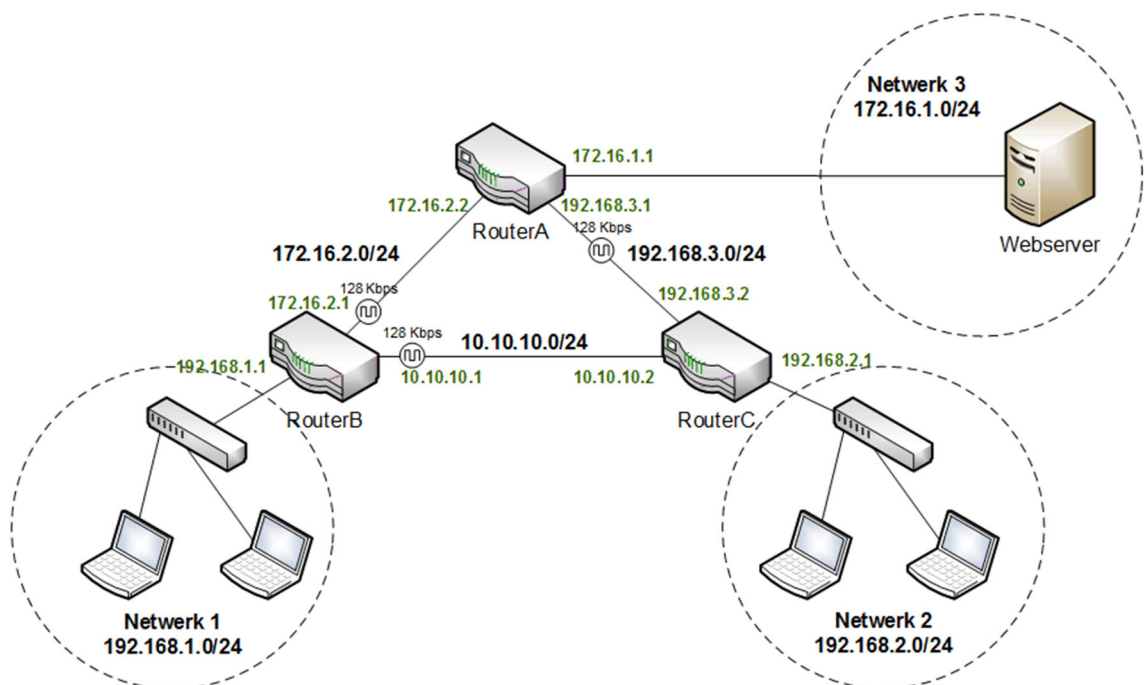
▪ Configureren van IPv4 floating static en default routes

Een vlottende route voeg je toe door een administratieve afstand toe te voegen. Als je dat niet vermeldt, dan geldt automatisch administratieve afstand 1 voor statische routes. In het voorbeeldnetwerk is nu een verbinding toegevoegd tussen router B en C. Deze kan als alternatieve route naar netwerk 3 toegevoegd worden.

```
RouterB(config)# ip route 172.16.1.0 255.255.255.0 10.10.10.2 5
```

Dit kan natuurlijk ook voor de standaardroute.

```
RouterB(config)# ip route 0.0.0.0 0.0.0.0 10.10.10.2 5
```



Figuur 7: Voorbeeldnetwerk uitgebreid met floating static routes

▪ Configureren van IPv6 floating static en default routes

Een vlottende IPv6 route werkt op soortgelijke manier als met IPv4. Veronderstel dat de toegevoegde route tussen router B en C als het 2001:DB8:ACAD:6::/64 netwerk is.

```
RouterB(config)# ipv6 route 2001:DB8:ACAD:2::/64 2001:DB8:ACAD:6::2 5
```

Dit kan natuurlijk ook voor de standaardroute.

```
RouterB(config)# ipv6 route ::/0 2001:DB8:ACAD:6::2 5
```

❖ Troubleshooting van IPv4 default routes

▪ Traceroute

Testen van routes kan met het traceroute commando

```
RouterB(config)#traceroute 172.16.1.1
```

Testen van routes kan ook vanaf een client met het traceroute commando (tracert in Windows).

```
C:\>tracert www.hotmail.com
```

Bezig met het traceren van de route naar www.hotmail.aate.nsatc.net
[166.63.208.158] via maximaal 30 hops:

1	<1 ms	<1 ms	<1 ms	192.168.1.4	
2	35 ms	19 ms	19 ms	dd5769801.access.telenet.be	[213.119.157.1]
3	19 ms	5 ms	6 ms	dd5E0FC02.access.telenet.be	[213.224.252.2]
4	12 ms	5 ms	6 ms	dd5E0FD3D.access.telenet.be	[213.224.253.61]
5	118 ms	9 ms	6 ms	dd5E0FD09.access.telenet.be	[213.224.253.9]
6	18 ms	14 ms	5 ms	dd5E0FD05.access.telenet.be	[213.224.253.5]
7	27 ms	13 ms	8 ms	dd5E0FD01.access.telenet.be	[213.224.253.1]
8	79 ms	14 ms	12 ms	dd5E0FD2D.access.telenet.be	[213.224.253.45]
9	55 ms	9 ms	7 ms	dd5E0FD66.access.telenet.be	[213.224.253.102]
10	20 ms	12 ms	13 ms	so-6-0-0-dcr2.amd.cw.net	[195.2.2.73]
11	27 ms	20 ms	19 ms	so-4-0-0-dcr1.tsd.cw.net	[195.2.10.146]
12	23 ms	20 ms	20 ms	so-4-0-0-bcr3.tsd.cw.net	[195.2.10.97]
13	29 ms	18 ms	21 ms	195.2.2.253	
14	28 ms	21 ms	22 ms	166.63.208.158	

De trace is voltooid.

▪ Extended ping

Als je van een router pingt ken je wel de destination, maar je weet eigenlijk niet van welke interface het vertrekt. Dit kan je bepalen door het bronadres toe te voegen.

```
RouterB(config)#ping 192.168.2.1 source 192.168.1.1
```

Dit kan ook door de broninterface toe te voegen.

```
RouterB(config)#ping 192.168.2.1 source g0/0
```

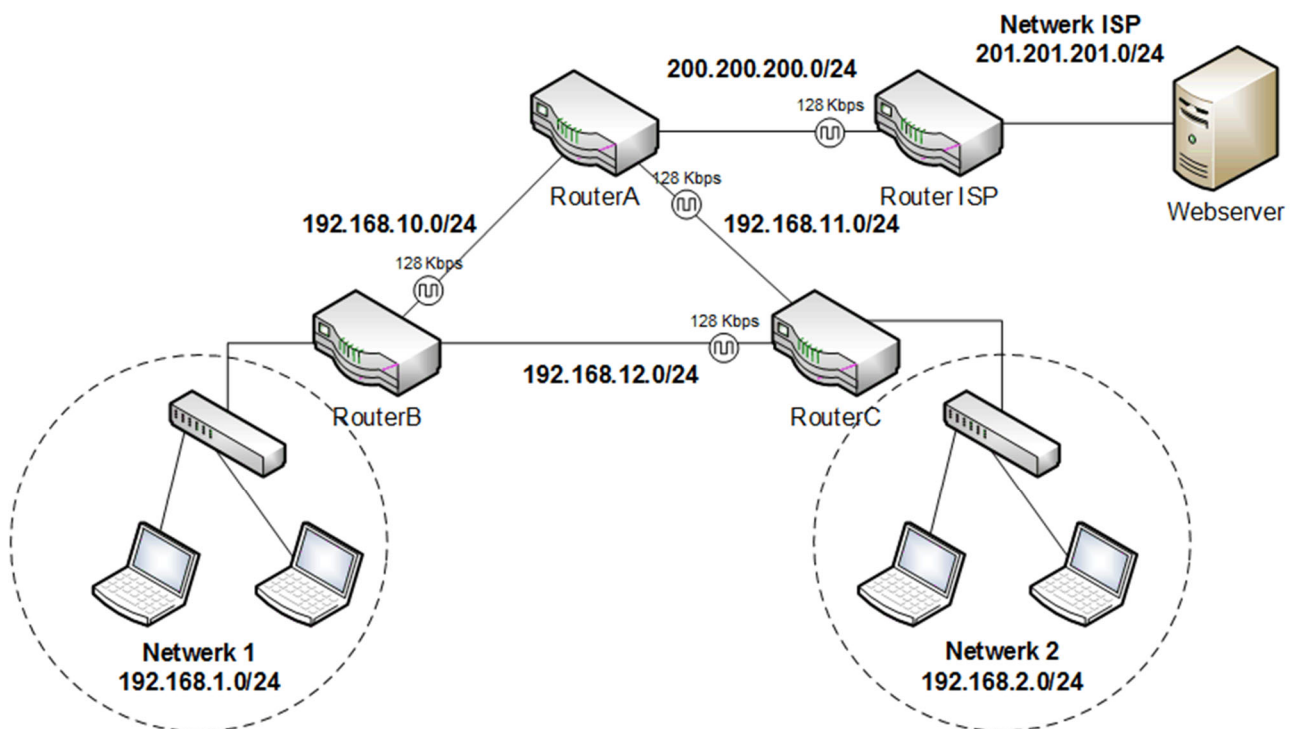
❖ Case study: Statische routes

Om de werking van statische routes te verduidelijken wordt de configuratie van een testopstelling uitgewerkt. Het testnetwerk bestaat uit drie routers die met redundante seriële lijnen met elkaar verbonden zijn. De snelheid is telkens 128000 Kbps en de DCE-kant is telkens aangesloten op de seriële poort S0/0. Seriële poort S0/1 is de DTE-kant en neemt de klok over van de DCE-kant.

Dit netwerk is verbonden met de router van de ISP. Daarachter zit het internet, waarvan netwerk 201.201.201.0/24 weergegeven is.

In het LAN zijn twee klassevolle netwerken aangesloten aan een fastethernetpoort 0/0.

Apparaat	Poort	IP-adres	Subnetmasker	Standaardrouter
Pc in netwerk 1	fa 0/0	192.168.1.2	255.255.255.0	192.168.1.1
Pc in netwerk 2	fa 0/0	192.168.2.2	255.255.255.0	192.168.2.1
Router A	S 0/0	192.168.11.1	255.255.255.0	nvt
	S 0/1	192.168.10.2	255.255.255.0	nvt
	S 0/2	200.200.200.2	255.255.255.0	nvt
Router B	S 0/0	192.168.10.1	255.255.255.0	nvt
	S 0/1	192.168.12.2	255.255.255.0	nvt
	fa 0/0	192.168.1.1	255.255.255.0	nvt
Router C	S 0/0	192.168.11.2	255.255.255.0	nvt
	S 0/1	192.168.12.1	255.255.255.0	nvt
	fa 0/0	192.168.2.1	255.255.255.0	nvt
Router ISP	S 0/0	200.200.200.1	255.255.255.0	nvt
	fa 0/0	201.201.201.1	255.255.255.0	nvt
Webserver	fa 0/0	201.201.201.254	255.255.255.0	201.201.201.1



Figuur 8: Case study voor statische routes (classfull)

Vooraleer je statische routes kan toevoegen moeten de routerinterfaces geconfigureerd worden, dit wordt hier geïllustreerd voor router B.

```
routerB#configure terminal
routerB(config)#interface Serial 0/0
routerB(config-if)#ip address 192.168.10.1 255.255.255.0
routerB(config-if)#clock rate 128000
routerB(config-if)#no shutdown
routerB(config-if)#exit
routerB(config)#interface Serial 0/1
routerB(config-if)#ip address 192.168.12.2 255.255.255.0
routerB(config-if)#no shutdown
routerB(config-if)#exit
routerB(config)#interface FastEthernet 0/0
routerB(config-if)#ip address 192.168.1.1 255.255.255.0
routerB(config-if)#no shutdown
routerB(config-if)#exit
```

Test de configuratie door de status van de interfaces op te vragen.

```
routerB#show ip interface brief.
```

Nadat alle poorten geconfigureerd zijn, kan je starten met het aanvullen van de routetabellen. Alle routers zijn reeds op de hoogte van hun lokale netwerken, hiervoor moet je niets doen. De voorlopige routetabel vraag je op met `show ip route`.

```
RouterB# show ip route
RouterB#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
...
Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.10.0/24 is directly connected, Serial0/0
C    192.168.12.0/24 is directly connected, Serial0/1
```

Het is dus kwestie om de netwerken toe te voegen die niet gekend zijn. Router B is nog niet op de hoogte van de LAN-netwerken 192.168.2.0/24 en 192.168.11.0/24. Die moet je toevoegen, evenals een standaardroute (quad-zero) naar de buitenwereld via router A.

```
RouterB(config)#ip route 192.168.2.0 255.255.255.0 192.168.12.1
RouterB(config)#ip route 192.168.11.0 255.255.255.0 192.168.12.1
RouterB(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.2
```

Dezelfde redenering trek je door voor routers A en C. Hier wordt puur ter illustratie gekozen om de "exit interface" op te geven in plaats van de "next hop". De configuratie met een exit interface is gemakkelijker maar ook foutgevoeliger aangezien de route uit de routetabel verwijderd wordt als die interface uit gaat.

```
RouterA(config)#ip route 192.168.1.0 255.255.255.0 Serial 0/1
RouterA(config)#ip route 192.168.2.0 255.255.255.0 Serial 0/0
RouterA(config)#ip route 192.168.12.0 255.255.255.0 Serial 0/0
RouterA(config)#ip route 0.0.0.0 0.0.0.0 Serial 0/2
```

```
RouterC(config)#ip route 192.168.1.0 255.255.255.0 Serial 0/0
RouterC(config)#ip route 192.168.10.0 255.255.255.0 Serial 0/0
RouterC(config)#ip route 0.0.0.0 0.0.0.0 Serial 0/1
```

De statische routes zijn terug te vinden bij het opvragen van de routetabel. De standaardroute is aangegeven met een asterisk.

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
...
Gateway of last resort is 192.168.10.2 to network 0.0.0.0

C    192.168.1.0/24 is directly connected, FastEthernet0/0
S    192.168.2.0/24 [1/0] via 192.168.12.1
C    192.168.10.0/24 is directly connected, Serial0/0
S    192.168.11.0/24 [1/0] via 192.168.12.1
C    192.168.12.0/24 is directly connected, Serial0/1
S*   0.0.0.0/0 [1/0] via 192.168.10.2
```

Als laatste wordt een statische route toegevoegd ter hoogte van de ISP-router.

```
RouterISP(config)#ip route 192.168.0.0 255.255.0.0 200.200.200.2
```

De gevolgde router kan vanaf een client getest worden met het tracert-commando, hier met de eerste computer uit netwerk 1.

```
PC>tracert 201.201.201.254

Tracing route to 201.201.201.254 over a maximum of 30 hops:

 1  62 ms     63 ms     62 ms     192.168.1.1
 2  94 ms     94 ms     78 ms     192.168.10.2
 3 109 ms    124 ms    124 ms    200.200.200.1
 4 156 ms    156 ms    156 ms    201.201.201.254

Trace complete.
```

Om redundantie in te bouwen kan je nu ook floating static routes toe voegen.

```
RouterB(config)#ip route 192.168.2.0 255.255.255.0 192.168.10.2 5
RouterB(config)#ip route 192.168.11.0 255.255.255.0 192.168.10.2 5
RouterB(config)#ip route 0.0.0.0 0.0.0.0 192.168.12.1 5
```

```
RouterA(config)#ip route 192.168.1.0 255.255.255.0 192.168.11.2 5
RouterA(config)#ip route 192.168.2.0 255.255.255.0 192.168.10.1 5
```

```
RouterC(config)#ip route 192.168.1.0 255.255.255.0 192.168.11.1 5
RouterB(config)#ip route 192.168.10.0 255.255.255.0 192.168.11.1 5
RouterB(config)#ip route 0.0.0.0 0.0.0.0 192.168.12.2 5
```

De werking van de vlottende statische routes kan getest worden door een interrouterverbinding te verwijderen en dan zou de connectie toch nog tot stand moeten komen.

Hoofdstuk 16: Troubleshoot Static and Default Routes

Hoofdstuk 17: Dynamic Routing - RIP

17.1. RIP v1: Routing Information Protocol versie 1

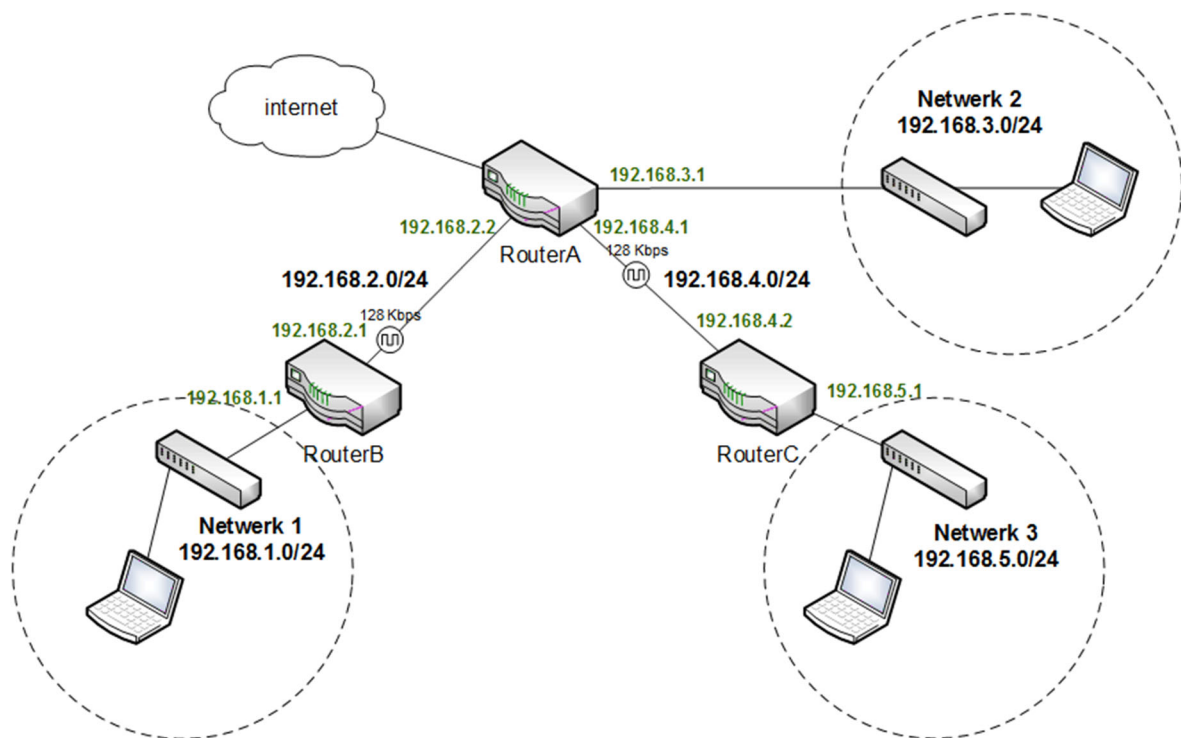
RIP versie 1 is een klassevol routeringsalgoritme. Er zijn enkele specifieke IOS-commando's om RIP te configureren.

Het aanzetten van RIP.

```
RouterB(config)# router rip
```

Standaard staat RIP op versie 1, maar indien nodig kan het terug op versie 1 gezet worden.

```
RouterB(config-router)# no version      (zet terug op de standaard, dus versie 1)
Of
RouterB(config-router)# version 1      (versie 1)
```



Figuur 9: Voorbeeldnetwerk voor dynamische routing

Na het aanzetten van RIP, geef je de netwerken in die via RIP moeten verstuurd worden.

```
RouterB(config-router)# network 192.168.1.0
RouterB(config-router)# network 192.168.2.0
```

Opvragen van meer informatie over het routingprotocol en de RIP-databank.

```
RouterB# show ip protocols
RouterB# show ip rip database
```

Extra informatie tonen voor RIP tijdens de configuratie en/of tijdens de werking.

```
RouterB# debug ip rip
```

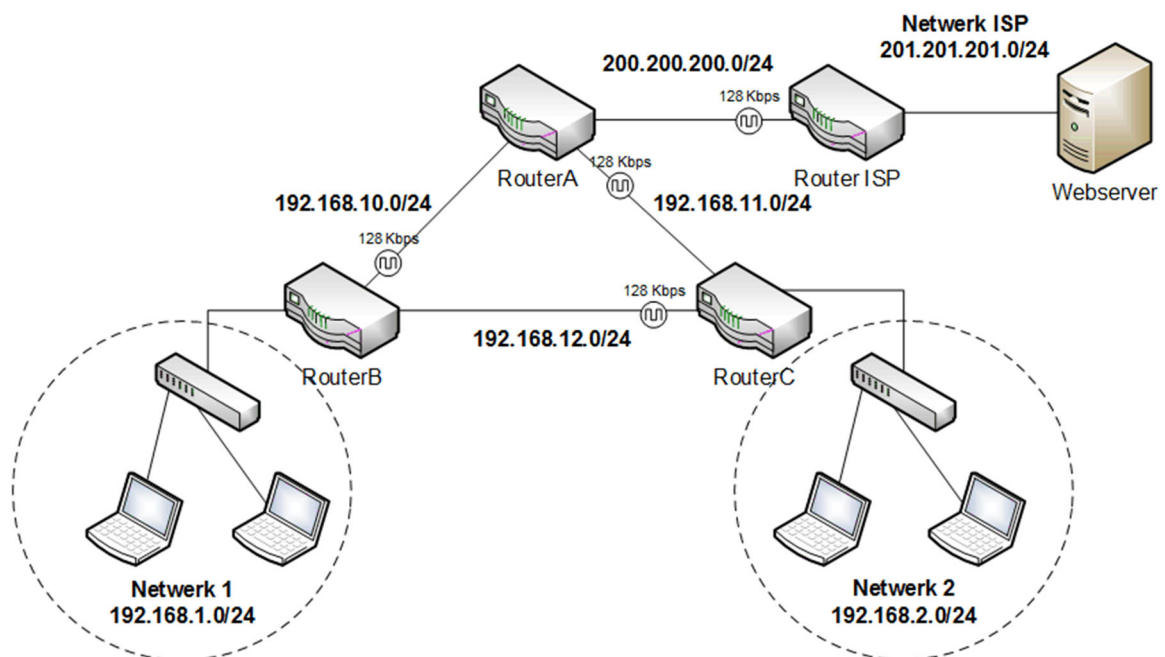
Het is onnodig en belastend voor het netwerk om RIP-pakketten te sturen naar netwerken waar geen routers meer luisteren, daarom kan je beter passieve interfaces definiëren die niet meedoen aan RIP.

```
RouterB(config-router)# passive-interface GigaEthernet 0/0
```

Ook bij RIP moet de standaardroute naar buiten door een quad-zero route bepaald. Dit doe je enkel op de router die met de buitenwereld verbonden is, daarna laat je de standaardroute met RIP verdelen. Laten we ervan uit gaan dat Router A ook in verbinding staat met de buitenwereld.

```
RouterA(config)# ip route 0.0.0.0 0.0.0.0 Serial 0/0
RouterA(config)# router rip
RouterA(config-router)# default-information originate
```

❖ Case study: RIP versie 1



Figuur 10: Case study RIP versie 1

Als testcase nemen we hier hetzelfde netwerk als dat van de testcase rond statische routes. De IP-configuratie is hetzelfde en wordt dus niet opnieuw herhaald.

Als opfrissing wordt hier van de routers A, B en C de interfaceconfiguratie getoond.

```
RouterA#show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
Serial0/0      192.168.11.1    YES manual up          up
Serial0/1      192.168.10.2    YES manual up          up
Serial0/2      200.200.200.2   YES manual up          up
```

```
RouterB#show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 192.168.1.1     YES manual up          up
Serial0/0      192.168.10.1    YES manual up          up
Serial0/1      192.168.12.2    YES manual up          up
```

```
RouterC#show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 192.168.2.1     YES manual up          up
Serial0/0      192.168.12.1    YES manual up          up
Serial0/1      192.168.11.2    YES manual up          up
```


In tegenstelling tot de configuratie van statische routes worden hier niet de ongekende netwerken, maar net de lokaal verbonden netwerken opgesomd bij de configuratie van RIP. Het zijn namelijk die gekende netwerken die naar routers gestuurd worden die deze netwerken moeten leren kennen. Om te voorkomen dat de RIP-advertisements verder gestuurd worden dan nodig worden op de drie routers passieve interfaces gezet.

```
RouterA(config)#router RIP
RouterA(config-router)#network 192.168.10.0
RouterA(config-router)#network 192.168.11.0
RouterA(config-router)# passive-interface serial 0/2
```

```
RouterB(config)#router RIP
RouterB(config-router)#network 192.168.10.0
RouterB(config-router)#network 192.168.12.0
RouterB(config-router)#network 192.168.1.0
RouterB(config-router)#passive-interface g0/0
```

```
RouterC(config)#router RIP
RouterC(config-router)#network 192.168.11.0
RouterC(config-router)#network 192.168.12.0
RouterC(config-router)#network 192.168.2.0
RouterC(config-router)#passive-interface g0/0
```

Ter hoogte van router A wordt de standaardroute naar buiten toegevoegd en bekend gemaakt aan de andere RIP-routers.

```
RouterA(config)#ip route 0.0.0.0 0.0.0.0 Serial 0/2
RouterA(config)# router rip
RouterA(config-router)# default-information originate
```

Dit laatste zal ervoor zorgen dat ook routers B en C de standaardroute overnemen. De routes die geleerd zijn met RIP zijn herkenbaar aan de "R" en de administratieve kost van 120.

```
RouterB#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
...
Gateway of last resort is 192.168.10.2 to network 0.0.0.0

C    192.168.1.0/24 is directly connected, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 192.168.12.1, 00:00:14, Serial0/1
C    192.168.10.0/24 is directly connected, Serial0/0
R    192.168.11.0/24 [120/1] via 192.168.10.2, 00:00:06, Serial0/0
      [120/1] via 192.168.12.1, 00:00:14, Serial0/1
C    192.168.12.0/24 is directly connected, Serial0/1
R*   0.0.0.0/0 [120/1] via 192.168.10.2, 00:00:06, Serial0/0
```

Het netwerk 192.168.11.0 heeft een gelijke kost voor de route over router A of over router B. Beide routes worden opgenomen en er zal "equal cost load balancing" plaatshebben. De pakketten worden dus altemnerend over beide routes gestuurd.

Bij foutzoeken moeten het eerst de routetabellen onderzocht worden. Is dit onvoldoende dan kan je meer informatie opvragen over de RIP-database.

```
RouterB#show ip rip database
0.0.0.0/0    auto-summary
0.0.0.0/0
    [1] via 192.168.10.2, 00:00:15, Serial0/0
192.168.1.0/24    auto-summary
192.168.1.0/24    directly connected, FastEthernet0/0
192.168.2.0/24    auto-summary
192.168.2.0/24
    [1] via 192.168.12.1, 00:00:13, Serial0/1
```

```

192.168.10.0/24    auto-summary
192.168.10.0/24    directly connected, Serial0/0
192.168.11.0/24    auto-summary
192.168.11.0/24    [1] via 192.168.10.2, 00:00:15, Serial0/0    [1] via 192.168.12.1, 00:00:13,
Serial0/1
192.168.12.0/24    auto-summary
192.168.12.0/24    directly connected, Serial0/1

```

Of je kan details opvragen over het RIP-protocol.

```

RouterA#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 19 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface          Send  Recv  Triggered RIP  Key-chain
Serial0/1             1     2  1
Serial0/0             1     2  1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  192.168.10.0
  192.168.11.0
Passive Interface(s):
  Serial0/2
Routing Information Sources:
  Gateway         Distance      Last Update
  192.168.10.1         120          00:00:00
  192.168.11.2         120          00:00:07
Distance: (default is 120)

```

Zeer krachtig is het aanzetten van de debugging van het RIP-protocol.

```

RouterB#debug ip rip
RIP protocol debugging is on
RouterB#RIP: received v1 update from 192.168.10.2 on Serial0/0
  0.0.0.0 in 1 hops
  192.168.2.0 in 2 hops
  192.168.11.0 in 1 hops
RIP: sending v1 update to 255.255.255.255 via Serial0/0 (192.168.10.1)
RIP: build update entries
  network 192.168.1.0 metric 1
  network 192.168.2.0 metric 2
  network 192.168.12.0 metric 1
RIP: sending v1 update to 255.255.255.255 via Serial0/1 (192.168.12.2)
RIP: build update entries
  network 0.0.0.0 metric 2
  network 192.168.1.0 metric 1
  network 192.168.10.0 metric 1
no debug all
All possible debugging has been turned off
RouterB#

```

17.2. RIP v2: Routing Information Protocol versie 2

In tegenstelling tot versie 1, is RIP v2 een classless routing protocol. Bij het uitwisselen van routes wordt dus ook een subnetmasker meegegeven.

Het aanzetten van RIP v2.

```

Router(config)# router rip
Router(config-router)# version 2

```

Je dient te voorkomen dat er automatische sommatie van routes is. Dit is belangrijk voor discontiguous netwerken.

```
Router(config-router)# no auto-summary
```

Je kan ook de ingegeven statische routes laten uitwisselen tussen de routers

```
Router(config)# ip route 192.0.2.0 255.255.255.0 Serial 0/1
Router(config)# router rip
Router(config-router)# redistribute static
```

Je moet erop letten dat **ip classless** aan staat (dit is de standaardinstelling vanaf IOS 11.3), anders wordt de standaardroute niet aangesproken.

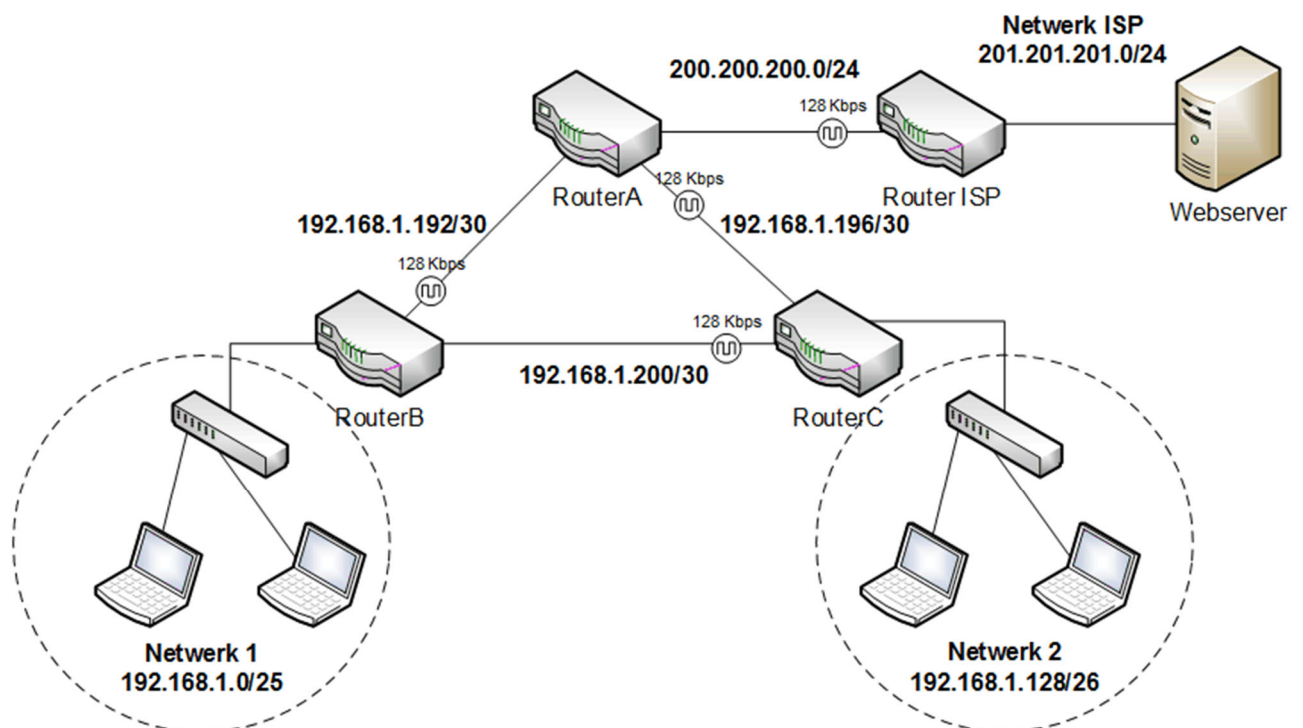
```
Router# show running-config
...
ip classless
...
```

Je kan dit terugzetten naar de vroegere standaard, maar dit is meestal niet gewenst.

```
Router(config)# no ip classless
```

❖ Case study: RIPv2

Aangezien RIPv2 een classless routingprotocol is wordt de testomgeving omgezet naar een LAN-netwerk waar gebruik gemaakt wordt van VLSM. Network 1 moet voorzien zijn voor 100 hosts, network 2 voor 50 hosts. Tussen de routers wordt telkens gekozen voor een /30-prefix.



Figuur 11: Case study voor RIPv2

Dit geeft een heel nieuw adresschema.

Apparaat	Poort	IP-adres	Subnetmasker	Standaardrouter
Pc in netwerk 1	fa 0/0	192.168.1.2	255.255.255.128	192.168.1.1
Pc in netwerk 2	fa 0/0	192.168.1.130	255.255.255.192	192.168.1.129
Router A	S 0/0	192.168.1.197	255.255.255.252	nvt
	S 0/1	192.168.1.194	255.255.255.252	nvt
	S 0/2	200.200.200.2	255.255.255.252	nvt
Router B	S 0/0	192.168.1.193	255.255.255.252	nvt
	S 0/1	192.168.1.202	255.255.255.252	nvt
	Gi 0/0	192.168.1.1	255.255.255.128	nvt
Router C	S 0/0	192.168.1.201	255.255.255.252	nvt
	S 0/1	192.168.1.198	255.255.255.252	nvt
	Gi 0/0	192.168.1.129	255.255.255.192	nvt
Router ISP	S 0/0	200.200.200.1	255.255.255.252	nvt
	Gi 0/0	201.201.201.1	255.255.255.0	nvt
Webserver	fa 0/0	201.201.201.254	255.255.255.0	201.201.201.1

Vooraleer je RIP kan starten moeten alle interfaces voorzien worden van de juiste IP-configuratie, dit wordt ook nu weer geïllustreerd voor router B.

```

routerB#configure terminal
routerB(config)#interface Serial 0/0
routerB(config-if)#ip address 192.168.1.193 255.255.255.252
routerB(config-if)#clock rate 128000
routerB(config-if)#no shutdown
routerB(config-if)#exit
routerB(config)#interface Serial 0/1
routerB(config-if)#ip address 192.168.1.202 255.255.255.252
routerB(config-if)#no shutdown
routerB(config-if)#exit
routerB(config)#interface GigaEthernet 0/0
routerB(config-if)#ip address 192.168.1.1 255.255.255.128
routerB(config-if)#no shutdown
routerB(config-if)#exit

```

Op de drie LAN-routers moet nu de configuratie van RIPv2 gebeuren en die is overal identiek. In dit geval is het voldoende om overal het netwerk 192.168.1.0 bekend te maken. Gezien het IP-adres met 192 begint, koppelt de router hier dadelijk een prefix /24 aan. Hij zal dan alle netwerken die hieronder vallen, samen met ingestelde subnetmasker van de poort waarachter het netwerk ligt, adverteren naar de andere routers. Ondanks dat RIPv2 een klasseloos protocol is, is het toch de bedoeling om klasvolle netwerken op te nemen in het commando.

```

Router(config)#router RIP
Router(config-router)#version 2
Router(config-router)#no auto-summary
Router(config-router)#network 192.168.1.0
Router(config-router)#passive-interface g0/0

```

Deze werking wordt duidelijk door debugging aan te zetten.

```

RouterB#debug ip rip
RIP protocol debugging is on
RouterB#RIP: received v2 update from 192.168.1.201 on Serial0/1
    192.168.1.128/26 via 0.0.0.0 in 1 hops
    192.168.1.196/30 via 0.0.0.0 in 1 hops
RIP: received v2 update from 192.168.1.194 on Serial0/0
    192.168.1.128/26 via 0.0.0.0 in 2 hops
    192.168.1.196/30 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via Serial0/0 (192.168.1.193)

```

```
RIP: build update entries
    192.168.1.0/25 via 0.0.0.0, metric 1, tag 0
    192.168.1.128/26 via 0.0.0.0, metric 2, tag 0
    192.168.1.200/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/1 (192.168.1.202)
RIP: build update entries
    192.168.1.0/25 via 0.0.0.0, metric 1, tag 0
    192.168.1.192/30 via 0.0.0.0, metric 1, tag 0
no debug ip rip
RIP protocol debugging is off
```

Je ziet dat router B dus toch twee 192.168.1.x netwerken ontvangt van router A, evenals van router C. Zelf stuurt router B drie netwerken naar router A en twee netwerken naar router C. Het subnet waarover de RIP-update gestuurd wordt, wordt niet in de RIP-advertentie opgenomen.

Het mag verwarrend lijken om enkel klasvolle netwerkadressen te gebruiken bij een klasseloos protocol, en dat is het vaak ook. Gelukkig is het niet fout om toch alle klasseloze netwerken op te nemen. De router zal er automatisch een klassevol adres van maken.

Dus onderstaande code werkt ook, klinkt logischer, maar is eigenlijk technisch minder correct.

```
RouterB(config)#router RIP
RouterB(config-router)#version 2
RouterB(config-router)#no auto-summary
RouterB(config-router)#network 192.168.1.0
RouterB(config-router)#network 192.168.1.192
RouterB(config-router)#network 192.168.1.200
```

In dit voorbeeld is het niet noodzakelijk om auto-summary af te zetten gezien de verschillende subnetten niet gescheiden worden door een volledig andere IP-range, maar het kan ook geen kwaad. Moest er tussen netwerk 1 en 2 bijvoorbeeld het netwerk 172.16.0.0/16 gebruikt worden, dan was dit wel nodig omdat router A de twee netwerken anders automatisch sommeert tot 192.168.1.0/24 en dan dus een gelijke kost heeft over de twee seriële lijnen. Er gebeurt dus equal cost load balancing, waardoor opeenvolgende pakketten telkens een alternerende route gaan volgen. Zonder de redundante verbinding tussen router B en C gaan dan pakketten verloren.

Net als bij RIPv1 moet ter hoogte van router A de standaardroute toegevoegd worden en verdeeld worden naar de andere RIP-routers. Het definiëren van passieve interfaces verschilt eveneens niet van RIPv1.

```
RouterA(config)#ip route 0.0.0.0 0.0.0.0 Serial 0/2
RouterA(config)# router rip
RouterA(config-router)# default-information originate
```

Hoofdstuk 18: Dynamic Routing - OSPF

18.1. Router-id

❖ Configure router-id

Bij het aanzetten van OSPF moet een proces-id meegegeven worden. In het onderstaand voorbeeld wordt "1" meegegeven. De proces-id moet een getal zijn tussen 1 en 65536, dit mag voor de verschillende routers hetzelfde getal zijn, maar dat hoeft niet.

```
Router(config)# router ospf 1
```

Binnen het OSPF-proces wordt elke router uniek geïdentificeerd, hiervoor zijn meerder mogelijkheden.

In de recente IOS-versies kan je rechtstreeks een router-id meegeven, deze methode geniet de voorkeur. Een router-id wint van een loopbackadres dat weer wint van het hoogste ip-adres van de interfaces.

Het ingestelde router-id heeft de vorm van een IP-adres, maar komt niet voor in de routetabellen.

```
Router1(config-router)# router-id 1.1.1.1  
Router2(config-router)# router-id 2.2.2.2
```

Bij oudere IOS-versies zonder het router-id commando kunnen loopbackadressen (virtuele interfaces) geconfigureerd worden om ervoor te zorgen dat elke router een vast router-id heeft. Een loopback staat immers altijd "up".

```
Router1(config)# interface loopback 0  
Router1(config-if)# ip address 1.1.1.1 255.255.255.255  
  
Router2(config)# interface loopback 0  
Router2(config-if)# ip address 1.1.1.1 255.255.255.255
```

Als je die identificatie niet specifiek definieert, dan neemt de router hiervoor het hoogste aanwezige actieve ip-adres van zijn interfaces. Als dit hoogste adres "down" gaat, dan verandert ook de router-id.

Als je problemen ondervindt met router-id's, dan kan je het ospf-process resetten met het volgend commando.

```
Router#clear ip ospf proces
```

18.2. Point-to-Point OSPF Networks

❖ Network command and wildcard mask

Bij het toevoegen van netwerken, dient de volgende syntax gevolgd te worden

“network network-address wildcard-mask area area-id”

```
Router(config)# router ospf 10
Router(config-router)# network 192.168.1.0 0.0.0.255 area 0
Router(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

Het wildcard-mask is de inversie van het werkelijk subnetmasker.

Dus 255.255.255.0 wordt 0.0.0.255, 255.255.255.240 wordt 0.0.0.15, enzovoort.

De area-id moet hetzelfde zijn voor alle routers die onderling met ospf-informatie uitwisselen, dit hoofdstuk handelt immers over single-area OSPF.

❖ Alternative: network command and quad-zero wildcard mask

Naast de bovenstaande methode, kan ook de volgende syntax gevolgd te worden

“network interface-address 0.0.0.0 area area-id”

```
Router(config)# router ospf 10
Router(config-router)# network 192.168.1.1 0.0.0.0 area 0
Router(config-router)# network 192.168.2.1 0.0.0.0 area 0
```

Bovenstaande commando's zorgen ervoor dat het OSPF-proces aangezet wordt op de interfaces.

❖ Alternative: ip ospf command

OSPF kan ook rechtstreeks aangezet worden via de interface, hiervoor gebruik je het “ip ospf” commando.

```
Router(config)# no router ospf 10
Router(config-router)# no network 192.168.1.1 0.0.0.0 area 0
Router(config-router)# no network 192.168.2.1 0.0.0.0 area 0
Router(config-router)# exit
Router(config)# interface GigabitEthernet 0/0
Router(config-if)# ip ospf 10 area 0
Router(config-if)# interface GigabitEthernet 0/1
Router(config-if)# ip ospf 10 area 0
```

Let wel op met het “ip ospf” commando op interface niveau, aangezien dit samen kan werken met de configuratie via “network” commando op router niveau. Best kan wel op het router niveau toch een router-id meegegeven worden.

❖ Passive interface

Net als bij andere routingprotocollen kan je passieve interfaces definiëren die niet meedoen aan OSPF.

```
Router(config)# router ospf 10
Router(config-router)# passive-interface GigabitEthernet 0/0
```

❖ Point-To-Point networks

Eerst een korte herhaling voor het instellen van seriële poorten. Je kan de bandbreedte van interfaces instellen (eenheid is kbps) om zo een verschil te maken tussen trage en snelle routes.

```
Router(config)# interface serial 0/0
Router(config-if)# bandwidth 64
```

Eens OSPF ingesteld is kan je de paramaters van een interface opvragen.

```
Router# show ip ospf interface serial S0/0/0
```

Bij een Point-to-Point verbinding wordt dit aangegeven.

Om een aanwezig netwerk te simuleren via een loopbackadres kan je dit als point-to-point configureren.

```
Router(config)# interface loopback 0
Router(config-if)# ip address 10.10.1.1 255.255.255.0
Router(config-if)# ip ospf network point-to-point
```

In geval van bovenstaand voorbeeld wordt dan het volledige 10.10.1.0/24 als netwerk opgenomen.

18.3. Multi-access OSPF Networks

❖ OSPF in Multiaccess Networks

Controleer de rol van de Router (DR, BDR, DROther).

```
Router# show ip ospf interface G0/0
```

Controleer de rol van de buurouters (DR, BDR, DROther).

```
Router# show ip ospf neighbor
```

Als je niet enkel wil afhangen van het router-id bij de verkiezing van de DR en BDR, kan je de DR-verkiezing sturen door een prioriteit met een waarde tussen 1-255 toe te kennen. De waarde 0 geeft aan dat het geen DR of BDR kan worden, 255 geeft de hoogste prioriteit.

```
Router(config)# interface G0/0
Router(config-if)# ip ospf priority 255
```

Als je problemen ondervindt met router-id's of prioriteiten, dan dien je het ospf-proces te resetten.

```
Router#clear ip ospf process
```

18.4. Modify Single-Area OSPFv2

❖ Reference bandwidth

OSPF werkt met een kost per verbinding. Om deze kost te berekenen wordt 10^8 bit gedeeld door de actuele bandbreedte. In bovenstaand voorbeeld is de kost van de 64 kbit seriële verbinding dus $10^8/64000 = 1562$. De kost voor een 100 Mbit verbinding is $10^8/10^8 = 1$.

In plaats van de bandbreedte kan je ook rechtstreeks de cost meegeven.

```
Router(config)# interface serial 0/0
Router(config-if)# no bandwidth 64
Router(config-if)# ip ospf cost 1562
```

De kost van een 10 Mbit verbinding is dus 10 en die van een 100 Mbit verbinding is 1. Aangezien 1 de minimale waarde is, is er geen verschil meer met nog snellere verbindingen (1 Gbit of 10 Gbit).

In geval van snellere verbindingen kan daarom best volgend commando gebruikt worden.

```
Router(config-router)# auto-cost reference-bandwidth 10000
```

Dit commando verandert de referentiebandbreedte van 10^8 naar 10^{10} . Met deze instelling krijgt een 10 Gbit verbinding de waarde 1 en een 100 Mbit verbinding te waarde 100. Het is vanzelfsprekend nodig dit op alle routers te doen.

Je kan terug gaan naar de standaardinstelling met het commando:

```
Router(config-router)# auto-cost reference-bandwidth 100
```

De ingestelde bandbreedte opvragen:

```
Router# show interfaces serial 0/0/0
```

De cost van een verbinding kan je opvragen met:

```
Router# show ip ospf interface serial 0/0/0
```


❖ Manually Set OSPF Cost

Naast automatisch de cost te laten berekenen op basis van het kabeltype kan je de cost ook configureren.

```
Router(config)# interface Serial 0/0/0
Router(config-if)# ip ospf cost 30
```

❖ Hello Packets interval

OSPFv2 Hello en Dead interval aanpassen.

```
Router(config)# interface Serial 0/0/0
Router(config-if)# ip ospf hello-interval 5
Router(config-if)# ip ospf dead-interval 20
```

OSPFv3 Hello en Dead interval aanpassen.

```
Router(config)# interface Serial 0/0/0
Router(config-if)# ipv6 ospf hello-interval 5
Router(config-if)# ipv6 ospf dead-interval 20
```

18.5. Default Route Propagation

De standaardroute verdelen naar de andere ospf-routers.

```
RouterA(config)# ip route 0.0.0.0 0.0.0.0 Serial 0/1/0
RouterA(config)# router ospf 10
RouterA(config-router)# default-information originate
```

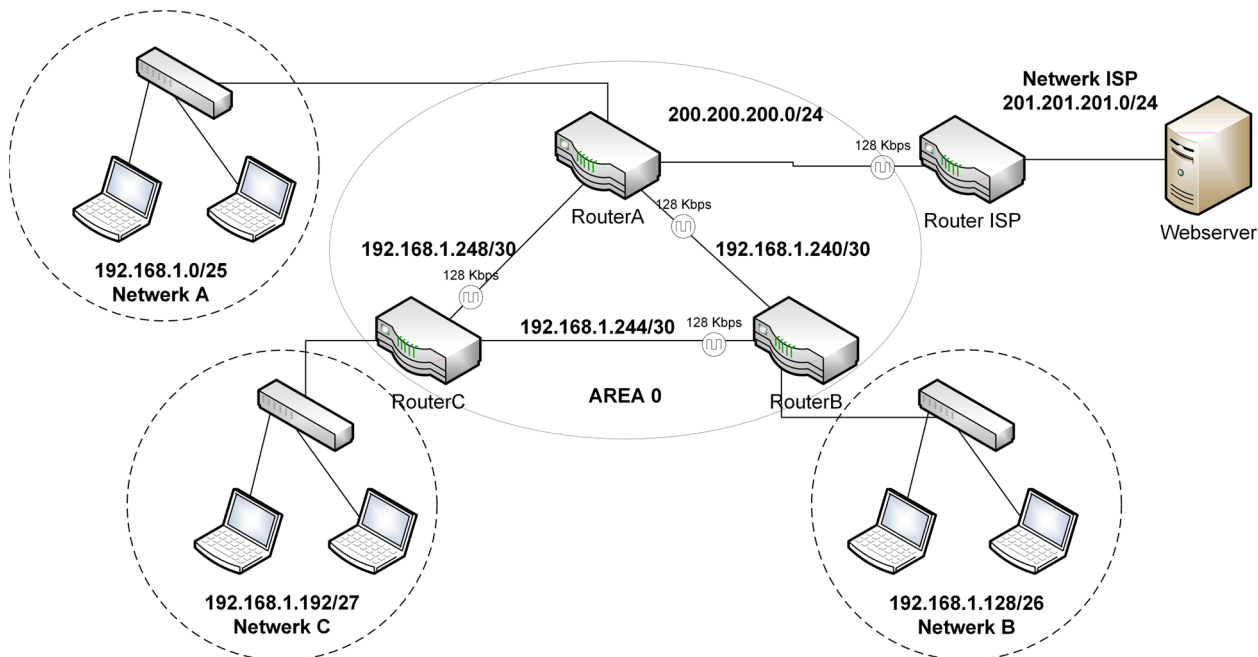
18.6. Verifying OSPF

Enkele verdere nuttige ospf-commando's.

```
Router# show ip route
Router# show ip protocols
Router# show ip ospf neighbor
Router# show ip ospf interface ...
```

❖ Case study 1: OSPFv2

Case study met onderstaand OSPF-netwerk



Figuur 12: Case study voor Open Shortest Path First

Dit geeft het adresschema.

Apparaat	Poort	IP-adres	Subnetmasker	Standaardrouter
Pc A in netwerk A	fa 0/0	192.168.1.2	255.255.255.128	192.168.1.1
Pc B in netwerk B	fa 0/0	192.168.1.130	255.255.255.192	192.168.1.129
Pc C in netwerk C	fa 0/0	192.168.1.194	255.255.255.224	192.168.1.193
Router A	Gi 0/0	192.168.1.1	255.255.255.128	nvt
	S 0/0/0	192.168.1.241	255.255.255.252	nvt
	S 0/0/1	192.168.1.250	255.255.255.252	nvt
	S 0/1/0	200.200.200.2	255.255.255.252	nvt
Router B	Gi 0/0	192.168.1.129	255.255.255.192	nvt
	S 0/0/0	192.168.1.245	255.255.255.252	nvt
	S 0/0/1	192.168.1.242	255.255.255.252	nvt
Router C	Gi 0/0	192.168.1.193	255.255.255.224	nvt
	S 0/0/0	192.168.1.249	255.255.255.252	nvt
	S 0/0/1	192.168.1.246	255.255.255.252	nvt
Router ISP	S 0/0/0	200.200.200.1	255.255.255.252	nvt
	Gi 0/0	201.201.201.1	255.255.255.0	nvt
Webserver	fa 0/0	201.201.201.254	255.255.255.0	201.201.201.1

Op de drie LAN-routers moet nu de configuratie van OSPF gebeuren. Vooraleer de netwerken toe te voegen krijgt elke router ook een router-id.

```
RouterA(config)# router ospf 1
RouterA(config-router)# router-id 10.0.0.1
RouterA(config-router)# network 192.168.1.0 0.0.0.127 area 0
RouterA(config-router)# network 192.168.1.240 0.0.0.3 area 0
RouterA(config-router)# network 192.168.1.248 0.0.0.3 area 0
```

```
RouterB(config)# router ospf 1
RouterB(config-router)# router-id 10.0.0.2
```

```
RouterB(config-router)# network 192.168.1.128 0.0.0.63 area 0
RouterB(config-router)# network 192.168.1.240 0.0.0.3 area 0
RouterB(config-router)# network 192.168.1.244 0.0.0.3 area 0
```

```
RouterC(config)# router ospf 1
RouterC(config-router)# router-id 10.0.0.3
RouterC(config-router)# network 192.168.1.192 0.0.0.31 area 0
RouterC(config-router)# network 192.168.1.244 0.0.0.3 area 0
RouterC(config-router)# network 192.168.1.248 0.0.0.3 area 0
```

In analogie met RIP zal router A de standaardroute verdelen naar de andere ospf-routers.

```
RouterA(config)# ip route 0.0.0.0 0.0.0.0 Serial 0/1/0
RouterA(config)# router ospf 1
RouterA(config-router)# default-information originate
```

De werking kan gecontroleerd worden door debugging aan te zetten.

```
RouterB# debug ip ospf events
OSPF events debugging is on
RouterB#
00:07:39: OSPF: Rcv hello from 10.0.0.3 area 0 from Serial0/0/0 192.168.1.246
00:07:39: OSPF: End of hello processing
00:07:40: OSPF: Rcv hello from 10.0.0.1 area 0 from Serial0/0/1 192.168.1.241
00:07:40: OSPF: End of hello processing
```

Gedetailleerde informatie over het gebruikte routingprotocol opvragen geeft eveneens inzicht in de werking, net zoals het opvragen van de buren of de ospf-databank.

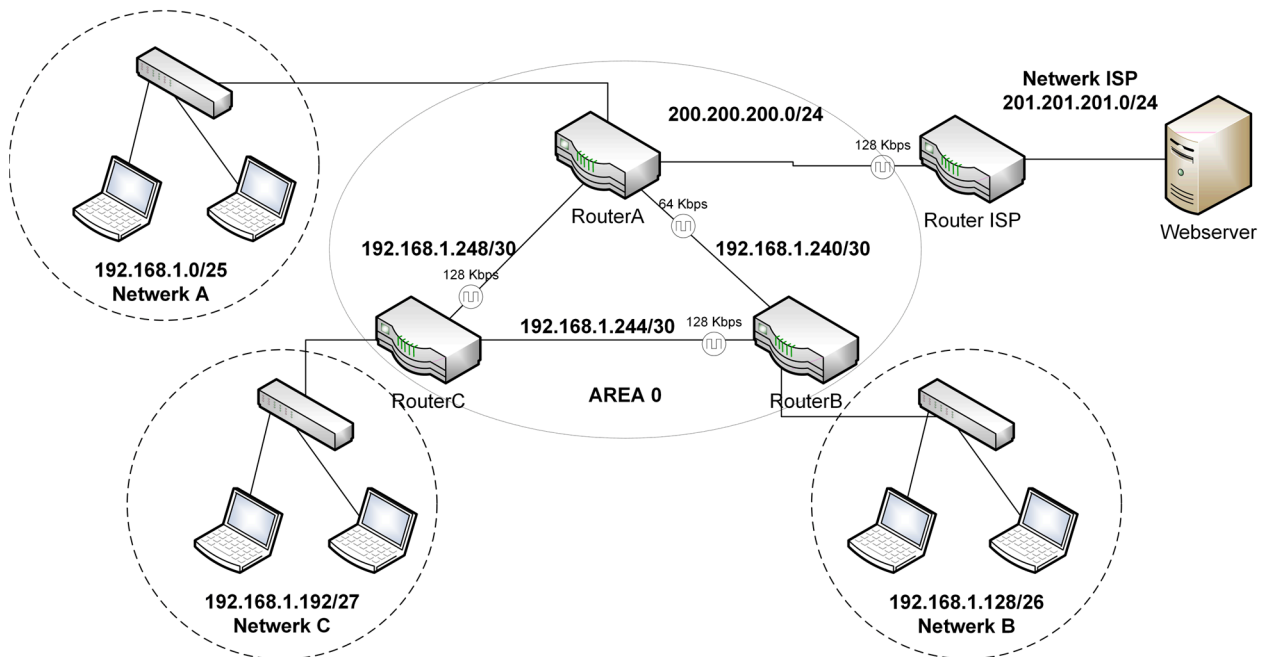
```
RouterB# show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.0.0.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.128 0.0.0.63 area 0
    192.168.1.240 0.0.0.3 area 0
    192.168.1.244 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.0.0.1         110          00:02:38
    10.0.0.2         110          00:03:56
    10.0.0.3         110          00:03:39
  Distance: (default is 110)
```

```
RouterB# show ip ospf database
      OSPF Router with ID (10.0.0.2) (Process ID 1)
      Router Link States (Area 0)
Link ID      ADV Router   Age         Seq#         Checksum Link count
10.0.0.2     10.0.0.2     300         0x80000005  0x00aed6  5
10.0.0.3     10.0.0.3     283         0x80000005  0x00dbd7  5
10.0.0.1     10.0.0.1     222         0x80000006  0x001a22  5
      Type-5 AS External Link States
Link ID      ADV Router   Age         Seq#         Checksum Tag
0.0.0.0     10.0.0.1     222         0x80000001  0x00bc0b  1
RouterB#
```

```
RouterB# show ip ospf 1 neighbor
Neighbor ID  Pri  State           Dead Time   Address        Interface
10.0.0.3     0   FULL/-         00:00:30   192.168.1.246 Serial0/0/0
10.0.0.1     0   FULL/-         00:00:31   192.168.1.241 Serial0/0/1
```

❖ Case study 2: Tuning OSPFv2

In deze testcase wordt hetzelfde VLSM-netwerk gebruikt als voorgesteld in de eerste OSPF-testcase, maar nu is verbinding tussen RouterA en RouterB vervangen door een 64 kbps seriële lijn in plaats van 128 kbps.



Figuur 13: Case study voor Open Shortest Path First

Een packet van een pc in netwerk B naar A zal altijd over de 64 kbps seriële lijn gaan.

```
C:\>tracert 192.168.1.2
Tracing route to 192.168.1.2 over a maximum of 30 hops:
 1  0 ms      0 ms      0 ms      192.168.1.129
 2  1 ms      0 ms      1 ms      192.168.1.241
 3  *          1 ms      0 ms      192.168.1.2
```

Deze 64 kbps lijn is echter bedoeld als back-up en is trager. Het is dus de bedoeling dat de route B-C-A gevolgd wordt aangezien dit 128 kbps-lijnen zijn. Het instellen van de clock rate speelt hierin geen rol, het is nodig de bandbreedte op te geven.

```
RouterA(config)# interface Serial0/0/0
RouterA(config-if)# clock rate 64000
RouterA(config-if)# bandwidth 64
RouterA(config-if)# exit
RouterA(config)# interface Serial 0/0/1
RouterA(config-if)# bandwidth 128
RouterA(config-if)# exit
```

```
RouterB(config)# interface Serial0/0/0
RouterB(config-if)# clock rate 128000
RouterB(config-if)# bandwidth 128
RouterB(config-if)# exit
RouterB(config)# interface Serial 0/0/1
RouterB(config-if)# bandwidth 64
RouterB(config-if)# exit
```

```
RouterC(config)# interface Serial0/0/0
RouterC(config-if)# clock rate 128000
RouterC(config-if)# bandwidth 128
RouterC(config-if)# exit
RouterC(config)# interface Serial 0/0/1
RouterC(config-if)# bandwidth 128
RouterC(config-if)# exit
```

Nu wordt de snelle route gevolgd over router C.

```
C:\>tracert 192.168.1.2
Tracing route to 192.168.1.2 over a maximum of 30 hops:
  0  0 ms    1 ms    0 ms    192.168.1.129
  1  1 ms    0 ms    0 ms    192.168.1.246
  2  1 ms    1 ms    2 ms    192.168.1.241
  3  11 ms   11 ms   13 ms   192.168.1.2
```

De kost per verbinding kan opgevraagd door gedetailleerde informatie van de interface te vagen. De cost is hier 1562 aangezien de bandbreedte op 64 Kbps staat. Het resultaat van de deling van 10^8 door 64000 is immers 1562.

```
RouterB# show int s0/0/1
Serial0/0/1 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 192.168.1.242/30
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
```

...

```
RouterB# show ip ospf interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Internet address is 192.168.1.242/30, Area 0
  Process ID 1, Router ID 10.0.0.2, Network Type POINT-TO-POINT, Cost: 1562
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
```

...

18.7. Extra: Single-Area OSPFv3

❖ Configuring OSPFv3

Vooraleer je OSPFv3 op een router kan aanzetten, dient IPv6 routing aangezet worden. Daarna start je het OSPFv3 proces met een procesnummer en een router-id.

```
RouterA(config)# ipv6 unicast-routing
RouterA(config)# ipv6 router ospf 10
RouterA(config-rtr)# router-id 1.1.1.1
```

Doe dat voor alle routers.

```
RouterB(config)# ipv6 router ospf 10
RouterB(config-rtr)# router-id 2.2.2.2
```

Als je het router-id commando niet gebruikt wordt het hoogste loopbackadres gebruikt, en als dit afwezig is, het hoogste actieve IP-adres van de interfaces.

In tegenstelling tot OSPFv2, worden de netwerken niet toegevoegd aan het OSPF-proces, maar wordt het proces gekoppeld aan een interface.

```
RouterA(config)# interface GigabitEthernet 0/0
RouterA(config-if)# ipv6 ospf 10 area 0
RouterA(config-if)# exit
RouterA(config)# interface Serial 0/0/0
RouterA(config-if)# ipv6 ospf 10 area 0
RouterA(config-if)# exit
```

Net als bij IPv4 kan je passieve interfaces definiëren die niet meedoen aan OSPF.

```
RouterA(config)# ipv6 router ospf 10
RouterA(config-rtr)# passive-interface GigabitEthernet 0/0
```

Controleer de status van de ospfv3 interfaces.

```
RouterA# show ipv6 ospf interface brief
```

Je kan ook de ingegeven IPv6 statische routes laten uitwisselen tussen de routers, dit werkt ook voor de default route.

```
Router(config)# ipv6 route ::/0 s0/0/1
Router(config)# ipv6 router ospf 10
Router(config-rtr)# default-information originate
```

❖ Verifying OSPFv3

Het controleren van de IPv6-instellingen van de interfaces

```
Router# show ipv6 interface brief
```

Het controleren van de OSPF-buren

```
Router# show ipv6 ospf neighbors
```

Het controleren van het OSPF-proces

```
Router# show ipv6 protocols
```

Opvragen van de routetabel

```
Router# show ipv6 route
```

Of enkel de OSPF-routes

```
Router# show ipv6 route ospf
```

Net als bij IPv4 kan je in geval van snellere verbindingen best de referentiewaarde verhogen..

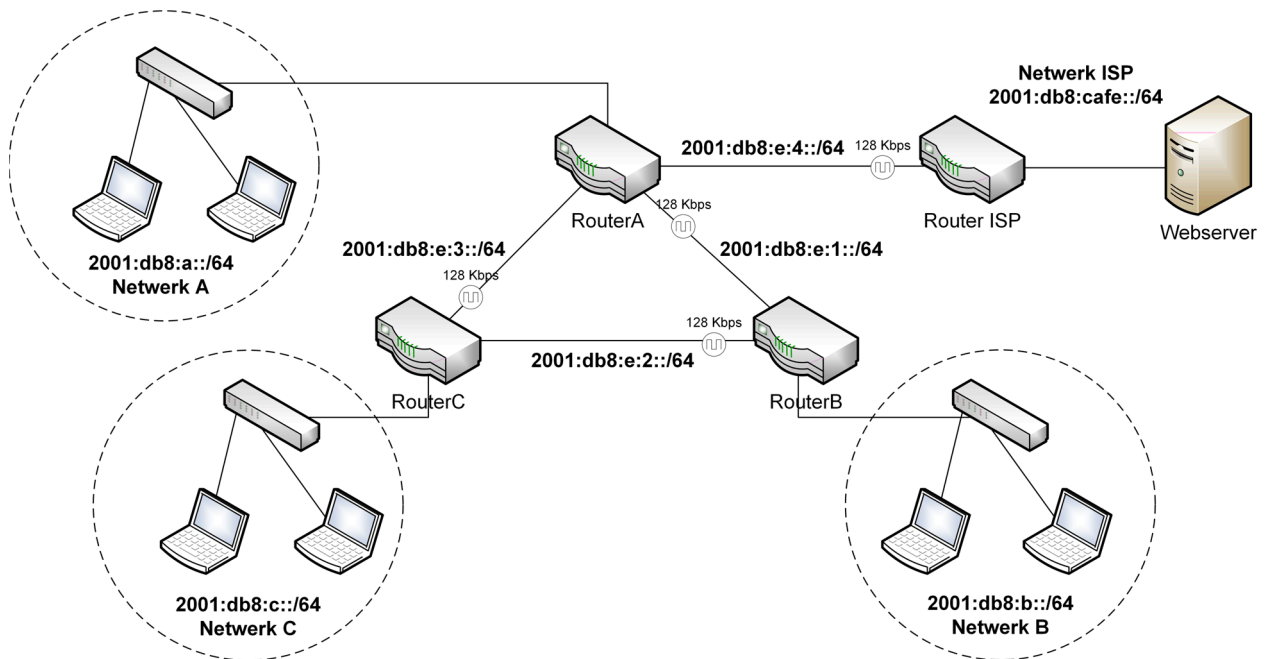
```
Router(config-rtr)# auto-cost reference-bandwidth 10000
```

Als je problemen ondervindt met router-id's, dan kan je het ospf-proces resetten met het volgend commando.

```
Router# clear ipv6 ospf proces
```

❖ Case study: OSPFv3

Hetzelfde netwerk als bij de case study van OSPFv2, al voorgeconfigureerd voor OSPFv2.



Figuur 14: Case study voor EIGRP met IPv6

Dit geeft het adresschema.

Apparaat	Poort	IPv6-adres	masker	Standaardrouter
Pc A in netwerk A	fa 0/0	2001:db8:a::2	/64	2001:db8:a::1
Pc B in netwerk B	fa 0/0	2001:db8:b::2	/64	2001:db8:b::1
Pc C in netwerk C	fa 0/0	2001:db8:c::2	/64	2001:db8:c::1
Router A	Gi 0/0	2001:db8:a::1	/64	Nvt
	S 0/0/0	2001:db8:e:1::1	/64	Nvt
	S 0/0/1	2001:db8:e:3::2	/64	Nvt
	S 0/1/0	2001:db8:e:4::2	/64	Nvt
Router B	Gi 0/0	2001:db8:b::1	/64	Nvt
	S 0/0/0	2001:db8:e:2::1	/64	Nvt
	S 0/0/1	2001:db8:e:1::2	/64	Nvt
Router C	Gi 0/0	2001:db8:c::1	/64	Nvt
	S 0/0/0	2001:db8:e:3::1	/64	Nvt
	S 0/0/1	2001:db8:e:2::2	/64	Nvt
Router ISP	S 0/0/0	2001:db8:e:4::1	/64	Nvt
	Gi 0/0	2001:db8:cafe::1	/64	Nvt
Webserver	fa 0/0	2001:db8:cafe::2	/64	2001:db8:cafe::1

Vooraleer je OSPFv3 kan starten moeten alle interfaces voorzien worden van de juiste IPv6-configuratie, dit wordt hier geïllustreerd voor router B. Aangezien OSPFv3 de link-local adressen gebruikt in de routetabel kunnen die best ook geconfigureerd worden zodat de routetabel vlotter kan gelezen worden. Alle interfaces van een router zullen hetzelfde link-local adres hebben, dus het is voldoende dit voor één interface in te stellen. We gebruiken hier fe80::a, fe80::b en fe80::c voor respectievelijk router a, b en c.

```
routerB# configure terminal
routerB(config)# interface Serial 0/0/0
routerB(config-if)# ipv6 address 2001:db8:e:2::1/64
routerB(config-if)# ipv6 address fe80::b link-local
routerB(config-if)# clock rate 128000
routerB(config-if)# no shutdown
routerB(config-if)# exit
routerB(config)# interface Serial 0/0/1
routerB(config-if)# ipv6 address 2001:db8:e:1::2/64
routerB(config-if)# no shutdown
routerB(config-if)# exit
routerB(config)# interface GigabitEthernet 0/0
routerB(config-if)# ipv6 address 2001:db8:b::1/64
routerB(config-if)# no shutdown
routerB(config-if)# exit
```

Op de drie LAN-routers moet nu de configuratie van OSPFv3 gebeuren en die methode is overal identiek.

RouterA:

```
RouterA(config)# ipv6 unicast-routing
RouterA(config)# ipv6 ospf 10
RouterA(config-rtr)# router-id 1.1.1.1
RouterA(config-rtr)# passive-interface s0/1/0
RouterA(config-rtr)# passive-interface g0/0
```

RouterB:

```
RouterB(config)# ipv6 unicast-routing
RouterB(config)# ipv6 ospf 10
RouterB(config-rtr)# router-id 2.2.2.2
RouterB(config-rtr)# passive-interface g0/0
```

RouterC:

```
RouterC(config)# ipv6 unicast-routing
RouterC(config)# ipv6 ospf 10
RouterC(config-rtr)# router-id 3.3.3.3
RouterC(config-rtr)# passive-interface g0/0
```

Daarna kan het OSPFv3-proces aan de interfaces gekoppeld worden.

```
RouterA(config)# interface GigabitEthernet 0/0
RouterA(config-if)# ipv6 ospf 10 area 0
RouterA(config-if)# exit
RouterA(config)# interface Serial 0/0/0
RouterA(config-if)# ipv6 ospf 10 area 0
```

En dit dient te gebeuren voor alle interfaces.

Net als bij IPv4 moet ter hoogte van router A de standaardroute toegevoegd worden en verdeeld worden naar de andere ospfv3-routers.

```
RouterA(config)# ipv6 route ::/0 2001:db8:e:4::1
RouterA(config)# ipv6 router ospf 10
RouterA(config-rtr)# default-information originate
```

Gedetailleerde informatie over het gebruikte routingprotocol opvragen geeft eveneens inzicht in de werking, net zoals het opvragen van de burens of de ospf-databank.

```
RouterB# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Interfaces (Area 0)
    GigabitEthernet0/0
    Serial0/0/1
    Serial0/0/0
  Redistribution:
    None
```



```

RouterB# show ipv6 ospf database
        OSPF Router with ID (2.2.2.2) (Process ID 10)
        Router Link States (Area 0)
ADV Router  Age      Seq#      Fragment ID  Link count Bits
2.2.2.2     464        0x80000021 0             2
3.3.3.3     832        0x8000001f 0             2
1.1.1.1     465        0x80000024 0             2          E
        Link (Type-8) Link States (Area 0)
ADV Router  Age      Seq#      Link ID      Interface
2.2.2.2     1525      0x8000000f 4            Se0/0/1
2.2.2.2     467       0x80000010 3            Se0/0/0
1.1.1.1     1027      0x80000011 3            Se0/0/1
        Intra Area Prefix Link States (Area 0)
ADV Router  Age      Seq#      Link ID      Ref-lstype  Ref-LSID
2.2.2.2     475      0x80000006 2            0x2001      0
1.1.1.1     475      0x80000006 2            0x2001      0
3.3.3.3     468      0x80000004 2            0x2001      0
        Type-5 AS External Link States
ADV Router  Age      Seq#      Prefix
1.1.1.1     259      0x80000002 ::/0

```

```

RouterB# show ipv6 ospf 10 neighbor
Neighbor ID  Pri  State      Dead Time  Interface ID  Interface
3.3.3.3      0    FULL/-     00:00:31   4            Serial0/0/0
1.1.1.1      0    FULL/-     00:00:31   3            Serial0/0/1

```

Hoofdstuk 19: ACLs for IPv4 Configuration

19.1. Create an ACL

❖ Numbered Standard IPv4 ACL

Je kan maar één ACL hebben per protocol, per interface en per richting (3P's):

- per protocol (bijv. IPv4 of IPv6)
- per richting (bijv. IN of OUT)
- per interface (bijv. GigabitEthernet0/0)

Bij een standaard ACL kan netwerk trafiek toegelaten of verboden worden vanaf de bron. Je gebruikt hiervoor netwerknummers en wildcard masks.

Een algemene richtlijn is om standard ACL's zo dicht mogelijk bij de bestemming te zetten.

```
Router(config)# access-list access-list-number {deny|permit|remark} source
[source-wildcard] [log]
```

De nummers voor standaard ACL's zijn 1 tot 99 en 1300 tot 1999.

```
Router(config)# access-list 10 remark Permit host from the 192.168.30.0 LAN
Router(config)# access-list 10 permit 192.168.30.0 0.0.0.255
```

❖ Named Standard IPv4 ACL

In plaats van met nummers kan ook met namen gewerkt worden.

```
Router(config)# ip access-list standard NO_ACCESS
Router(config-std-nacl)# deny host 192.168.10.10
Router(config-std-nacl)# permit any
Router(config-std-nacl)# exit
Router(config)# interface g0/0
Router(config-if)# ip access-group NO_ACCESS out
```

Een specifiek IP-adres host kan je ook met "host" aanduiden in plaats van de wildcard mask 0.0.0.0 mee te geven.

```
Router(config)# access-list 10 permit 192.168.30.1 0.0.0.0
of
Router(config)# access-list 10 permit host 192.168.30.1
```

In plaats van netwerknummer 0.0.0.0 met wildcard mask 255.255.255.255 mee te geven, kan dit ook met "any" aangeduid worden.

```
Router(config)# access-list 10 permit 0.0.0.0 255.255.255.255
of
Router(config)# access-list 10 permit any
```

ACL's worden sequentieel uit de toegangslijst gelezen tot de router een match vindt. Als er geen match gevonden wordt, dan wordt de trafiek geblokkeerd ook zonder dit echt op te nemen (implicit deny). De ACL1 en ACL2 hebben dus dezelfde werking.

```
Router(config)# access-list 1 permit ip 192.168.10.0 0.0.0.255
of
Router(config)# access-list 2 permit ip 192.168.10.0 0.0.0.255
Router(config)# access-list 2 deny any
```

Let er op om geen conflicten te creëren. De tweede regel heeft hier geen nut aangezien de eerste regel dit al tegen houdt.

```
Router(config)# access-list 3 deny 192.168.10.0 0.0.0.255
Router(config)# access-list 3 permit host 192.168.10.10
```

De volgorde wijzigen biedt een oplossing. Als beide netwerken niet in conflict zijn, maakt de volgorde niets uit.

```
Router(config)# access-list 3 permit host 192.168.10.10
Router(config)# access-list 3 deny 192.168.10.0 0.0.0.255
```

Controle van de configuratie:

```
Router# show access-lists
```

Indien er een probleem is met een ACL is het vaak gemakkelijker de bestaande ACL te verwijderen en opnieuw in te voeren. Dit voorkomt problemen.

```
Router(config)# no access-list 3
Router(config)# access-list 3 deny host 192.168.10.2
Router(config)# access-list 3 permit 192.168.10.0 0.0.0.255
```

❖ Apply a Standard IPv4 ACL

Een ACL moet gekoppeld worden aan een interface, waarbij bepaald wordt of het inbound of outbound is.

```
Router(config)# interface Gi0/0
Router(config-if)# ip access-group 3 out
```

Vraag de informatie van de poort op en controleer de instelling bij Outgoing en Inbound access list.

```
Router# show ip interface Gi0/0
GigabitEthernet0/1 is up, line protocol is up (connected)
Internet address is 192.168.1.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is 3
Inbound access list is not set
```

19.2. Modify IPv4 ACLs

Als een ACL dient ingegeven of gewijzigd te worden is het vaak gemakkelijker om de ACL in een teksteditor in te geven en dan in de CLI te plakken

Een ingewikkeldere methode is het werken met de sequentienummers. Stel dat je je vergist hebt in onderstaande ACL en dat je eigenlijk de host 192.168.10.3 wou blokken.

```
Router(config)# access-list 3 deny host 192.168.10.2
Router(config)# access-list 3 permit 192.168.10.0 0.0.0.255
```

Vraag dan de ACL-lijst op om zeker te zijn van de sequentienummers.

```
Router# show access-lists
Standard IP access list 3
  10 deny host 192.168.10.2
  20 permit 192.168.10.0 0.0.0.255
Router#
```

Daarna kan je bepaalde sequentienummers overschrijven. Let op! Hiervoor gebruik je "ip access-list", dus de methode van de ACL's met naam.

```
Router#configure terminal
Router(config)#ip access-list standard 3
Router(config-std-nacl)#no 10
Router(config-std-nacl)#10 deny host 192.168.10.3
Router(config-std-nacl)#end

Router#show access-lists
Standard IP access list 3
    10 deny host 192.168.10.3
    20 permit 192.168.10.0 0.0.0.255
Router#
```

Dezelfde methode kan gebruikt worden voor ACL's met naam.

```
Router#configure terminal
Router(config)#ip access-list standard NO_ACCESS
Router(config-std-nacl)#no 10
Router(config-std-nacl)#10 deny host 192.168.10.3
Router(config-std-nacl)#15 deny host 192.168.10.4
Router(config-std-nacl)#end

Router#show access-lists
Standard IP access list NO_ACCESS
    10 deny host 192.168.10.3
    15 deny host 192.168.10.4
    20 permit 192.168.10.0 0.0.0.255
Router#
```

▪ Opvragen van de statistieken

Je kan het aantal keren opvragen dat een regel is aangesproken, en indien gewenst de tellers ook terug op nul zetten.

```
Router# show access-lists
Standard IP access list 3
    10 deny host 192.168.10.2 (4 match(es))
    20 permit 192.168.10.0 0.0.0.255

Router# clear access-lists counters

Router# show access-lists
Standard IP access list 3
    10 deny host 192.168.10.2
    20 permit 192.168.10.0 0.0.0.255
```

19.3. Secure vty-ports with a standard IPv4 ACL

Een standaard ACL is zeer geschikt om de vty-lijnen verder te beveiligen:

```
Router(config)# line vty 0 4
Router(config-line)# login local
Router(config-line)# transport input ssh
Router(config-line)# access-class 21 in
Router(config-line)# exit
Router(config)# access-list 21 permit 192.168.10.0 0.0.0.255
Router(config)# access-list 21 deny any
```

19.4. Extended IPv4 ACLs

Bij een extended ACL kan netwerktrafiek toegelaten of verboden worden vanaf de bron, naar een bestemming, behorende tot een bepaald protocol en/of op poort. Je gebruikt hiervoor netwerknummers en wildcard masks.

Een algemene richtlijn is om extended ACL's zo dicht mogelijk bij de bron te zetten.

❖ Numbered extended ACL

De nummers voor extended ACL's zijn 100 tot 199 en 2000 tot 2699.

```
R1(config)# access-list access-list-number {deny|permit|remark} protocol
source [source-wildcard] [operator operand] [port port-number or name]
destination [destination-wildcard] [operator operand] [port port-number or
name] [established]
```

TCP-verkeer mogelijk van netwerk 192.168.30.0 naar overal, voor poorten 80 en 443.

```
R1(config)# access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
R1(config)# access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 443
```

TCP-verkeer mogelijk van overal naar netwerk 192.168.30.0, zolang de aanvraag maar vanaf 192.168.30.0 gestuurd is (dus voor ACK- en RST-segmenten).

```
R1(config)# access-list 104 permit tcp any 192.168.30.0 0.0.0.255 established
```

Ook een extended ACL moet gekoppeld worden aan een interface, waarbij bepaald wordt of het inbound of outbound is.

```
R1(config)# interface gi 0/0
R1(config-if)# ip access-group 103 in
R1(config-if)# ip access-group 104 out
```

In plaats van poortnummers kunnen ook protocolnamen gebruikt worden.

```
R1(config)# access-list 101 permit tcp 192.168.30.0 0.0.0.255 any eq 20
R1(config)# access-list 101 permit tcp 192.168.30.0 0.0.0.255 any eq 21

of

R1(config)# access-list 101 permit tcp 192.168.30.0 0.0.0.255 any eq ftp
R1(config)# access-list 101 permit tcp 192.168.30.0 0.0.0.255 any eq ftp-data
```

Gebruik van de protocolnaam voor telnet.

```
R1(config)# access-list 101 deny tcp any 192.168.30.0 0.0.0.255 eq 23

of

R1(config)# access-list 101 deny tcp any 192.168.30.0 0.0.0.255 eq telnet
```

❖ Named extended ACL

In plaats van met nummers kan ook met namen gewerkt worden.

```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# permit tcp 192.168.10.10 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.10 0.0.0.255 any eq 443
R1(config-ext-nacl)# exit
R1(config)# ip access-list extended BROWSING
R1(config-ext-nacl)# permit tcp any 192.168.10.10 0.0.0.255 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group SURFING in
```

```
R1(config-if)# ip access-group BROWSING out
```

❖ **Verify extended ACL**

Je kan de gekoppelde ACL controleren per interface.

```
R1# show ip interface g0/0
```

Je krijgt dan de info op de outgoing en inbound.

Hoofdstuk 20: Network Address Translation

20.1. NAT Characteristics

20.2. Types of NAT

20.3. NAT Advantages and Disadvantages

20.4. Static NAT for IPv4

❖ Configuring Static Translation of Inside Source Addresses

Configureer statische translatie van inside bronadressen als je een één-op-één mapping wil tussen inside local adressen en inside global adressen. Statische translatie is nuttig als een host aan de binnenkant dient bereikt te worden door een vast adres aan de buitenkant.

▪ Te volgen stappen

1. enable
2. configure terminal
3. ip nat inside source static local-ip global-ip
4. interface type number
5. ip address ip-address mask [secondary]
6. ip nat inside
7. exit
8. interface type number
9. ip address ip-address mask
10. ip nat outside
11. end

▪ Voorbeeld

```
Router> enable
Router# configure terminal
Router(config)# ip nat inside source static 192.168.10.1 201.201.201.1
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 192.168.20.1 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface fastethernet 0/1
Router(config-if)# ip address 200.200.200.1 255.255.255.240
Router(config-if)# ip nat outside
Router(config-if)# end
```

De volgende commando's zijn handig om fouten te zoeken in de NAT-instelling

```
Router# show ip nat translations
Router# show ip nat statistics
Router# clear ip nat statistics
Router# debug ip nat
```

20.5. Dynamic NAT

❖ Configuring Dynamic Translation of Inside Source Addresses

Dynamische translatie resulteert in een mapping tussen één inside lokaal adres en een pool van globale adressen. Dynamische translatie is nuttig als meerdere gebruikers van een privaat network toegang tot het internet nodig hebben.

De dynamisch geconfigureerde pool van IP-adressen wordt volgens nood gebruikt en wordt terug vrijgegeven nadat de toegang niet langer nodig is.

▪ Te volgen stappen

1. enable
2. configure terminal
3. ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}
4. access-list access-list-number permit source [source-wildcard]
5. ip nat inside source list access-list -number pool name
6. interface type number
7. ip address ip-address mask
8. ip nat inside
9. exit
10. interface type number
11. ip address ip-address mask
12. ip nat outside
13. end

▪ Voorbeeld

```
Router> enable
Router# configure terminal
Router(config)# ip nat pool net-208 172.16.233.208 172.16.233.223 prefix-
length 28
Router(config)# access-list 1 permit 192.168.34.0 0.0.0.255
Router(config)# ip nat inside source list 1 pool net-208
Router(config)# interface ethernet 1
Router(config-if)# ip address 10.114.11.39 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface ethernet 0
Router(config-if)# ip address 172.16.232.182 255.255.255.240
Router(config-if)# ip nat outside
Router(config-if)# end
```

20.6. PAT

❖ Using NAT to Allow Internal Users Access to the Internet over one global address (=PAT)

Deze methode geeft alle gebruikers toegang tot het internet met slechts één inside globaal adres, maar met overloading.

▪ Te volgen stappen

1. enable
2. configure terminal
3. access-list access-list-number permit source [source-wildcard]
4. ip nat inside source list access-list-number interface interface-name overload
5. interface type number

6. ip address ip-address mask
7. ip nat inside
8. exit
9. interface type number
10. ip address ip-address mask
11. ip nat outside
12. end

▪ Voorbeeld

```
Router> enable
Router# configure terminal
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# ip nat inside source list 1 interface g0/0 overload
Router(config)# interface g 0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface s0/0/0
Router(config-if)# ip address 20.0.0.2 255.255.255.252
Router(config-if)# ip nat outside
Router(config-if)# end
```

▪ Troubleshooting

De volgende commando's zijn handig om fouten te zoeken in de NAT-instelling

```
Router# show ip nat translations
Router# show ip nat statistics
Router# clear ip nat statistics
Router# debug ip nat
```

20.7. Port forwarding using IOS

▪ Voorbeeld

```
Router> enable
Router# configure terminal
Router(config)# ip nat inside source static tcp 192.168.10.254
80 209.168.200.225 8080
Router(config)# interface g 0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface s0/0/0
Router(config-if)# ip nat outside
Router(config-if)# end
```