Cisco CCENT / CCNA 200-120
(ICND1 100-101 + ICND2 200-101)
Samenvatting / CheatSheet

Jarno Baselier

Inhoudsopgave

Netwerk info (algemeen)

OSI & TCT/IP model

OSI model bestaat uit 7 lagen:

1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

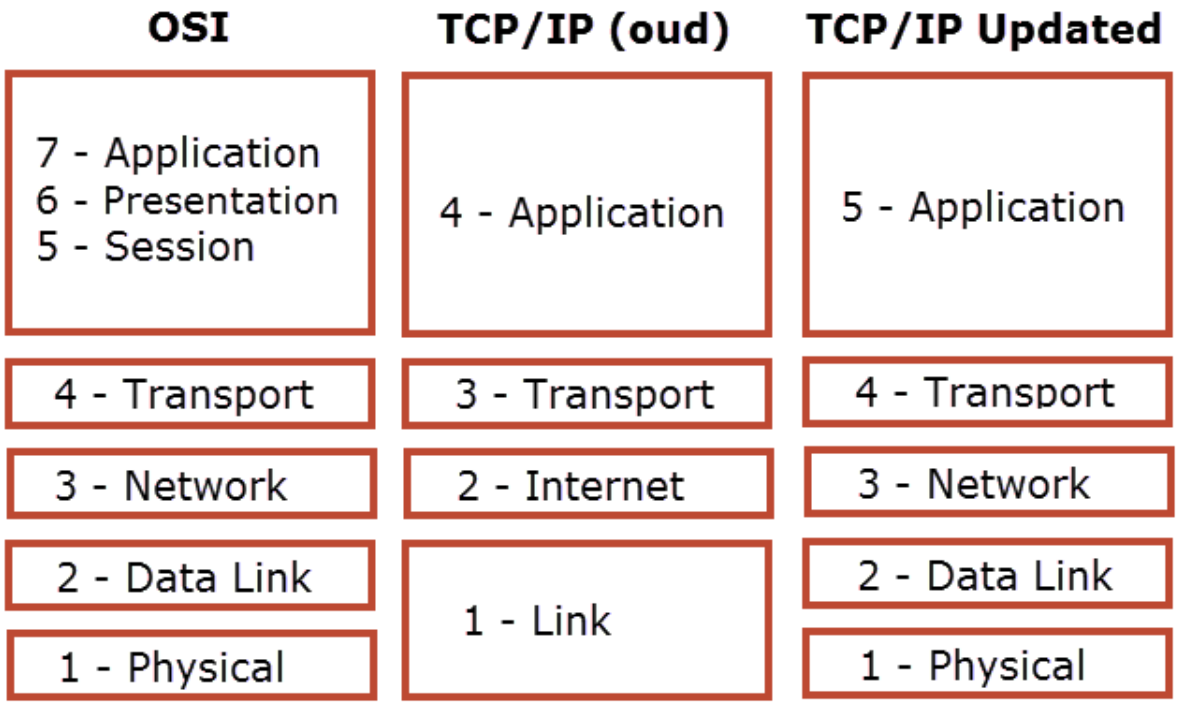
Laag 5 t/m 7 zijn alle 3 applicatielagen. Naast het OSI model is er een oud en een nieuw TCP/IP model welke deze lagen gecombineerd heeft. Het oude TCP/IP model heeft 4 lagen:

1. Link
2. Internet
3. Transport
4. Application

Het nieuwe TCP/IP model heeft 5 lagen:

1. Physical
2. Data Link
3. Network
4. Transport
5. Application

In networking wordt ondanks de populariteit van TCT/IP vrijwel altijd verwezen naar het OSI model.



OSI lagen + Protocollen

7 – Application
Software welke met andere end-devices communiceert + user authentication.
Protocollen: HTTP / FTP / DHCP / SMTP

6 – Presentation
Negotiates data formats (ASCII / Binary / JPEG) + encryption
Protocollen: TLS

5 – Session
Bepaald hoe sessies te starten, stoppen en controleren
Protocollen: NETBIOS / SMB / SOCKS

4 – Transport
Hoe data overbrengen op ander device. Flow control + error recovery
Protocollen: TCP / UDP

3 – Network
Logische adressering – Routing – Path determination
Protocollen: IP / ARP / ICMP / IGMP

2 – Data Link
Regels wanneer een apparaat over een medium kan verzenden + packet header formaat + packet trailer
Protocollen: Ethernet / HDLC

1 – Physical
Regels over fysieke aansluitingen zoals bedrading en connectors
Protocollen: RJ45 / Ethernet

Adjacent Layer Interaction
Wanneer een laag communiceert met een bovenliggende laag op hetzelfde device

Same Layer Interaction
Wanneer een laag communiceert met dezelfde laag op een ander device

Onthouden van OSI lagen (laag 7 naar 1)
APSTNDP
=All People Seem To Need Data Protection

Protocol Data Unit / Pakket informatie door de lagen heen

OSI noemt ieder pakketje dat tussen de lagen wordt verstuurd een PDU (Protocol Data Unit). De PDU wordt gemarkeerd aan de laag. Een PDU op laag 5 heet L5PDU en een pakketje op laag 2 een L2PDU.

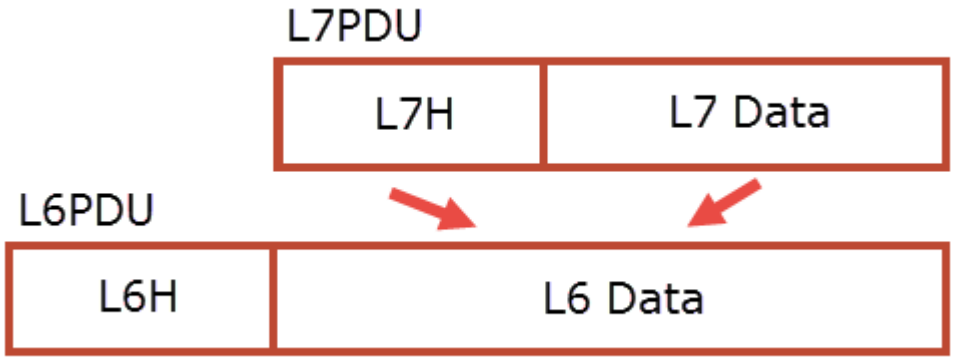
Het TCP/IP model gebruikt niet het PDU principe maar werkt per laag met een anderen naam.

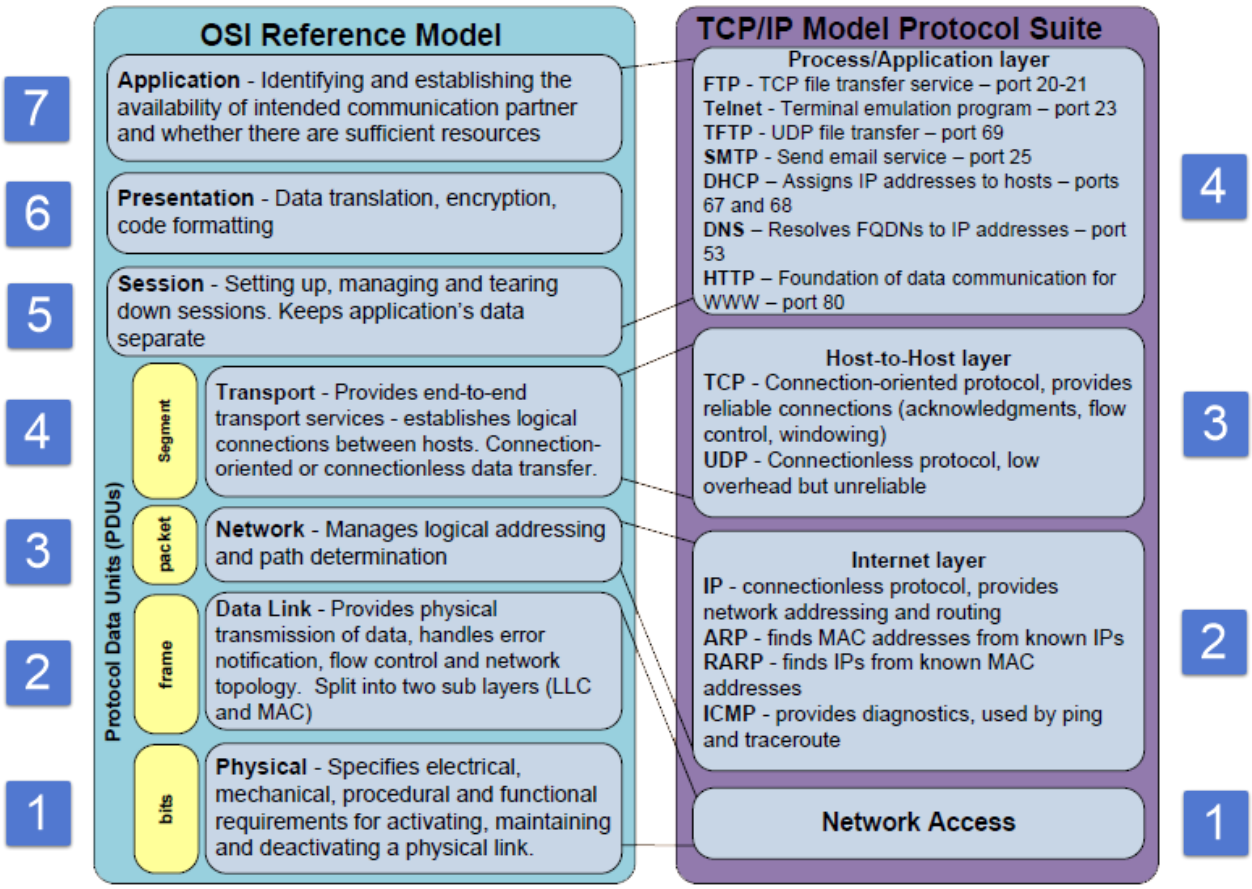
4 – Transport =	Segment
3 – Network =	Packet
2 – Data Link =	Frame
1 – Physical =	Bits

De 4 termen die belangrijk zijn, zijn: Segment, Packet en Frame ofwel SPF (Simple Packet Format).

Encapsulation

Elke laag converteert de data van het voorgaande pakket (incl. de header). Dit noemen we “encapsulation” (het opnieuw inpakken van…).





Type LAN's & Wireless LAN's

Ethernet:
Het Ethernet gebruikt kabels. Standaarden beginnen met de snelheid en eindigen op het type bekabeling. Zo staat T voor koper. De formele IEEE standaarden beginnen met: 802.3

Standaard	IEEE code	Max. Afstand	Snelheid	Type bekabeling
10BASE-T	802.3i	100m	10 mbit/s	TIA-CAT3 >
100BASE-T	802.3u	100m	100 mbit/s	TIA-CAT5 2 pair >
1000BASE-T	802.3ab	100m	1000 mbit/s	TIA-CAT5e 4 pair >
1000BASE-SX		550m	1000 mbit/s	Multimode fiber
1000BASE-LX		550m	1000 mbit/s	Multimode fiber
1000BASE-LX		5km	1000 mbit/s	Single mode fiber
10GBASE-LR		10km	10000 mbit/s	Single mode fiber

Cisco hanteert verschillende namen voor verschillende snelheden:

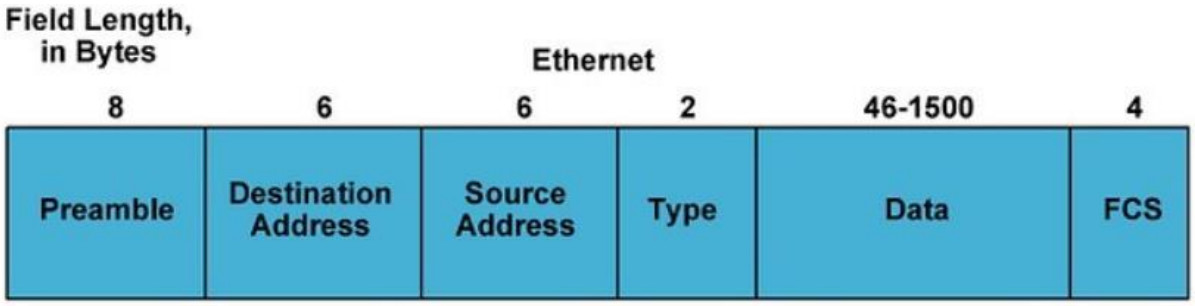
10 mbp/s = Ethernet
100 mbp/s = Fast Ethernet (FE)
1000 mbp/s = Gigabit Ethernet (GE)

Wireless:
Wireless maakt gebruik van radiogolven op verschillende frequenties. Standaarden beginnen met: 802.11.

Protocol	Jaartal	Frequentie (GHz)	Bandbreedte (MHz)	Modulatie
802.11a	1999	5	20	OFDM
802.11b	1999	2.4	22	DSSS
802.11g	2003	2.4	20	OFDM
802.11n	2009	2.4 & 5	20 & 40	MIMO-OFDM
802.11ac	2013	5	20 & 40 & 180 & 160	MIMO-OFDM
802.11ad	2012	60	2,160	OFDM / Single carrier / Low-Power Single Carrier
802.11ay	2017	60	8000	OFDM / Single Carrier

Data frames:

Ethernet frame
Een normaal Ethernet frame met payload size (MTU – Maximum Transmission Unit)) van 1500 octetten:



Grotere frames die ondersteund worden over snellere verbindingen zoals Gigabit Ethernet noemen we “Jumbo Frames”.

Classless Inter-Domain Routing – CIDR

CIDR is een methode voor het uitdelen van IP adressen om zo de snelle leegloop van de IPv4 pool tegen te gaan. Dit uitdelen van IP adressen gaat volgens een principe welke wereldwijd gehanteerd wordt. Door deze strategische uitgave worden routetabellen stukken korter. CIDR is afhankelijk van classless protocollen en werkt middels “Route Aggregation” en “Route Summarization”.

Layer 1 (physical) info

Full Duplex
Zenden & ontvangen tegelijkertijd

Half Duplex
Zenden of ontvangen. Bij Half Duplex gebruiken nodes CSMA/CD om botsingen te voorkomen.

Auto Negotiation
Auto Negotiation is een methode waarbij de NIC's automatisch de beste snelheid bepalen om data loss te voorkomen. Auto Negotiation kent de volgende regels:

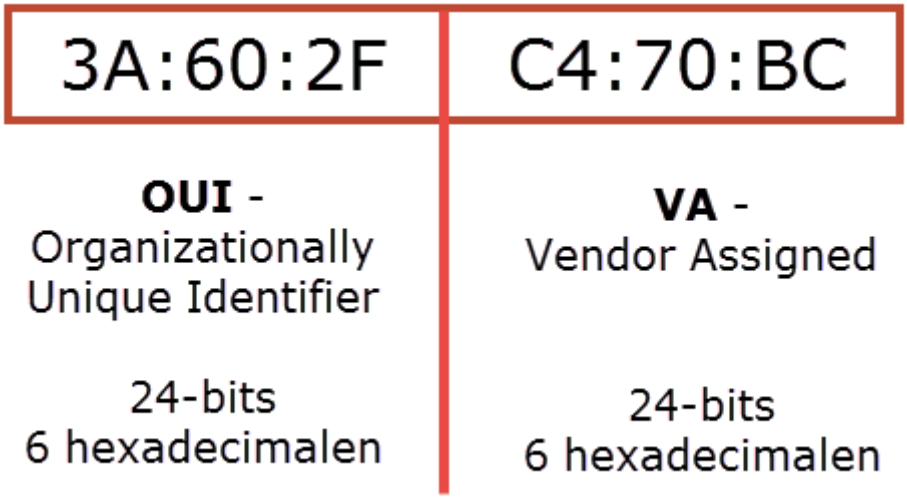
- Speed: Gebruik de laagste speed welke ondersteund is
- Duplex: Gebruik half duplex bij 10/100 en full duplex bij 1000

Layer 2 (Data Link / Switching) info

Onder Layer 2 vallen apparaten die intern kunnen communiceren binnen hetzelfde collision domein. Deze apparaten routeren frames op basis van MAC adres en niet op IP adres.

Mac adres:

Het MAC adres is een eigenschap die op layer 2 gebruikt wordt. Een MAC adres bestaat uit 48 bits en wordt vaak geschreven als 12 hexadecimale karakters. De eerste 6 karakters (24-bits) worden gebruikt om het merk te identificeren (dit noemen we de OUI = Organizationally Unique Identifier). De laatste 6 karakters (24-bits) zijn om het apparaat de identificeren en noemen we de VA = Vendor Assigned.



MAC adressen zijn uniek en moeten uniek zijn om succesvol binnen een netwerk te kunnen functioneren.

Broadcast Frame: FFFF:FFFF:FFFF

MAC tabel

Switches en Routers beschikken over een MAC tabel. Deze MAC adressen in deze tabel worden door het apparaat toegevoegd (geleerd) door naar het source adres te kijken van binnenkomende pakketten. Als het MAC adres niet bekend is wordt het frame naar elke poort (behalve de binnenkomende poort) gestuurd. Dit proces noemen we “flooding”.

QoS – Quality of Service

Quality of Service controleert de volgende onderdelen om de QoS te garanderen:

Bandwidth:
Aantal bits per seconde welke de applicatie nodig heeft

Delay:
De tijd die het IP pakket nodig heeft om van afzender naar ontvanger te gaan

Jitter:
De variatie in “delay” (tijd)

Loss:
Het aantal pakketten dat onderweg verloren wordt (en bij TCP opnieuw verzonden moeten worden)

Collision Domain

Een Collision Domain is de range waarin collisions / data botsingen kunnen voorkomen. Alle aangesloten apparaten op een hub ontvangen al het verkeer en moeten op elkaar wachten tijdens het verzenden en ontvangen van data. Alle apparaten op een hub zitten in 1 collision domain. Een Switch regelt het verkeer intern en daarom is iedere verbinding tussen device en switch 1 collision domain. Met andere woorden, apparaten hebben geen last van elkaar.

Broadcast Domain

Een broadcast domain bestaat uit alle PC’s die broadcast pakketten van elkaar kunnen ontvangen.

LAN – Local Area Network

Een LAN zijn alle apparaten in 1 broadcast domain. Een Campus LAN is een groot LAN netwerk al dan niet bestaande over meerdere gebouwen / lokaties.

Spanning Tree Protocol - STP

STP (IEEE 802.1D) zet poorten in een forwarding of blocking status. Forwarding betekend dat de poort data frames kan ontvangen en forwarden en blocking betekend dat de poort dit niet kan.

STP wordt gebruikt om layer 2 loops te voorkomen. STP verstuurt pakketjes tussen switches (en bridges en andere STP ondersteunende apparaten). Deze pakketjes noemen we Bridge Protocol Data Units (BPDU). Er zijn verschillende varianten van STP waaronder RSTP (Rapid Spanning Tree Protocol – IEEE 802.1w) en Per VLAN Spanning Tree Plus (PVST+ - 802.1D). Cisco gebruikt standaard PVST+.

STP (ongeacht de variant) werkt met 3 basisprincipe:

- Selecteren van de Root Bridge (RB)
- Selecteren van de Root Port (RP) op de niet RB switches
- Selecteren van de Designated port op de niet RB switches

*Alle poorten die niet op de RB zitten of RP of DP zijn worden in een blocking status gezet. RB, RP en DP zijn rollen. Poorten hebben verschillende statussen (states):

- Forewarding – De poort update zijn MAC tabel via binnengekomen pakketjes en foreward de data
- Blocking – Stable state – De poort is niet down maar foreward geen verkeer en werkt MAC tabel niet bij
- Disabled – Stable state – De poort is administratively down en wordt niet door STP gebruikt
- Lisening – Transitory state – De poort foreward nog geen data maar verwijderd alle ongebruikte MAC adressen (waar geen data van binnen is gekomen gedurende de lisening state).

- Learning – Transitory state – De poort foreward nog geen data en begint met het leren van nieuwe MAC adressen (waar in deze periode data van binnenkomt).

Root Bridge
De Root Bridge is de enige switch in het netwerk die alle poorten in een forwarding state heeft staan (alle poorten zijn designated poorten met een 0 cost). De RB wordt de switch die de laagste Bridge ID (BID) heeft. Het bridge ID bestaat bij standaard STP uit 2 delen, namelijk een 16-bits priority field en het MAC adres. Als er switches zijn met dezelfde priority (de eerste check) dan wordt het MAC adres als tiebreaker gebruikt. Het laagste MAC adres wint dan. Een switch die net online komt adverteert zijn eigen BID als root bridge. Als de switch echter een BPDU helo bericht ontvangt met waarin een RB vermeld is met een lagere Bridge ID dan zal de switch de helo BPDU berichten van de root bridge doorsturen.

Het Bridge ID bestaat uit 3 delen wanneer PVST+ gebruikt wordt. Het 16-bits priority gedeelte is opgesplitst in een 4-bit priority gedeelte en een 12-bit System ID gedeelte. Het System ID wordt gebruikt om VLAN informatie in op te slaan. VLAN's hebben een range van 1 tot 4094. Om dit aan te geven zijn 12 bits nodig. Het voorgaande priority gedeelte moet daarom oplopen in stappen van 4096, dus 0 – 4096 – 8192 – 12288 etc. Er zijn 16 mogelijkheden (4-bits) t/m 61440. De default priority is 32768. Het enige gedeelte dat door een Cisco administrator beheerd kan worden is het priority gedeelte.

Om het bridge ID aan te passen moeten we de volgende commando's gebruiken:

()spanning-tree vlan 1 priority 0

Het is echter ook mogelijk om 2 root bridges aan te wijzen. 1x de primaire RB en 1x de secundaire RB voor het geval dat de primaire RB down gaat. Dit commando is als volgt:

()spanning tree vlan 1 root primary
&
()spanning tree vlan 1 root secundary

Root Port
De Root Port (RP) is de poort van switch X die de laagste STP path cost heeft om bij de Root Bridge switch te komen. Het kan voorkomen dat er meerdere connecties mogelijk zijn. 1 van deze connecties wordt de Root Port (de poort die de data foreward). De Root Port wordt geselecteerd op basis van zijn totaal STP path cost. Het kan dus voorkomen dat een directe verbinding tussen de Root Bridge en switch X langzamer is dan de connectie van switch X naar switch Y en dan naar de Root Bridge. In dat geval wordt de interface op switch X die verbonden is met switch Y de Root Port.

Soms eindigt de keuze voor de root port in een "tie" / gelijkspel. Als dat gebeurt dan bepaald de switch zijn root port via het volgende scenario:

- Kies op basis van de neighbor met het laagste BID
- Kies op basis van de neighbor met de laagste port priority
- Kies op basis van de neighbor met het laagste interne poortnummer

Port Priority
Poorten kunnen geconfigureerd worden met "port priority". Standaard heeft een Cisco poort een priority van 128. De waarde kan vallen tussen 0 en 255. Normaliter geld de regel "hoe lager de port priority, des te beter.

Designated Port
De designated port is de poort die de laagste root cost heeft binnen een LAN segment (meestal tussen 2 switches want bij een switch en een PC wint de switch altijd). In het geval van een "tie"/gelijkspel wordt de DP gekozen op de switch met het laagste BID. Een switch kan meerdere DP's hebben en een DP kan nooit een RP zijn. Niet-Root Bridges adverteren helo berichten op het netwerk. In deze berichten staat hoeveel de root cost is (van die interface naar de Root Bridge). De interface met de laagste root cost wordt de designated port voor dat LAN segment.

De kosten van een poort worden standaard behaald door te kijken naar de snelheid van de poort.
10 Mbps = 100
100Mbps = 19
1 Gbps = 4
10 Gbps = 2

Uiteraard kunnen deze waardes door de beheerder veranderd worden. Om de poortkosten vast te zetten gebruik je:
(-)spanning tree vlan 1 cost 50 <- 50 geeft de port cost aan voor VLAN 1 (alleen op trunk)
(-)spanning tree cost 50 <- 50 geeft de port cost aan voor de interface

Convergence:
Op het moment dat er een link down gaat moet SPT opnieuw vaststellen wat de RB, RP en DP zijn. Dit noemen proces noemen we "convergence". Dit proces is gebaseerd op timers die vastgesteld worden door de Root Bridge. Er zijn 3 timers nodig:

- Helo (de tijd tussen de helo berichten) – standaard 2 seconden
- MaxAge (de tijd die een switch moet wachten en door moet gaan met normaal functioneren als deze geen helo berichten meer ontvangt) – standaard 10 helo's
- Foreward Delay (De tijd die gewacht wordt als een interface van blocking naar forewarding state gebracht moet worden. Deze tijd wordt gebruikt om MAC adressen te leren. In deze periode gaat de poort door de listening en learning fase) – standaard 15 seconde per fase

Als een status veranderd en een poort moet van blocking naar forewarding modus gezet worden duurt dit (met standaard settings) dus 2x10 + 15 + 15 = 50 seconde.

Geavanceerde STP technieken:

Etherchannel
EtherChannel is het bundelen van poorten. Deze techniek ziet 2 of meer (maximaal 8) connecties tussen een switch als 1 connectie met een andere switch. Als er 1 lijn uitvalt neemt de andere lijn het over en hoeft er geen convergence plaatst te vinden. Een ander voordeel is de load balancing. De snelste verbinding in de bundel wordt gebruikt voor het doorsturen van data.

Als er poorten / links toegevoegd worden aan een etherchannel groep dan moeten de specificaties van deze poort overeenkomen met de specificaties van de poorten die al in de channel zitten. Als dit niet is zal de poort toegevoegd worden maar niet werken en in een err-disabled state worden geplaatst. Zo moeten o.a. de volgende specificaties overeenkomen:

- Snelheid & Duplex
- Alles moet access of alles moet truck zijn. Trunk & Access samen werkt niet
- Als access port, dan moet het VLAN overeenkomen
- Als trunk poort, dan moet de allowed VLAN list overeenkomen (volgens het commando “switchport trunk allowed”. Ook moet het native VLAN overeenkomen
- STP interface instellingen

Bij manuele configuratie worden deze instellingen gecontroleerd met het CDP (Cisco Discovery Protocol) en bij dynamic etherchannel via PAgP of LACP (later meer hierover).

Tijdens de configuratie worden 3 termen door elkaar gebruikt. Channel-group (voor configuratie), etherchannel (in show commands) en portchannel (in output van show commands). Ethernet kan manueel en dynamisch geconfigureerd worden.

Manual Etherchannel
De configuratie van manual etherchannel is in de basis gemakkelijk:
>Open elke interface die lid is van de etherchannel groep en geef het commando om ze lid te maken (channel-group 1 mode on)

Dynamic Etherchannel
Voor configuratie van dynamic etherchannel kunnen 2 protocollen gebruikt worden. Deze protocollen controleren of de lijn voldoet aan alle eisen om lid te worden van de etherchannel groep. Deze protocollen zijn:

- Port Aggregation Protocol (PAgP) = Cisco only protocol
- Link Aggregation Control Protocol (LACP) = general protocol

Om een poort dynamic etherchannel te laten gebruiken moet de poort aan 1 kant geactiveerd worden. De andere kant van de poort mag dan ook geactiveerd staan of op passieve modus staan. De passieve modus zal actief worden wanneer er een signaal geïnitieerd wordt.

PAgP heeft 2 opties: desirable = actief & auto = passief
LACP heeft 2 opties: active = actief & passive = passief

Om een poort automatisch te laten confituren gebruik je bij PAgP:
channel-group 1 mode desirable

En bij LACP
channel-group 1 mode active

PortFast
Portfast kan een poort sneller van blocking naar learning state zetten door de listening en learning fases (30 seconde) over te slaan. Dit kan toegepast worden op poorten die met endpoints verbonden zijn omdat deze nooit hoeven te onderhandelen over de route naar de RB. Een client heeft na het booten van zijn PC veel sneller verbinding en hoeft geen extra 30 seconde te wachten alvorens STP besloten heeft dat het een DP is en verkeer mag forewarden.

Schakel PortFast in:
(-)spanning-tree portfast

Schakel PortFast op alle poorten in:
()spanning-tree portfast default

BPDU Guard
BPDU Guard is een veiligheidsfeature welke op alle endpoint poorten geactiveerd kan worden. BPDU zorgt ervoor dat de poort geblokkeerd wordt als deze een BPDU helo ontvangt en er dus een STP apparaat op aangesloten wordt. Dit kan een Rogue switch van een hacker zijn of een goedkope consumer switch. BPDU voorkomt deze gevaren. Vaak worden BPDU Guard en Portfast op dezelfde endpoint poorten (access poorten) geactiveerd.

Schakel BPDU Guard in:
(-)spanning-tree bpduguard enable

Schakel BPDU Guard op alle poorten in:
()spanning-tree portfast bpduguard default

Rapid STP:
Van Rapid STP (RSTP) is het goed om te weten dat RSTP compatible is met STP (802.1D) en dat RSTP nieuwe (alternatieve en backup) poort rollen definieert binnen zijn topologie. Het voordeel van RSTP is dat hij veel sneller is met het omzetten van de flow na een link failure (reconverging) en dat de tijd korter is dat poorten in een forwarding state geplaatst worden.

Troubleshooting
STP is een moeilijk protocol om te troubleshooten. Hierbij een aantal tips:

Kies de root bridge:
1. Maak een lijst of diagram met alle switches
2. Streep de switches met een RP door (een RB heeft nooit een RP)
3. Gebruik “show spanning-tree” of “show spanning-tree root” voor meer informatie over de RB
4. Met meerdere VLAN’s gebruik je “show spanning-tree vlan X”

Root Port problemen oplossen:
1. Gebruik “show spanning-tree” en “show spanning-tree root” om informatie over de root port te krijgen.
2. Onthoud de cost values op basis van de verbinding (snelheid)
3. Ga er niet vanuit dat standaard costs worden gebruikt op het examen. Kijk dit na met bovenstaande commando’s.

Switches type’s
Cisco beschrijft 3 typen switches:

Access Switch:
Verbonden met end-user devices

Distribution Switch:
Verbonden met access switches, elkaar en eventueel de core switches

Core Switch:
Top Switch. Verbonden met elkaar en de distribution switches

Port Security

Poorten kunnen beveiligd worden met de Port Security feature:

- Configuratie / enable per poort
- Beveiliging gebaseerd op MAC adres
- Stel een maximaal aantal MAC adressen in voor toegang op de poort
- Poort moet een access (switchport mode access) of trunk (switchport mode trunk) zijn
- Er zijn 3 security modes (*shutdown is default mode):

	Protect	**Restrict**	**Shutdown***
Drop ongeautoriseerde toegang	Y	Y	Y
Verzend logs en SNMP info	X	Y	Y
Disables de interface	X	X	Y

Indien port security ingesteld is om bij een violation in shutdown mode te gaan wordt de poort in "err-disabled" status gezet. De enige manier om de poort weer te laten functioneren is om de poort uit- en in te schakelen (shutdown & no shutdown op de poort).

VLAN's

- Een VLAN zijn alle apparaten in hetzelfde broadcast domain
- VLAN Trunk: Dit is een poort die VLAN's van switch A naar switch B kan sturen
- Tagging: de trunk voegt een VLAN ID toe aan het pakket om deze naar een apparaat (andere switch) te sturen die het pakket binnen dit VLAN moet distribueren. Na ontvangst van het pakket wordt de tag weer verwijderd
- Verschillende VLAN's moeten allen voorzien zijn van een verschillend subnet zodat layer 3 switches of routers pakketten naar dit andere VLAN en netwerk kunnen routeren.
- Als er vanuit een switch 1 kabel naar een router gaat (de trunk) dan noemen we deze opstelling ook wel "router on a stick" (ROAS)

Trunk's en Trunking Protocollen

Voor CCNA zijn er 3 belangrijke trunking protocollen:

1. **VTP – VLAN Trunking Protocol**
    - Cisco only protocol
    - Voor advertising van VLAN's naar andere Cisco devices
    - Kan niet altijd volledig uitgeschakeld worden

VTP uitschakelen:

()vtp mode off OF ()vtp mode transparent

VTP modes:

Client	-	Een cliënt kan geen VLAN's aanmaken
Server	-	Een server kan VLAN's aanmaken in de range 1-1005
Transparent	-	Device doet niet mee aan VTP (doet geen VLAN's advertisen of syncen

2. **ISL – InterSwitch Link**
    - Cisco only protocol
    - Header heeft een 12-bits tag voor VLAN ID

3. **IEEE 802.1Q**
    - Standaard protocol (werkt ook op switches van andere vendors)
    - Voegt geen VLAN ID toe aan pakketten van en naar het native VLAN
    - Header heeft een 12-bits tag voor het VLAN ID

Middels deze 12-bit die gereserveerd zijn voor VLAN's in de headers van ISL & 802.1Q kunnen 4096 VLAN ID's meegestuurd worden. Deze range van 4096 VLAN ID's is opgedeeld in:

Gereserveerde VLAN ID's:
0 & 4095

Standaard range:
1 – 1005. Deze range kan door iedere VLAN switch gebruikt worden. Binnen deze range heeft Cisco standaard de volgende VLAN's aangemaakt:

1 = native VLAN
1002 = fddi-default
1003 = token ring default
1004 = fddinet-default
1005 = trnet-default

Extended range:
1006 – 4096 = 3090 (minus ID 4095) = 3089 bruikbare extended adressen. Deze kunnen echter niet op alle switches gebruikt worden. Of deze gebruikt kunnen worden is afhankelijk van de VTP configuratie.

Trunking VLAN's aanpassen
In een trunk zitten standaard alle VLAN's. Om VLAN's uit te zonderen of weer toe te voegen kunnen we de volgende commando's uitvoeren:

(-)switchport trunk allowed vlan %mode hieronder% %VLAN ID%

add	-	VLAN toevoegen
all	-	Alle VLAN's toelaten
except	-	Alle VLAN's toelaten behalve de opgegeven except range
remove	-	VLAN verwijderen

VLAN's worden niet over een trunk gestuurd als:

- VLAN uitgesloten is middels het "remove" commando
- VLAN niet in de config bestaat van de switch
- VLAN administratively down is (shutdown)
- Uitgesloten (pruned) is door VTP
- VLAN SPT (Spanning Tree Protocol) de trunk interface in blocking mode heeft geplaatst

Switchport modes

Een switchpoort kan geconfigureerd zijn in een aantal verschillende modes. Dit zijn:

Trunk - Poort is altijd een trunking poort
Access - Maximaal lid van 1 VLAN. Geen VLAN Trunking
Dynamic Desirable - Initieert trunking messages + responds
Dynamic Auto - Standaard setting. Responds only to trunking messages om trunking te activeren. Initieert zelf geen trunking messages.

	Access	**Dynamic Auto**	**Trunk**	**Dynamic Desirable**
Access	Access	Access	XXX	Access
Dynamic Auto	Access	Access	Trunk	Trunk
Trunk	XXX	Trunk	Trunk	Trunk
Dynamic Desirable	Access	Trunk	Trunk	Trunk

Configureer dus nooit aan 1 kant een Access poort en aan de andere kant een Trunk poort. Dit resulteert in een falende verbinding.

Informatie over de switchport modes van een poort bekijken:
>enable
#show interface fastethernet 0/1 switchport

Interface status

Iedere interface heeft een bepaalde status welke opgevraagd kan worden met het commando:

#show interfaces status

Dit commando laat eigenschappen zien als snelheid, duplex en kabeltype. Dit commando laat ook 2 statussen zien, namelijke:

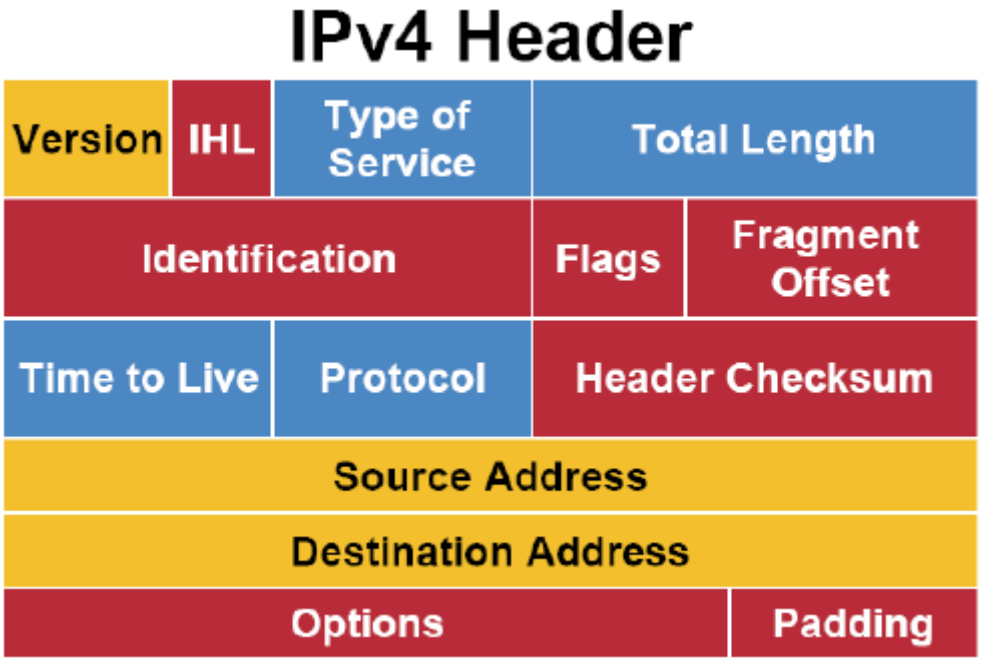
- Line Status (layer1)
- Protocol status (layer2)

De volgende combinaties zijn mogelijk:

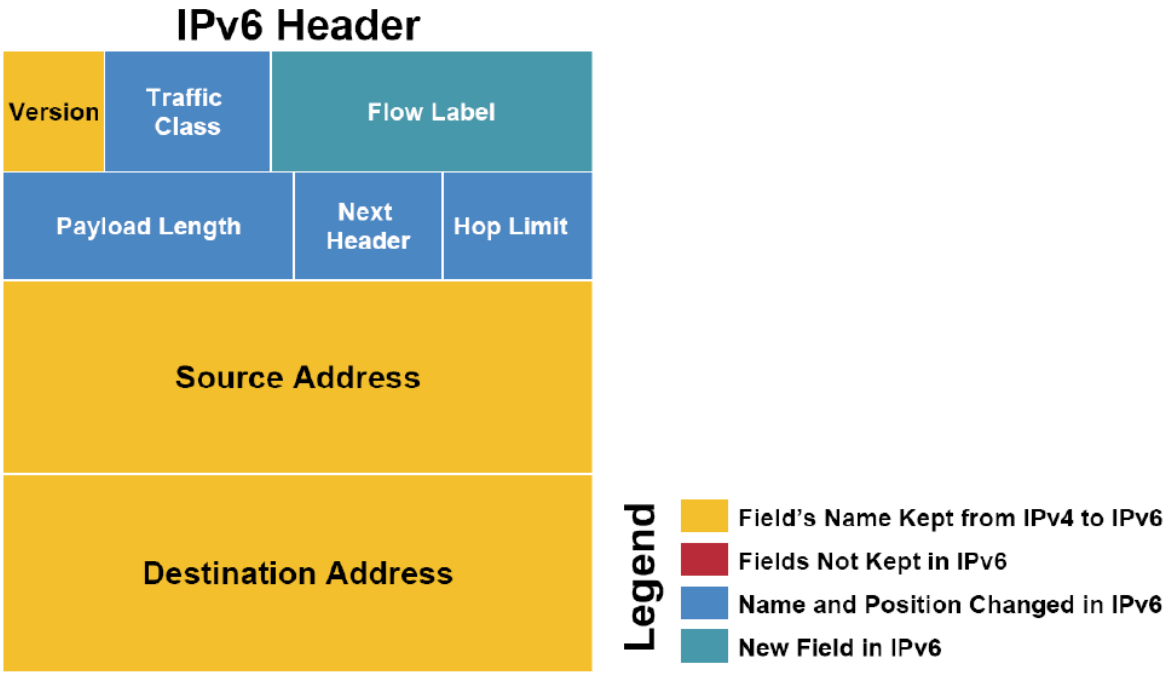
Line Status	**Protocol Status**	**Interface Status**	**Info**
Administratively Down	Down	Disabled	Configured Shutdown
Down	Down	NotConnect	Geen of slechte kabel
Up	Down	NotConnect	Deze combi komt niet voor op een LAN switch
Down	Down (err-disabled)	Err-disabled	Port security disabled
Up	Up	Connected	Up

IP Packet voorbeelden

IPv4 Header



IPv6 header



Protocollen

CSMA/CD - Carrier Sense Multiple Access / Collision Detection
Dit protocol bepaald wanneer netwerkapparaten mogen verzenden. Dit protocol voorkomt collisions (botsingen) en zorgt ervoor dat er maar 1 apparaat tegelijkertijd kan verzenden. CSMA/CD wordt gebruikt bij verbindingen die werken op Half Duplex.

Cisco Routers

- Cisco routers hebben in tegenstelling tot Cisco Switched een aan/uit button
- Connect een router altijd aan de CSU / DSU en de CSU / DSU aan de internetlijn van de aanbieder
- Veel routers hebben een interne CSU / DSU
- Routers hebben een AUX port en switches niet. De AUX poort wordt gebruikt om te verbinden met een extern modem en telefoonlijn zodat externe gebruikers via de AUX poort remote in kunnen loggen op de router
- Interfaces zijn administratively shutdown by default
- Routers routeren geen pakketjes alvorens een interface geconfigureerd is met een IP en subnetmask.
- Routers routeren pakketjes tussen alle interfaces in up/up modus
- De snelheid van de seriele verbinding met de CSU / DSU wordt aangepast naar de snelheid van de CSU / DSU. De CSU / DSU is hier dus de master en bepaald de snelheid. Dit automatisch aanpassen noemen we “clocking”. De CSU / DSU zend deze clock pulses over de kabel.

Iedere interface heeft een bepaalde status welke opgevraagd kan worden met het commando:

#show ip interface brief

Dit commando laat je 2 eigenschappen zien van de interface

- (Line) Status (layer1)
- Protocol (status) (layer2)

De volgende combinaties zijn mogelijk:

Line Status	**Protocol Status**	**Interface Status**	**Info**
Administratively Down	Down	Disabled	Configured Shutdown
Down	Down	NotConnect	Layer 1 issue of geen / slechte kabel
Up	Down	NotConnect	Data Link Layer (2) probleem zoals configuratie problemen
Up	Up	Connected	Up

Routetabel

Het toevoegen van routes aan een routetabel kan op 3 manieren geschieden:

- Connected (Cisco kent de routes naar subnets waarmee hij succesvol verbonden is)
- Statisch (handmatige invoer)
- Routing Protocols (automatisch middels een routing protocol)

Routing in VLAN's + Trunking

Een router kan en zal het verkeer tussen VLAN's routeren. Hiervoor moet de router een ip adres hebben in elk subnet van de VLAN's. Cisco gebruikt hiervoor "subinterfaces". Dit zijn virtuele interfaces op de trunk poort (1 fysieke poort).

Routers initiëren nooit trunking. Trunking moet altijd enabled worden op de router om trunking toe te staan.

Om trunking (802.1Q) toe te staan moet je:

- Een (unieke) subinterface maken in ieder subnet van de VLAN's die over de lijn gaan
- Activeer het trunking protocol op de subinterface (encapsulation dot1q %vlan id%)

Statische routes worden door de router verwijderd als de interface offline gaat maar worden weer toegevoegd als de interface online komt. Om het verwijderen tegen te gaan kun je een statische route toevoegen met het commando "permanent".

Als routers geen route hebben in hun routing table voor het pakketje wordt het pakketje verwijderd. Ook een router kan een "default gateway" ofwel "default route" hebben. Wanneer het pakketje niet matched wordt het over deze route naar buiten gerouteerd. Deze router wordt aangegeven in de routing table als de 0-route (0.0.0.0/0) = IP + Mask = 0. Deze route kan statisch aangemaakt worden of dynamisch wanneer routing protocollen gebruikt worden. Een router kan meerdere default routes kennen. De gebruikte default route wordt aangegeven in de "show ip route" als "Gateway of last resort". Alle overige kandidaat default routes worden aangeven met een * ervoor.

Zero subnet

Het "zero" subnet is een subnet binnen elk classfull IP waarbij het toegestaan is om alle subnet binary nummers op 0 of 1 te zetten. Vroeger was dit standaard niet mogelijk (kon voor problemen zorgen). Tegenwoordig is subnet zero standaard geactiveerd.

Stel je het volgende class A netwerk voor:

10.0.0.0/10

Class A heeft normaliter 8 bits voor het subnet (netwerk ID) maar leent er nog 2 van het hosts gedeelte om subnetten te maken. De volgende subnetten zijn mogelijk:

50.00 000000.x.x
50.01 000000.x.x
50.10 000000.x.x
50.11 000000.x.x

Als subnet zero actief is mogen er geen IP adressen aangemaakt worden in de subnetten die uit volledig nullen en enen bestaan.

50.00 000000.00000000.11000000 = 50.0.0.192 - Mag niet!
50.01 000000.00000000.11000000 = 50.64.0.192 Mag wel!

Zero subnet activeren:	()ip subnet zero
Zero subnet deactiveren:	()no ip subnet zero

Als het zero subnet uitgeschakeld wordt dan moeten alle IP adressen voldoen aan de regel "IP adressen in subnets met allemaal nullen en enen mogen niet voorkomen"

Routing protocollen

Routing protocollen verzorgen de volgende functies:

- Leren route informatie (naar IP subnets) van neighbor routers (connected routers)
- Adverteren route informatie naar neighbor routers
- Als meerdere routes naar een subnet bestaan kies dan de beste route
- Als de netwerk toplologie veranderd (b.v. een link gaat down) reageer hierop en adverteer dat sommige routes gefaald zijn en kies een nieuw optimaal pad naar de subnets (dit proces heet "convergence")

Er zijn 2 groepen routing protocollen:
IGP's = Interior Gateway Protocols: voor gebruik binnen 1 autonoom systeem (AS). Een AS is een netwerk welke in beheer valt van 1 organisatie zoals b.v. een kantoor of school.
EGP's = Exterior Gateway Protocols: voor gebruik binnen verschillende autonome systemen. Dus binnen verschillende netwerken van verschillende organisaties.

Routing protocol algoritmes
Er zijn verschillende routing algoritmes die door routing protocollen gebruikt worden:

- Distance Vector (ofwel Bellman-Ford)
- Advanced Distance Vector (ofwel Balanced Hybrid)
- Link State

Distance Vector protocollen

- RIP (Routing Information Protocol) – IGRP (Interior Gateway Routing Protocol)
- Vanuit historisch oogpunt gebruikt door de eerste routing protocollen

Distance Vector staat voor wat de router weet van de route op het moment dat deze berekend is, namelijk de afstand (metric) en de outgoing interface en next-hop router (de direction ofwel vector). Om de distance metric te berekenen gebruikt EIGRP de waardes van de link bandwidth en de delay. Distance Vector routers wisselen onderling update berichten uit. Deze noemen ze "update messages" (OSPF noemt ze LSU). Oude routing protocollen zoals RIP gebruiken de update messages om hun router informatie te publishen en om te kijken of de neighbor nog online is. EIGRP gebruikt hiervoor net als OSPF een proces van helo berichten. Na het niet ontvangen van x helo berichten wordt de neighbor "offline" verklaard.

OSPF en EIGRP verzenden periodiek hun route informatie maar vragen eerst of deze werkelijk nodig is. Oudere protocollen zoals RIP adverteren elke 30 sec. de gehele routetabel met uitzondering van de routes die de eigen interface als "outgoing interface" hebben staan. Deze routes worden niet meegezonden omdat deze waarschijnlijk ook geleerd zijn via deze interface / connectie. Dit proces noemen we "split horizon".

Een methode die door Distance Vector protocollen gebruikt wordt om ervoor te zorgen dat er geen routing loops ontstaan is "Route Poisoning". Route Poisoning zorgt ervoor dat de routers zo snel mogelijk geupdate worden als een route offline gaat. Dit gebeurt middels een speciale "infinity" metric met een waarde van 16 (voor RIP). Als er een infinity metric ontvangen wordt zal de ontvangende router deze route meteen verwijderen of als "onbruikbaar" markeren.

Advanced Distance Vector protocollen

- EIGRP (Enhanced Interior Gateway Routing Protocol) = Cisco only

Link State protocollen

- OSPF (Open Shortest Path First) – IS-IS (Intergraded Intermediate System to Intermediate System)
- Informatie publiceren naar andere routers heet “flooding”

Metric
Routing protocollen gebruiken verschillende manieren om hun route te berekenen. Deze worden aangegeven als de “metric”. Er zijn:

- **Hop count** (het aantal tussenliggende routers / hops)
- **Cost** (een interface heeft een waarde / cost op basis van de snelheid, duplex etc. De Cost metric telt alle waardes van tussenliggende interfaces op en berekend per route een totaal cost
- **Composite of Bandwidth & Delay** (gebaseerd op de traagste link van een route en de vertraging (delay) tussen iedere interface op de route

Classfull of Classless routing protocollen
Routing protocollen kunnen classfull of classless zijn. Classless routing protocollen ondersteunen VLSM (Variable Length Subnet Mask) en dus classless subnets. Classfull routing protocollen sturen geen subnet mee in hun advertisements en ondersteunen dus ook geen afwijkende subnetten of VLSM.

Administrative Distance
Routes in de routetabel hebben allemaal een “administrative distance”. Dit is een waarde die aan de route gegeven wordt n.a.v. de manier waarop hij in de routetabel gekomen is. Hoe lager de waarde des te geloofwaardiger de route. Een paar waardes:

- Connected (interne interface): 0
- Statische route: 1
- BGP (externe routes): 20
- EIGRP (interne routes): 90
- OSPF: 110
- RIP: 120
- EIGRP (externe routes): 170
- BGP (interne routes) 200

Als een router 3 routes heeft naar een subnet en hij heeft deze geleerd via OSPF, EIGRP en een statische route dan zal de router de statische route gebruiken omdat deze een lagere “administrative distance” heeft.

De “administrative distance” is ook aan te passen. Zo kun je een statische route toevoegen met de administrative distance van 210 door de administratvice distance achter het commando te voegen:
()ip route 192.168.1.0 255.255.255.0 192.168.10.254 **210**

RIP - Routing Information Protocol

- Metric: hop count
- Classfull
- Algoritme: Distance Vector
- Ondersteuning voor :manual summarization: Nee
- Routing updates verzonden naar multicast IP: Nee
- Convergence: Traag
- Vendor onafhankelijk

RIP-2 - Routing Information Protocol version 2

- Metric: hop count
- Classless
- Algoritme: Distance Vector
- Ondersteuning voor :manual summarization: Ja
- Routing updates verzonden naar multicast IP: Ja
- Convergence: Traag
- Vendor onafhankelijk

OSPFv2 Open Shortest Path First version 2

- Metric: cost
- Classless
- Algoritme: Link State
- Ondersteuning voor manual summarization: Ja
- Routing updates verzonden naar multicast IP: Ja
- Convergence: Snel
- Vendor onafhankelijk

LSA: Link State Advertisements & LSDB: Link State DataBase
De topologie die OFPF opbouwt wordt opgebouwd met behulp van LSA (Link State Advertisements). LSA's zijn typologieën van het netwerk zoals deze in de LSDB zitten van de router. Deze typologieën worden verzonden met LSU (Link-State Update) pakketjes. De LSA topologie wordt opgeslagen in de LSDB (Link State DataBase) als deze nog niet aanwezig was. Iedere OSPF router adverteert zijn eigen LSA naar andere verbonden OSPF routers (in hetzelfde VLAN). De eigen LSA bestaat uit informatie van zijn eigen hardware, subnets en snelheden. LSA's worden opnieuw geflood als er informatie veranderd (er gaat b.v. een link down). LSA's hebben een nummer. Alvorens het pakket geflood wordt er aan de ontvangende router gevraagd of ze al over het pakket beschikken. Zo ja, dan wordt het pakket niet verder geflood.

De LSDB alleen zorgt niet voor de beste routes in de routetabel. Hiervoor is rekenwerk nodig. Dit gebeurt door het Dijkstra SPF algoritme. Dit algoritme brekend alle mogelijke routes. Elke interface op de route heeft een "cost" waarde. Hoe lager de uiteindelijke "cost" waarde is des te beter / sneller de route is. De laagste "cost" waarde (metric) wordt de beste route en wordt toegevoegd aan de routing tabel. De cost van een interface kan ook door de administrator beinvloed worden. Dit klan op 2 manieren:

- De cost vast in te stellen op een interface (-)ip ospf cost 10

- De cost door IOS middels een formule laten berekenen maar wel de input van de formule zelf bepalen

Optie 2 werkt door de default OSPF cost formule te manipuleren. Deze formule is als volgt:
reference_bandwidth / interface_bandwidth

Deze waardes kun je handmatig manipuleren. Zo kun je op de interface een bandwidth waarde opgeven (dit heeft geen invloed op de werkelijke snelheid). Dit doe je door het commando:
(-)bandwidth %snelheid in Kbps%

Je kunt ook de referentie bandbreedte aanpassen (van toepassing op alle OSPF interfaces). Dit kun je doen door voor de cost berekening en is ook nodig als je een snellere verbinding hebt dan 100Mbps. De default waarde is namelijk 100Mbps wat resulteert in OSPF cost 1. Ook snellere lijnen zouden eindigen met 1 (1000 Mbps zou niet 0,1 maar ook 1 worden omdat 1 het laagste is):
()router ospf 1
(-)auto-cost reference-bandwidth %snelheid in Mbps%

Stel je voor dat je 2 lijnen hebt met beide een 1 Gbps (1.000.000 Kbps) verbinding. Beide zouden een cost van 1 krijgen (1000000 / 100000). Als lijn A de preferred interface moet worden dan veranderen we eerst de default speed op lijn A en B

LijnA
(-)bandwidth 1000000

LijnB
(-)bandwidth 500000

Vervolgens veranderen we de referentie bandbreedte:
(-)auto-cost reference-bandwidth 1000

Dat resulteert in onderstaande plaatje waarbij lijn A de preferred lijn wordt.

LijnA
1000000 / 1000000 = 1

LijnB
1000000 / 500000 = 2

Als een route aan de tabel wordt toegevoegd middels OSPF dan krijgt deze een administrative distance van 110. Een static route in de routetabel zal een metric van 1 krijgen en dus gebruikt worden om naar de destination te gaan. Verschillende metrics zijn:

- Connected (interne interface): 0
- Statische route: 1
- BGP (externe routes): 20
- EIGRP (interne routes): 90
- OSPF: 110
- RIP: 120
- EIGRP (externe routes): 170
- BGP (interne routes) 200

Er zijn verschillende type LSA, zeker wanneer OSP in verschillende area's gebruikt wordt. Dan hebben we:

- Type 1 - Router LSA – Gewone LSA die de router beschrijft
- Type 2 - Network LSA – LSA verzonden door DR welke het netwerk beschrijft en wie de DR en BDR zijn. Dit is het netwerk tussen 2 routers binnen een area
- Type 3 - Summary LSA – LSA die een subnet in een ander area omschrijft (subnet ID, mask en RID van de ABR (area border router) die de LSA verzend)

Router ID – RID
Elke router die OFPF draait moet voorzien zijn van een RID (Router ID). Dit router ID is 32 bits lang en meestal weergegeven als decimale nummers gebaseerd en lijkende op hun IP adres. Het Router ID kan ook handmatig geconfigureerd worden). Het RID wordt als volgt gekozen:

- Als Router ID handmatig is toegevoegd, dan die gebruiken
- Als er een loopback interface een IP geconfigureerd is en de interface is up/up dan selecteert de router het hoogste IP nummer van alle loopback interfaces als RID
- Als er geen loopback interface is dan selecteert de router het hoogste IP van alle up/up interfaces als RID

Loopback interface
Een router kan voorzien zijn van een loopback interface. Een loopback interface is een virtuele interface welke voorzien is van een IP adres. Deze loopback interface kan gebruikt worden voor administrative toegang of monitoring taken. Een loopback interface is altijd in up/up modus en daarom ideaal voor OSPF

OSPF pakketjes:

- Helo
    - Lists het Router ID – RID
    - Regulier verzonden naar multicast ip: 224.0.0.5
    - Laat weten wie je bent om te berekenen of je "neightbours" moet worden. Zo zullen b.v. OSPF routers alleen neighbors worden als ze in hetzelfde subnet zitten.

Als er geen routers aangesloten zijn op een interface dan is het niet nodig om hier helo pakketjes naartoe te sturen en bandbreedte en processorkracht hieraan te verspillen. De engineer kan dan de interface passief (ongebruikt) maken voor OSPF. Dit doet hij met het commando:

()router ospf 1
(-)passive-interface gigabitethernet0/0.10

De helo pakketjes zorgen ervoor dat de routers van elkaar weten wie ze zijn en of ze neighbours kunnen worden om hun LSDB uit te wisselen. Het proces is als volgt (ExStart – Exchange – Loading – Full):

Status router 1	**Type pakket**	**Type pakket**	**Status router 2**
Null	Helo ->		**Init** (weet wie 1 is)
2-way (weet wie 2 is en dat ze neighbors mogen worden)		<- Helo	Init
2-way	Helo ->		**2-way** (weet wie 1 is en dat ze neighbors mogen worden)

ExStart (Dit is mijn database. Heb je deze info en wil je starten met uitwisselen LSDB info middels LSA's in LSU pakketjes)?	->		
		<-	**Exchange** (Jazeker, laten we uitwisselen, dit is mijn database)
Loading (vergelijk LSA's en werk LSDB bij waar nodig)	->	<-	**Loading** (vergelijk LSA's en werk LSDB bij waar nodig)
Full (compleet up-to-date)			**Full** (compleet up-to-date)

In ethernet LAN's zullen sommige routers nooit de full status krijgen maar maximaal de 2-way status (dat ze neighbors zijn). In deze netwerken (vaak met meerdere OSPF routers) zitten 2 belangrijke routers:

- DR – Designated Router
- BDR – Backup Designated Router

De DR en BDR synchroniseren hun database met elkaar en met andere routers en kunnen dus een "full" status halen. Andere routers (DRO / DROthers) synchroniseren hun database niet met andere routers waardoor ze maximaal een "2-way" status met die neighbor (andere DRO) kunnen hebben. De BDR neemt het over van de DR als deze faalt en wordt dan de nieuwe DR en kiest weer een andere BDR.

OSPF maintenance tasks & Timers:
OSPF kent verschillende taken zodat de topologie up-to-date blijft. Deze zijn:

- Maintaining Neighbor State – Dit wordt gedaan middels 2 verschillende timers:
    - Helo Interval (hoe vaak worden helo pakketjes verzonden om te kijken of alles nog up-to-date is)
    - Dead Interval (de tijd dat er geen helo pakketjes ontvangen zijn (standaard 4 helo pakketjes) en dat de neighbor dus als offline wordt beschouwd
- Flood changed LSA's naar iedere neightbor
- Reflood onveranderde LSA's als de lifetime voorbij is (standaard 30 min). Flood eerst pakket nummer / timestamp en als de LSA echt opnieuw nodig is wordt deze verzonden

OSPF area's:
OSPF kan geconfigureerd worden om alleen topologie informatie te verwerken van zijn eigen area. In een groot netwerk waarbij OSPF netwerken opgedeeld zijn in verschillende area's kan dit de OSPF routers veel calculatie / processorkracht besparen!

OSPF Network Parameter:
Met de OSPF network parameter kun je OSPF activeren op meerdere interfaces. Dit activeren doe je middels een wildcard. De wildcard is gebaseerd op de octetten. Het commando ziet er als volgt uit:

(-)network %Subnet ID% % Wildcard% area 0

Bijvoorbeeld:

(-)network 192.168.99.0 0.0.0.255 area 0

De wildcard is: 0.0.0.255. Een 0 in de wildcard is het octet dat overeen moet komen en de 255 in de wildcard is het octet dat onbelangrijk is.

OSPF wordt in bovenstaande voorbeeld geactiveerd op alle interfaces die beginnen met: 192.168.99.x

De wildcard 0.0.0.0 betekend een match van het exacte IP adres (compleet) en 255.255.255.255 betekend “vergelijk niets” dus alle interfaces matchen aan deze wildcard. Je kunt ook met andere getallen werken die betekenen “tot en met”. 192.168.150.0 0.0.0.3 betekend dat 3 adressen matchen, namelijk:

192.168.150.0
192.168.150.1
192.168.150.2

OSPFv3 Open Shortest Path First version 3 (for IPv6)

OSPFv3 is vrijwel (qua opzet en configuratie) gelijk aan OSPFv2. Het grootste verschil zit hem in de interne werking en configuratie. Configuratie begint met de volgende stappen:

```
>enable
#configure router
()Ipv6 unicast routing                    <- Activeer IPv6 routeringen
()ipv6 router ospf 2                      <- Schakel uniek OSPFv3 ID in
(-)router-id 2.2.2.2                      <- Stel RID in
(-)exit
()interface gigabitethernet0/0
(-)mac-address 0200.0000.0002             <- Stel MAC in van interface
(-)ipv6 address 2001:db8:1:23::2/64       <- Stel IP in van interface
(-)ipv6 ospf 2 area 23                    <- Schakel OSPF ID2 in op area 23
(-)exit
```

Om een interface passief te maken geef je deze instelling op in de OSPFv3 configuratie:

```
>enable
#configure router
()ipv6 router ospf 2                      <- ga naar OSPFv3 proces ID 2
(-)passive-interface gigabitethernet0/1
```

Interface cost

Interface cost wordt bij OSPFv3 net zo gebruikt als bij OSPF2, namelijk om de beste route te berekenen. OSPFv3 zal dus alle mogelijke routes bekijken, interface cost toekennen en de route met de laagste kosten wint en komt in de routetabel. Ook het beinvloeden van de interface cost werkt op dezelfde manieren:

- Statisch een interface cost aanmaken (-)ipv6 ospf cost x
- De bandwidth van een interface aanpassen en verbeteren voor de kostenberekening. (-) bandwidth x (Kbps)
- De referentie bandbreedte aanpassen (-)auto-cost reference-bandwidth x (Mbps)

Om OSPF configuratie te bekijken zijn verschillende show commando’s essentieel:

- Show running-config (globale stats van interfaces)
- Show ipv6 protocols (laat alle IPv6 OSPF interfaces zien, ook de passieve zonder dit te melden)
- Show ipv6 ospf interface brief (laat o.a. area info zien)
- Show ipv6 ospf interface (laat o.a. area info zien en laat als enige commando zien of een interface passief is.
- Show ipv6 ospf adj (laat zien wat er tijdens het adjacency proces gebeurt, dus het worden van neighbors)
- Show ipv6 ospf neighbors (laat neighbors en hun status zien waaronder helo en dead timers)

Alle overige zaken tussen OSPF2 en OSPF3 zijn te vergelijken. Het enige verschil is dat OSPF met IPv6 werkt. De volgende zaken zijn wel verschillend:

- De naam van de type3 LSA's
- OSPF neighbors hoeven niet in hetzelfde subnet te vallen (bij IPv4/OSPF2 wel)
- OSPF3 gebruikt nieuwe type LSA's t.o.v. OSPF2
- De details in LSA pakketjes is verschillend

De IPv6 LSA pakketjes zijn als volgt:

- Type 1 - Router LSA – Gewone LSA die de router beschrijft
- Type 2 - Network LSA – LSA verzonden door DR welke het netwerk beschrijft en wie de DR en BDR zijn. Dit is het netwerk tussen 2 routers binnen een area
- Type 3 - Summary LSA – LSA die een subnet in een ander area omschrijft (subnet ID, mask en RID van de ABR (area border router) die de LSA verzend)

OSPF3 gebruik link-local adressen voor het vormen van routing adjecencies

EIGRP - Enhanced Interior Gateway Routing Protocol

- Metric: combinatie van bandbreedte en delay
- Classless
- Algoritme: Advanced Distance Vector
- Ondersteuning voor :manual summarization: Ja
- Routing updates verzonden naar multicast IP: Ja
- Convergence: Snel
- Cisco proprietary

EIGRP is een distance vector protocol maar doet veel dingen een stuk beter en geavanceerder dan RIP en doet sommige dingen ook compleet anders. Sommige mensen zeggen dat RIP een uniek hybride protocol is i.p.v. een distance vector protocol.

De dingen die EIGRP anders doet is b.v.:

- Adverteert iedere route slechts 1x (om deze te leren)
- Verzend gedeeltelijke updates als er iets veranderd (nieuwe of gefaalde routes)

Tijdens de configuratie van EIGRP gebruik je een AS nummer (Autonomous System number). Dit nummer functioneert als de "area" bij OSPF. Dus om routers van eenzelfde verantwoordelijkheid voor het netwerk met elkaar te laten praten. Als deze EIGRP routers moeten dus hetzelfde AS nummer hanteren.

Omdat EIGRP geen periodieke updates stuurt verstuurd EIGRP periodieke helo berichten om te kijken of zijn neighbors nog online zijn. Iedere EIGRP router gebruikt zijn eigen “time” & “hold” interval voor de helo pakketjes.

- Time Interval – Elke X aantal seconde van de time interval worden de helo pakketjes verstuurd (standaard = 5 seconde)
- Hold Interval – Het aantal helo berichten dat gemist mag worden alvorens de router als “offline” gezien wordt (standaard = 15 seconde = 3x helo)

Neighbors
Het proces om een neighbor te vinden gaat als volgt.

1. Helo pakketjes worden gestuurd naar 224.0.0.10
2. Een router die dit helo pakket ontvangt controleert de volgende voorwaarden:
    a. Kan de router zich authentiseren (als dit is ingeschakeld)
    b. Moet beschikken over hetzelfde ID nummer (Autonomous System Number / ASN). De ASN kan lopen van 1 tot 65.535
    c. Moet in hetzelfde subnet zitten als de local router interface
3. Alles alle voorwaarden akkoord zijn werander EIGRP zijn state naar “working” state en zijn de router EIGRP neighbors. Nu kunnen de routers hun routing topology en update messages uitwisselen. Het uitwisselen van deze pakketten gaat als volgt:
    a. Router verzend update messages naar een unicast adres (als er 1 EIGRP neighbor router is) of naar een multicast adres (als er meerdere EIGRP neighbors zijn).
    b. Update messages worden gestuurd middels het RTP (Reliable Transport Protocol) welke EIGRP berichten kan opnieuw verzenden als deze door een neightbor gemist zijn.
    c. Nieuwe neighbors krijgen een volledige (full) update van de topologie
    d. Bestaande neighbors krijgen een incrementele update (partial update)

Bij EIGRP wordt de beste route berekend door een formule toe te passen. De default formule (dus als er geen andere waardes toegevoegd worden aan de formule wat wel mogelijk is) gebruikt dfe bandwidth & delay en is als volgt:

$$\left(\frac{10.0000000}{\text{Least Bandwidth}} + \text{Cumulative Delay}\right) * 256$$

De volgende defaults zijn handig om te weten tijdens het berekenen van de formule:

	Bandwidth	**Delay (microseconds)**
Serial	1544	20.000
Gigabit - 1000 Mbps	100000	10
100 Mbps	10000	100
10 Mbps	1000	1000

EIGRP Successor, Feasible successor & DUAL
EIGRP berekend voor elke route naar een subnet de beste route. De beste route naar een subnet noemen we de “successor”. Deze route zal in de routetabel geplaatst worden. De metric voor deze route noemen we ook wel de “feasible distance” (FD). Als EIGRP 2 routes vindt met eenzelfde FD dan worden deze routes beide successor routes en wordt “Equal-Cost Load Balancing” toegepast om het

netwerkverkeer over deze routes te verdelen. Beide routes worden dan aan de topologie en routetabel toegevoegd. Standaard kunnen er 4 load balancing routes zijn maar dat aantal kan veranderd worden met het commando (-)maximum-paths %number%.

Omdat het echter zelden voorkomt dat EIGRP voor 2 routes exact dezelfde metric berekend en dus meerdere successor routes toevoegt kent EIGRP ook de functie “Unequal-Cost Load Balancing” ofwel “Variance”. Met Variance kiest EIGRP waardes die dicht bij elkaar liggen om toe te voegen als load balancing routes aan de route tabel. Variance werkt met een multiplier van 1-128. De multiplier vermenigvuldigd dan de router FD van de successor route. Stel je voor dat de succerssor route een FD van 50 heeft, Route 2 van 90 en Route 3 van 120. Een variance van 1 = 1x50. Alleen de successor route wordt toegevoegd. Een variance van 2 = 2*50=100. Nu wordt elke route toegevoegd met een metric van 100 en lager (dus ook Route 2). Route 3 met een waarde van 120 wordt nog niet toegevoegd. Met een variance van 3 (150) zou route 3 toegevoegd kunnen worden. Als deze route echter niet een FS (feasible successor) route is dan wordt deze niet toegevoegd aan de load balancing group omdat er dan routing loops kunnen ontstaan.

Als men de EIGRP topologie opvraagt (#shop ip eigrp topology) dan zie je per netwerk 2 regels.

Op de eerste regel staat vermeld hoeveel successor routes er voor dat netwerk zijn en wat de feasible distance (FD) is. De volgende regeld vermelden de routes (met het woord via). De route met de feasible distance is de successor route. De route met een lagere reported distance (RD) dan de FD van de successor route is de feasible successor route. De FD en RD staan achter elkaar vermeld als (1236612/9945877). Het eerste getal (1236612) is de FD (ofwel metric) en het 2^{e} getal (9945877) is de RD.

EIGRP berekend ook een loopvrije backup route voor als de successor route faalt. Deze route bewaard hij in zijn topologie tabel en noemen we de “feasible successor”. Als de successor route en feasible successor route falen dan gebruikt EIGP een ander protocol om de route te bepalen. Dit protocol heet DUAL (Diffusing Update Algorithm). DUAL maakt gebruik van queries en replies en zal dus langer duren alvorens DUAL een goede backup route gevonden heeft.

EIGRP Autosummarization & Discontiguous Networks

Een probleem waar veel oudere routers en routing protocollen last van hebben is autosummarization & discontiguous networks. Dit gebeurt vooral bij border routers tussen Class X en Class Y. Met autosummarization worden alle netwerken samengevoegd in 1 regel. Ook een EIGRP kan autosummarization aan gezet worden. Een router die dan route 10.100.0.0 en 10.200.0.0 kent zal deze samenvoegen in 1 regel, namelijk 10.0.0.0/8. Dit is niet altijd correct. Als netwerk A via netwerk B naar netwerk C gaat en netwerk C werkt ook met een 10.300.0.0 netwerk en autosummarization waardoor hij zegt de route naar 10.0.0.0/8 te zijn dan weet netwerk B niet weer waar hij 10.0.0.0/8 naartoe moet sturen. Naar netwerk A of C? Een classfull netwerk welke pakketjes stuurt via ten minste 1 ander subnet noemen we een “discontiguous netwerk”. Bij default staat autosummarization uit als je EIGRP inschakelt. Anders kun je deze uitschakelen met “(-)no auto-summarization”.

Access Controll Lists - ACL

- 2 typen (standard & extended)
- Binnen elk type zijn 2 soorten (numbered & named)
- Standard ACL zijn alleen op basis van afzender IP (source)
- Extended ACL kunnen op basis van afzender en ontvanger IP + poorten
- Iedere interface kan slechts 2 ACL's toegewezen krijgen (1x inbound en 1x outbound)
- Regels op ACL's worden gematched v.a. de top (als een pakketje binnenkomt wordt de ACL van boven naar beneden bekeken. Matched een pakketje de regel dan wordt de actie uitgevoerd en der overige ACL genegeerd. Plaats daarom de specifieke regels bovenaan en de algemene regels onderaan de ACL.
- De laatste (onzichtbare) regel van iedere ACL is een "deny all" regel

ACL Wildcards:
ACL Wildcards zien we als volgt uit (in decimale vorm) en lijken (maar zijn geen) subnetmasks:

0.0.255.255

0	-	Match overeenkomstig octet bij IP adres
255	-	Negeer overeenkomstig octet bij IP adres

192.168.1.0 0.0.0.255 betekend dus de hele range van 192.168.1.0 tot 192.168.1.255

Je kunt het wildcard mask uitrekenen met behulp van het subnetmask. Hiervoor gebruik je de formule:

255.255.255.255 – subnetmask = wildcard mask

Dus 192.168.1.5 met subnetmask 255.255.255.0 zou matchen op wildcard mask:
255.255.255.255
255.255.255.0
_____-
0.0.0.255

Een wildcard mask welke voldoet aan alle regels is gewoon "any" (geen nummer).

Standard numbered ACL:
Plaats standard ACL's altijd zo dicht mogelijk bij de bestemming (destination) zodat het verkeer niet te vroeg tegengehouden wordt.

Deze kennen de volgende nummers:

1-99	-	Standard numbered
100-199	-	Extended numbered
1300-1999	-	Additional standard numbered
2000-2699	-	Additional extended numbered

Een standard numbered commando is een global config commando en ziet er als volgt uit:

access-list | ID | Actie (permit / deny) | Source IP | Wildcard
()access-list 1 permit 192.168.1.0 0.0.0.255

Extended numbered ACL:
Dit type ACL heeft meer opties dan een standard ACL. Bij een extended ACL kun je niet alleen filteren op source IP maar ook op destination IP en poorten. Plaats extended ACL's zo dicht mogelijk bij de afzender (source) zodat overige apparaten niet belast worden met onnodige filtering.

Een extended numbered commando is een global config commando en ziet er als volgt uit:

access-list | ID | Actie (permit / deny) | protocol | Source IP + Wildcard | Destination IP + Wildcard
()access-list 101 permit tcp 192.168.1.0 0.0.0.255 any

Let op: als je 1 specifieke host wilt gebruiken dan moet bij een extended ACL altijd het voorvoegsel "host" gebruikt worden. Dus:

()access-list 101 permit tcp 192.168.1.0 0.0.0.255 **host** 192.168.2.1

Extended ACL's kunnen uitgebreid worden tot poortfiltering. Je kunt poorten specificeren op poortnummer maar ook op application name (dit kan alleen met alle well known poorten / applicaties). Eveneens kun je een range aangeven met "greater than" = "gt" en "lower than" = "lt". Een exacte poort wordt aangegeven met eq (equal). De poorten worden achter de IP + Wildcards gezet. Dus:

()access-list 102 deny tcp host 192.168.1.1 gt 1023 192.168.2.0 0.0.0.255 gt 0

Bovenstaande regel blokkeert al het verkeer van poorten boven 1023 van host 192.168.1.1 die gestuurd worden naar elke cliënt en poort in het 192.168.2.x netwerk.

Voor meer duidelijkheid is het handig om een opmerking toe te voegen. Dit doe je met de remark optie.

()access-list 102 remark Dit is uitleg over access-list 102

Dynamic ACL

- Dynamic ACL worden gebruikt in combinatie met een authenticatieserver zoals TACACS+ of RADIUS om de gebruiker te verifiëren en toegang te verlenen op basis van zijn credentials.

Standard + Extended Named ACL
De named ACL hebben een aantal voordelen t.o.v. de numbered ACL. Named ACL:

- Zijn gemakkelijker te onthouden
- Hebben een eigen configuratie interface (config subcommands)
- Hebben edditing features om gemakkelijker individuele regels te sorteren / verwijderen

Named ACL worden ook wel IP Access Lists genoemd. Dit komt omdat men v.a. firmware 12.3 een ACL Editing feature heeft toegevoegd. Door het nieuwe commando te gebruiken (met toevoeging van "ip") kun je de ACL's bekijken in hun eigen configuratie interface. Je kunt hier gemakkelijkers regels toevoegen, verwijderen en sorteren. Ook normale numbered ACL's kunnen met het commando "ip" toegevoegd worden om deze voordelen te benutten. Named ACL's kunnen niet zonder gebruikt worden.

()ip access-list extended Filter_FTP

Door bovenstaande commando te gebruiken is de Extended Named ACL genaamd "Filter_FTP" aangemaakt (als hij nog niet bestond) en ga je meteen in de ACL configuratiemodus.

Het toevoegen van een regel in de ACL config heeft de volgende opbouw:

Actie (permit / deny) | protocol | Source IP + Wildcard | Destination IP + Wildcard

Verder zijn dezelfde regels (m.b.t. protocollen e.d.) van toepassing zoals bij de Extended Numbered ACL.

ACL Editing
Vanaf firmwareversie 12.3 heeft Cisco een ACL editing feature om zowel named als numbered ACL's te editten. Dit betekend dat we regels kunnen verplaatsen of verwijderen.

Edit numbered ACL:

()ip access-list 24	<- Enter (of maak) ACL 24
(-)do show ip access-list 24	<- Laat de sequence numbers zien van de individuele lijnen
(-)no 20	<- Verwijder lijn / regel 20
(-)20 deny 192.168.1.1	<- Voeg een nieuwe lijn toe op positie 20

ACL gebruiken op virtuele poorten (telnet en SSH)

Ook op de VTY lijnen kunnen access-lists geplaatst worden. Dit doe je door het "access-class" commando te gebruiken:

()line vty 0 4
(-)login
(-)password %wachtwoord%
(-)access-class 1 in

"access-class 1" refereert aan de regels in ACL ID 1. "in" staat voor "incomming", dus van buiten naar binnen. En "out" staat voor "outgoing" dus van binnen naar buiten.

EIGRPv6

Net zoals bij OSPFv3 is EIGRP6 erg vergelijkbaar met EIGRP4.

Een EIGRP6 configuratie gaat als volgt (let op, de enige toevoeging voor EIGRP6 is "ipv6"):

Activeer EIGRP6 op seriele interface:

>enable	
#configure terminal	
()ipv6 router eigrp 1	<- Start EIGRP proces met Autonomous System Nr
(-)eigrp router-id 1.1.1.1	<- Stel routerID in (optioneel)
(-)exit	
()interface serial 0/0/0	
(-)ipv6 address 2001:db8:1:2::2/64	<- Stel seriële interface in met een IPv6 adres
(-)clock rate 64000	<- Verkregen van CSU
(-)bandwidth 64	<- Verkregen van CSU
(-)no shutdown	
(-)ipv6 eigrp 1	<- Start EIGRPv6 ASN 1 op de interface

*Let op! Het laatste commando is anders dan bij EIGRP4. Bij EIGRP4 stelde we de netwerken waarop EIGRP actief was in met het "network" command in de EIGRP configuratie. Dit commando wordt door EIGRP6 niet meer ondersteund. Nu stel je EIGRP6 in op de fysieke interface. Deze methode is vergelijkbaar met OSPF3 en voorkomt het intypen van lange IPv6 perfixes.

Network Address Translation – NAT

NAT veranderd het source IP in de header bij een outgoing pakketje en NAT veranderd de destination (in de header) bij een incomming pakketje. Dit zodat het pakketje van extern naar intern gerouteerd kan worden. Alvorens we verder gaan met NAT is het goed om te weten hoe Cisco zijn adressering benoemd:

Wat:		**Cisco benaming:**
Intern Private	=	Inside local (host met intern private IP)
Intern Private met mapped public address	=	Inside Global
Externe host	=	Outside Global
Externe host met IP aangepast door NAT	=	Outside Local

Binnen een Cisco apparaat werk je met “inside local” en “inside global” adressen.

Er zijn verschillende soorten NAT:

Static NAT:

- Mapt 1 intern IP adres aan 1 extern IP adres (hoor elke interne host is een extern IP adres nodig)

Dynamic NAT:

- Gebruikt een pool met “Inside Global” (geregistreerde publieke IP adressen voor NAT) addressen om deze dynamisch uit te delen

Port Address Translation – PAT (ofwel NAT Overload Feature):

- Beste NAT methode
- Veranderd in de header het inside local naar het inside global address + unieke poort
- Maar 1 extern IP nodig (poort nummer veld in header is 16 bits en dus zijn er 65000 mogelijke poorten. In theorie dus 65000 gelijktijdige cliënts die van PAT naar het internet kunnen routeren)

First Hop Routing Protocol – FHRP

FHRP wordt gebruikt om een redundante gateway te creëren zodat bij uitval van gateway A, gateway B het overneemt zonder dat de configuratie aan de cliënt aangepast dient te worden.

- Zet routers in een failover cluster
- Routers delen een virtueel IP (welke door de hosts gebruikt wordt)
- Routers in het FHRP cluster communiceren met elkaar (o.a. om te bepalen wie de primaire router is) door FHRP berichten uit te wisselen

Er zijn 3 soorten FHRP protocols:

- HSRP – Hot Standby Routing Protocol
- VRRP – Virtual Router Redundancy Protocol
- GLBP – Gateway Load Balancing Protocol

Hot Standby Routing Protocol – HSRP

- Cisco only protocol + protocol bij voorkeur van Cisco
- Active/Standby (primaire router is actief en verricht het werk, de standby router neemt het werk over als de actieve router faalt)
- Werkt per subnet / VLAN
- Werkt middels een virtueel IP (in hetzelfde subnet als de interface / router)
- Router kan actief zijn in VLAN 1 en passief in VLAN B

Virtual Router Redundancy Protocol - VRRP

- Algemeen protocol
- Active/Standby (primaire router is actief en verricht het werk, de standby router neemt het werk over als de actieve router faalt)
- Werkt per subnet / VLAN

Gateway Load Balancing Protocol - GLBP

- Cisco only protocol
- Active/Active (Alle routers zijn actief. 1 router is de AVG = “Active Virtual Gateway”. Deze router beantwoord alle ARP requests voor het virtuele IP. Deze beantwoord hij soms met het virtuele MAC adres van router A en soms met het virtuele MAC adres van router B. Zo wordt het verkeer verdeeld / load balancing.)
- Werkt per host
- Alle routers hebben een virtueel IP en een virtueel MAC adres.
- Supports clear-tekst + MD5 authenticatie tussen GLBP leden
- Load balancing van traffic
- Supports 1024 virtual routers

Virtual Private Networks - VPN

VPN verbindingen maken het mogelijk om op een veilige methode met een site te verbinden, of om een site aan een andere site te koppelen over een onveilig netwerk (meestal het internet). VPN komt voor op laag 2 en laag 3 van het OSI model. VPN zorgt voor:

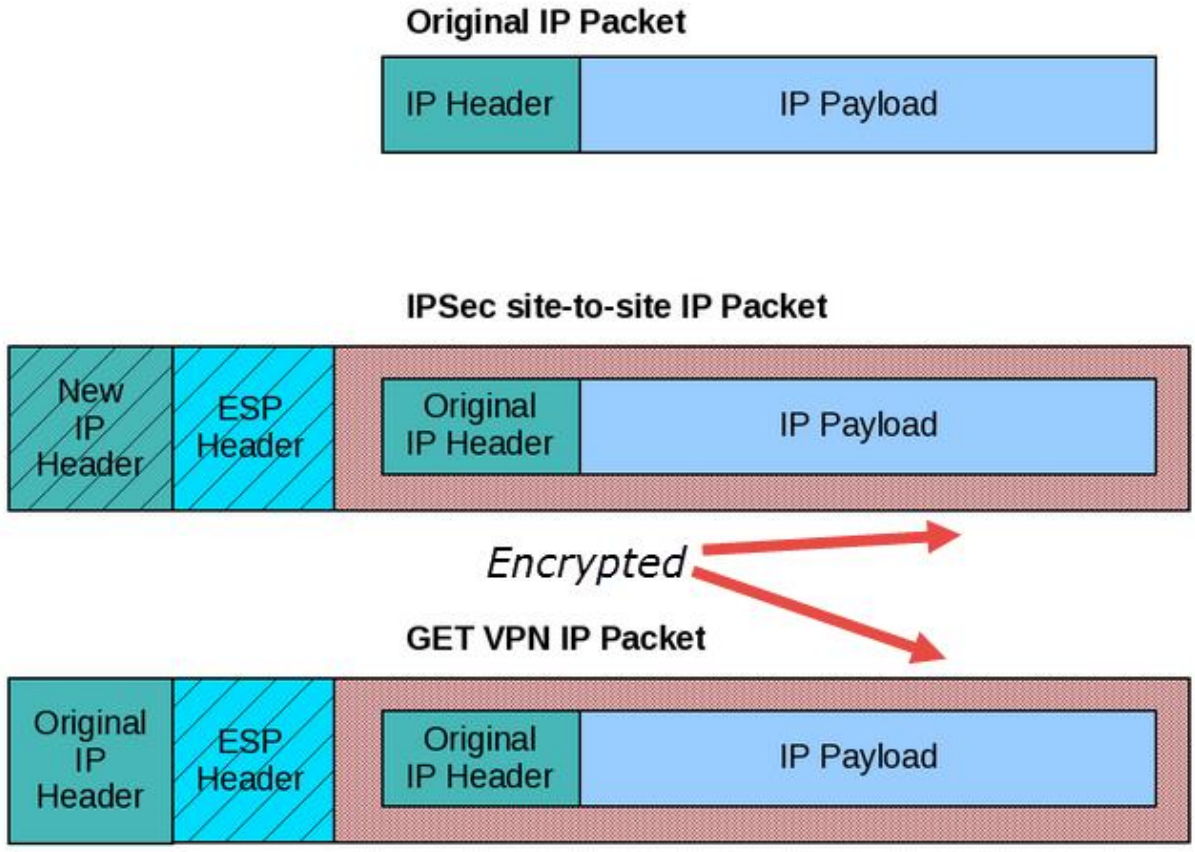
- Privacy (encryptie)
- Authentication
- Data Integrity (data niet gemodificeerd)
- Anti-Replay (data kan niet “opgenomen” worden en later worden “afgespeeld” om de beveiliging te omzeilen. Hackers gebruiken deze methode om data “op te pakken”, te modificeren en vervolgens weer door te sturen naar de host.

We kennen 2 type VPN verbindingen:

- Remote Access VPN (1host-to-1host)
- Site-to-Site Intranet VPN (1site-to-1site)

Een 3e type VPN is een Extranet VPN. Dit is ook een site-to-site VPN maar dan niet naar een eigen site maar naar een site van een externe partij (b.v. leverancier).

VPN pakket:
Over het algemeen zal een VPN pakket het originele pakket inpakken en encrypten (encapsulation) en zijn eigen IP header en VPN header toevoegen.



Protocollen
IPsec (Internet Protocol Security):
IPsec is het bijna altijd het voorkeursprotocol om een VPN tunnel te maken. IPsec bestaat uit meerdere cryptografische protocollen en functioneert op laag 3. Voor de versleuteling moeten beide partijen over de juiste sleutels en/of certificaten beschikken. IPsec biedt echter geen goede ondersteuning voor gebruikersauthenticatie en protocolroutering.

GRE (Generic Routing Encapsulation):
GRE is een Cisco tunnelprotocol welke voornamelijk gebruikt wordt voor site-to-site VPN verbindingen maar welke ook gebruikt kan worden voor remote access verbindingen (in combinatie met PPTP).

SSL/TLS:
SSL/TLS kan gebruikt worden om een VPN verbinding te maken maar is niet een veelgebruikte optie. Een bekend softwarepakket die deze optie wel gebruikt is OpenVPN. SSL/TLS verbindingen zijn niet ontzettend veilig maar kan versleuteld worden met AES waardoor de connectie wel ontzettend veilig is. Ook de snelheid is prima.

L2TP/IPsec:
L2TP/IPsec is een zeer goede en krachtige combinatie voor het opzetten van een veilige tunnel. L2TP

is de opvolger van L2F van Cisco en is een laag 2 protocol. Omdat L2TP geen sterke beveiliging biedt is de combinatie met IPsec een goede en krachtige oplossing. L2TP/IPsec kan gebruikt worden voor encryptie, integriteit, gebruikersauthenticatie en protocol routering.

Layer 4 (Transport) info

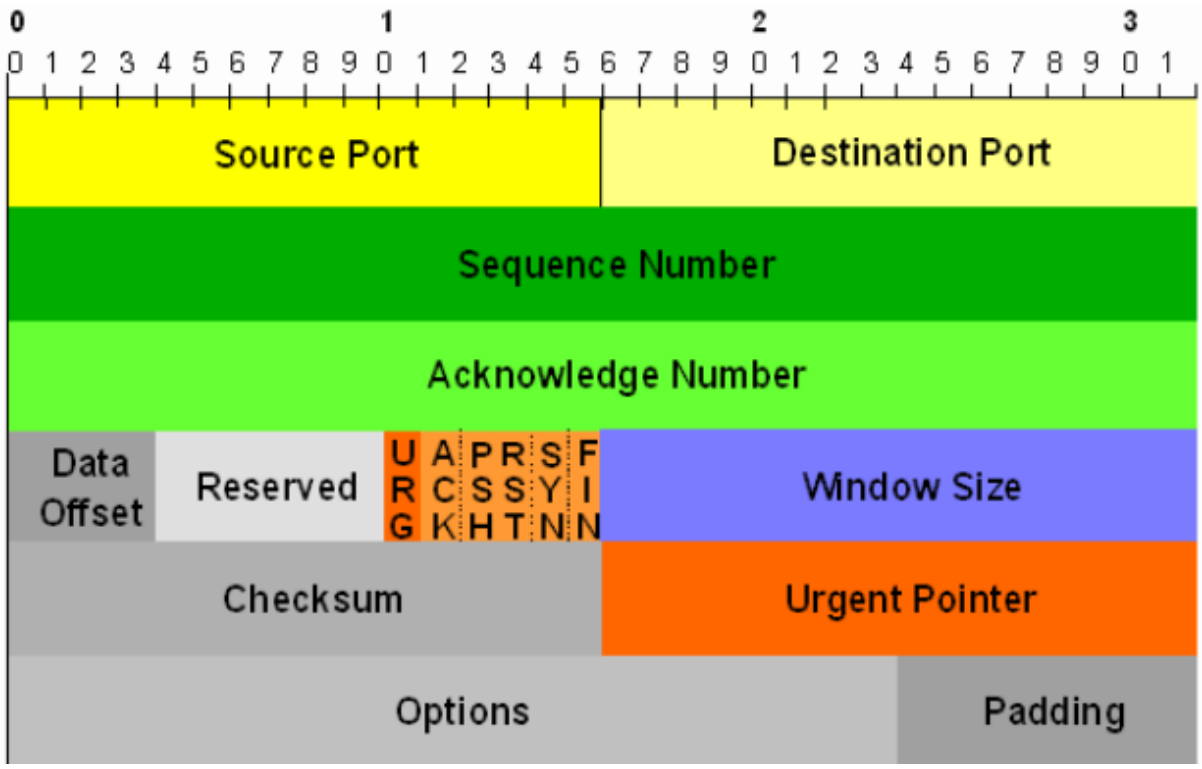
TCP - Transmission Control Protocol

- Meer services
- Meer overhead
- TCP Header + Data = TCT Segment (ofwel L4PDU)+
- Connection Oriënted Protocol (Pakketjes moeten uitgewisseld worden voor starten en afbreken connectie)

Services:

- Multiplexing using ports (applicaties toekennen aan poorten)
- Error Recovery (sequence nummers aan pakketten geven voor retransmission)
- Flow control / Windowing (bescherming van buffer door de juiste window space te hanteren)
- Connection Establishment & Termination (gecontroleerd opzetten en afbreken van verbinding)
- Ordered Data Transfer and Data Segmentation (continue stroom van opvolgende bytes.

TCP Header



UDP - User Datagram Protocol

- Minder services
- Sneller
- Connectionless protocol (om te communiceren is geen handshake nodig, dus geen overeenkomst om de transfer te starten of stoppen.

Services:

- Multiplexing using ports
- Data transfer

UDP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Length																Checksum															

Multiplexing + Sockets

TCT + UDP gebruiken “multiplexing”. Met multiplexing weet de ontvangende computer welke applicatie de data mag verwerken. TCP multiplexing gebruikt een socket. Een socket bestaat uit een IP adres, transport protocol en poortnummer.

Layer 7 (Application) info

DHCP (Dynamic Host Configuration Protocol)

DHCP kan ip adressen + bijbehorende subnet masks, default gateways en DNS servers leasen aan een cliënt. Deze cliënts hebben nog geen IP configuratie. Hiervoor zijn 2 speciale IP adressen. De DHCP server luistert op het 255.255.255.255 subnet broadcast address (routers forwarden deze pakketjes niet) en de cliënt met local IP configuration luistert op IP 0.0.0.0.

Het leasen van een IP adres van een DHCP server gebeurt via het volgende proces:

- **Discover**
  Verzonden door cliënt naar welke een DHCP server zoekt naar broadcast IP 255.255.255.255
- **Offer**
  Een DHCP server ontvangt het discover bericht en biedt een vrij IP adres + parameters aan. Deze zend hij naar 0.0.0.0.
- **Request**
  De cliënt vraagt of de server dat IP voor hem wil reserveren (naar 255.255.255.255)
- **Acknowledgement**
  De server bevestigd dat de cliënt het IP mag gebruiken en geeft het subnetmask, default router en DNS servers door (naar 0.0.0.0).

Ezelsbruggetje: De eerste letters spellen: DORA

DHCP in remote LAN
Omdat routers DHCP broadcasts (naar 255.255.255.255) niet routeren moet er iets speciaals op de router gebeuren om een cliënt in subnet A een IP adres te laten leasen van DHCP server in subnet B. Om dit de doen moet er een “IP Helper” ingesteld worden op de router. Als de IP Helper is ingesteld dan zal de router het volgende proces hanteren:

- Kijk naar inkomende DHCP broadcasts (naar 255.255.255.255)
- Verander het bron IP van het pakketje (0.0.0.0) naar het IP adres van de inkomende interface van de router (b.v. 192.168.10.1)
- Verander het destination adres van het pakketje (255.255.255.255) naar het IP adres van de DHCP server (zoals aangegeven in het IP Helper commando, b.v. 192.168.1.1)
- Routeer het pakketje naar de DHCP server
- De DHCP server ontvangt het pakketje en stuurt een Offer retour naar 192.168.10.1
- De router ontvangt de DHCP offer en realiseert zich dat deze niet voor hem bestemd is. De router veranderd het destination IP (192.168.10.1) weer naar 255.255.255.255.
- De cliënt ontvangt nu het pakketje retour

Bovenstaande proces we “DHCP Relay”.

Network Time Protocol – NTP

Het NTP protocol wordt gebruikt om de tijd en datum netjes en up-to-date weer te geven in de router en daarmee ook in alle logberichten.

Je router instellen als NTP cliënt is simpel. Je moet hiervoor het juiste IP adres (of naam als DNS goed werkt) van een NTP server hebben.

()ntp server 82.55.142.30 version 4 <- Verwijst naar NTP server en gebruikt NTP versie 4

Om NTP settings (associations) te bekijken type je:

#show ntp associations

IPv4 addressing

IPv4

- Een IPv4 adres bestaat uit 4 segmenten gescheiden door punten. Ieder segment is 1 byte (8 bits).
- Totaal 32-bits (12 decimalen)
- Meer dan 4 biljoen IP adressen mogelijk met IPv4
- Opmaak: XXX.XXX.XXX.XXX

Classfull IP adressen
Dit zijn adressen die gebruik maken van volledige subnetten (1 segment van het subnetmask is 0 of 255 en nooit anders). Binnen classfull adressen wordt het IP adres in 2 delen verdeeld, het netwerk ID (welke het subnet mask vormt) en het host gedeelte.

Classless IP adressen
Dit zijn adressen die gebruik maken van een afwijkend subnetmasker zodat IP adressen efficiënter gebruikt kunnen worden. Binnen classless adressen wordt het IP adres in 3 delen verdeeld, het netwerk ID + subnet (welke samen het subnet mask vormen) en het host gedeelte.

VLSM – Variable Length Subnet Masks
VLSM staat het gebruik toe van meerdere subnet masks in een classfull netwerk.

10.0.0.1 – 255.255.255.0
11.0..0.1 – 255.255.240.0

Bovenstaande is geen VLSM omdat beide class A adressen een ander subnetmask gebruiken. Onderstaande is wel een voorbeeld van VLSM.

172.16.4.1 – 255.255.252.0
172.16.5.1 – 255.255.255.0

Om problemen met VLSM te troubleshooten maak je een lijst van alle netwerk IP's en Broadcast IP's.

We hebben b.v. een netwerk met de volgende apparaten:

172.16.4.1/23
172.16.5.1/24
172.16.2.1/23
172.16.9.1/30
172.16.9.5/30

Dit zijn allen class B adressen. Om het subnet te bereken maken we de lijst compleet:

IP - Subnetmask	Network IP	Broadcast IP
172.16.4.1 – 255.255.254.0	172.16.4.0	172.16.5.255
172.16.5.1 – 255.255.255.0	172.16.5.0	172.16.5.255
172.16.2.1 – 255.255.254.0	172.16.2.0	172.16.3.255
172.16.9.1 – 255.255.255.252	172.16.9.0	172.16.9.3
172.16.9.5 – 255.255.255.252	172.16.9.4	172.16.9.7

De rood aangegeven adressen zijn overlappende adressen. Als een router met bovenstaande adressen in zijn routing tabel iets naar 172.16.5.10 moet sturen weet deze niet naar welk netwerk het moet. Omdat VLSM dit niet gemakkelijk laat zien is er wat rekenwerk nodig om deze problemen te ontdekken. Dit probleem heb je niet met SLSM (Static Length Subnet Mask) omdat je dan meteen aan het subnetmask ziet dat er een probleem is.

IPv4 klassen:

Class A
1.x.x.x t/m 126.x.x.x
Subnetmask: 255.x.x.x
Private use range: 10.x.x.x
126 netwerken
16.777.214 hosts per netwerk
Veel gebruikte netwerken: 8.x.x.x / 13.x.x.x / 24.x.x.x / 125.x.x.x / 126.x.x.x

Class B
128.x.x.x t/m 191.x.x.x
Subnetmask: 255.255.x.x
Private use range: 172.16.x.x
16.384 netwerken
65.534 hosts per netwerk
Veel gebruikte netwerken: 128.1.x.x / 172.20.x.x /191.191.x.x /150.0.x.x

Class C
192.x.x.x t/m 223.x.x.x
Subnetmask: 255.255.255.x
Private use range: 192.168.x.x
2.097.152 netwerken
254 hosts per netwerk
Veel gebruikte netwerken: 199.1.1.x / 192.168.1.x / 200.1.200.x / 209.209.1.x

Class D
224.x.x.x t/m 239.x.x.x
Multicast adressen

Class E
240.x.x.x t/m 255.x.x.x
Experimental

Onthouden van de classen:

1. De eerste range is t/m 127 maar 127 is gereserveerd (127.0.0.1 = b.v. loopback adres) dus class A is van 1 t/m 126
2. Het bekendste X netwerk is 192, daarvoor alles B (dus 128 t/m 191)
3. Begint bij 192 en gaat door tot BBC (B = 2 en C = 3, dus 223)
4. Het D subnet is 15 cijfers groot dus 224 t/m 239

Subnetting IPv4

Een uitleg over de omzetting van decimaal naar bits. 1 segment (XXX.XXX.XXX.[XXX]) bestaat uit 8 bits. Een bit kan 0 of 1 zijn dus 2 waardes per bit. 2 bits geven dus 2x2=4 mogelijkheden en 4 bits geven dan 2x2x2x2=16 mogelijkheden. 1 segment kent dus 256 mogelijkheden. Als we 1 segment uitschrijven zien we welke waardes de posities hebben:

_	_	_	_	_	_	_	_
128	64	32	16	8	4	2	1

Om het getal 178 te vormen moeten we de volgende waardes invullen:

X		X	X			X	
_	_	_	_	_	_	_	_
128	64	32	16	8	4	2	1

Dit is: 128 + 32 +16 +2 = 178

Binair ziet er dit als volgt uit (alle benodigde posities zijn 1 en de overige zijn 0):
10110010

Als we terugrekenen vanuit binair dan gaat dat exact omgekeerd:
11000000

X	X						
_	_	_	_	_	_	_	_
128	64	32	16	8	4	2	1

En is dus 128 + 64 = 192

Subnets + Hosts berekenen in classfull network:
Voor het uitrekenen van het aantal subnets + hosts in een classfull network waarbij alles hetzelfde subnetmask heeft ga je als volgt te werk:

1. Bereken eerst de hoeveelheid bits die bezet zijn (b.v. 16 bij een class B netwerk)
2. Bereken hoeveel bits je voor je netwerken nodig hebt
3. Bereken hoeveel bits je nodig hebt voor je hosts

Bereken het subnetmask:
Het berekenen van het subnetmask is simpel. Zet alle netwerk + subnet bits op 1 en alle hosts bits op 0. Dus:

172	16	8	2
N	N	S	H
11111111	11111111	11111111	00000000
255	255	255	0

Subnets worden ook vaak aangeduid als CIDR (Classless Inter-Domain Routing.) notatie. Dit zijn het aantal actieve bits (netwerk + subnet). Bovenstaande voorbeeld van 255.255.255.0 heeft een CIDR notatie van /24 (24 actieve bits)

Nog een voorbeeld:

172		16		8		2	
N		N		S		H	
11111111		11111111		11111110		00000000	
255		255		254		0	

Bij bovenstaande voorbeeld “leent” het subnet ID de laatste 7 bits van het hosts gedeelte. Door 7 bits te lenen zien we dat het subnet in het 3e octet 254 wordt (128+64+32+16+8+4+2).

X	X	X	X	X	X	X	
_	_	_	_	_	_	_	_
128	64	32	16	8	4	2	1

Met deze 7 bits zijn (7 tot de macht 2) zijn 128 subnets te maken met ieder 512-2=510 hosts (9 tot de macht 2).

Bereken het netwerk ID, first (usable) address, broadcast address en last (usable) address:
Definieer de netwerk class en verdeel de netwerken en de hosts. Als voorbeeld: 172.16.8.2 = een class B netwerk. De verdeling is dus:

Netwerken		Hosts	
172.16		8.2	
172.16		0.0	<- Zet alle hosts bits op 0 = netwerk ID
172.16		0.1	<- Doe bovenstaande +1 = first address
172.16		255.255	<- Zet alle hosts bits op 255 = broadcast address
172.16		255.254	<- Last usable address

Bereken het aantal hosts (classfull en classless):
Het aantal mogelijke hosts is afhankelijk van het netwerk en het subnet. In bovenstaande voorbeeld (172.16.8.2) weten we hoeveel hosts we hebben omdat dit een classfull IP is en dus het subnetmask heeft van 255.255.0.0. Er zijn dus 16 bits voor het host gedeelte. 16 tot de macht 2 is: 65536 hosts. Hier moet je echter 2 adressen van afhalen (netwerk ID en Broadcast address) dus in het totaal 65534 usable host IP adressen.

Hosts tellen op zoals een klok dat doet. Van achter naar voor. Dus in dit voorbeeld:
172.16.0.0 (Network ID)
172.16.0.1 (First usable IP)
172.16.8.2
172.16.8.255
172.16.9.0
172.16.9.255
172.16.10.0
172.16.254.255
172.16.255.0
172.16.255.254 (Last usable IP)
172.16.255.255 (Broadcast IP)

In een classless range moet je het subnet mask weten om het aantal hosts uit te reken. Bovenstaande B class heeft heel veel hosts, maar slechts 1 netwerk.

Als we 100 netwerken willen dan lenen we hiervoor 7 hosts bits van het 3e segment:

X	X	X	X	X	X	X	-
_	_	_	_	_	_	_	_
128	64	32	16	8	4	2	1

7 tot de macht 2 = 128 en dus voldoende voor 100 subnets. Er blijft nu nog maar 1 bit over (in het 3e octet) voor de host + 8 in het 4e octet. In het totaal dus 9 bits. 9 tot de macht 2 is 512-2 = 510 hosts per subnet.

Het subnet mask komt er dan als volgt uit te zien:

N		N		S	\	H		H
11111111	|	11111111	|	1111111	\	0	|	00000000
255	|	255	|	254	\		|	0

Dit class B netwerk heeft nu een subnet van 255.255.254.0. Omdat dit subnet afwijkt van het subnet dat eigenlijk bij deze class hoort (255.255.0.0) noemen we dit een classless subnet. Met classless subnets kunnen IP adressen efficiënter gebruikt worden.

Host IP, subnet ID, Broadcast etc via DHCP bereken via subnet:
Cisco examenvragen kunnen er als volgt uitzien:

Je krijgt de opdracht om een DHCP server te configureren in het 10.1.4.0/23 netwerk waarbij je de laatste 100 bruikbare IP adressen uitdeelt. Welk IP adres kan er in deze lease vallen?

Om dit te doen moet je eerst weten welke netwerken er zijn. Hier is een formule voor:

/23 = subnet: 255.255.254.0

Regel 1: als een subnetmask octet 255 is neem dan de waarde uit hetzelfde octet van het IP adres over
Regel 2: als een subnetmask octet 0 is, plaats dan een 0
Regel 3: als een subnetmask octet een andere waarde heeft dan doe je 256-%waarde subnetmask%

Als we deze regels invullen dan:

10.1.4.0
255.255.254.0

Na regel 1 ziet het resultaat er zo uit:
10.1…….

Na regel 2 ziet het resultaat er zo uit:
10.1……0

Na regel 3 ziet het resultaat er zo uit:
10.1.2.0

Het eerste subnet heeft dus de volgende info:
Netwerk ID: 10.1.0.0
First address: 10.1.0.1
Broadcast ID: 10.0.1.255
Last address: 10.0.1.254

Ieder subnet heeft 9 bits over voor de hosts en heeft dus 510 IP adressen. Dit is voldoende om een DHCP scope met 100 IP adressen te configureren.

De uitkomst na de formule was: 10.1.2.0. In stap 3 bereken je het moeilijke octet: 10.1.**2**.0. De uitkomst hiervan is de vermenigvuldigingsfactor. Dus in dit geval subnets in stappen van 2:

0
2
4
6
etc.

Ons IP: 10.1.4.0 gaat dus van:

Netwerk ID: 10.1.4.0
First address: 10.1.4.1
Broadcast ID: 10.0.5.255
Last address: 10.0.5.254

De laatste 100 bruikbare adressen zijn dan: 10.0.5.154 t/m 10.0.5.254. Een van de antwoorden zal dan in deze range vallen.

Summarized Routes
Summarized routes zijn bredere subnetten die meerdere kleine subnetten omvatten. Met andere woorden. Als subnet 192.168.10.0/24 en 192.168.20.0/24 in een routetabel voorkomen dan kunnen deze ook samengevoegd worden als: 192.168.0.0/16. Let erop dat dit voorbeeld werkt maar veel te veel overige adressen meeneemt. Het is de kunst om de beste summarization route te vinden. Dit doe je door zo min mogelijk overige adressen in de summarization mee te nemen. Bijvoorbeeld:

Vindt de beste route summarization voor 192.168.1.64/28 + 192.168.1.80/28 + 192.168.1.96/28.

Om dit te doen noteren we van alle netwerken het netwerk ID + broadcast adres:

Netwerk	Netwerk IP	Broadcast IP
192.168.1.64/28 = x.x.x.240	192.168.1.64	192.168.1.79
192.168.1.80/28 = x.x.x.240	192.168.1.80	192.168.1.95
192.168.1.96/28 = x.x.x.240	192.168.1.96	192.168.1.111

De range die we moeten omvatten is: 192.168.1.64 t/m 192.168.1.111.

Het subnetmask dat gebruikt werd is /28. Haal hier 1 van af en probeer het met subnet 27 (stappen van 32). Dit werkt niet. Probeer dan /26 (stappen van 64). Dit zou voldoende moeten zijn 0-63 / **64-128**). 192.168.1.64/26 is dus de beste summarization route.

Subnet Mask CheatSheet

Prefix	Addresses	Hosts	Netmask	Amount of a Class C
/32	0	0	255.255.255.255	1/256
/31	2	0	255.255.255.254	1/128
/30	4	2	255.255.255.252	1/64
/29	8	6	255.255.255.248	1/32
/28	16	14	255.255.255.240	1/16
/27	32	30	255.255.255.224	1/8
/26	64	62	255.255.255.192	1/4
/25	128	126	255.255.255.128	1/2
/24	256	254	255.255.255.0	1
/23	512	510	255.255.254.0	2
/22	1024	1022	255.255.252.0	4
/21	2048	2046	255.255.248.0	8
/20	4096	4094	255.255.240.0	16
/19	8192	8190	255.255.224.0	32
/18	16384	16382	255.255.192.0	64
/17	32768	32766	255.255.128.0	128
/16	65536	65534	255.255.0.0	256

IPv6 addressing

IPv6, ofwel Internet Protocol versie 6 is de opvolger van het alom bekende IPv4. IPv4 heeft een 32-bits adres waardoor er in theorie 4.294.967.296 mogelijke IPv4 adressen uitgegeven kunnen worden. Doordat we de laatste jaren in hoog tempo IPv4 adressen consumeren is dit aantal te weinig om iedereen in de toekomst de kunnen voorzien van een IPv4 adres. Het IPv6 protocol heeft niet 32 maar 128-bits. Dit hoge aantal is voldoende om theoretisch iedere zandkorrel op de aarde te voorzien van een eigen IPv6 adres.

IPv6 algemeen

- Host moet IPv6 adres van de router weten om pakketjes buiten het netwerk te kunnen routeren
- Als een IPv6 pakketje door de router ontvangen wordt dan wordt deze “de-encapsulate”en vervolgens weer “re-encapsulate”
- Als een apparaat zowel IPv4 als IPv6 routeert noemen we dat een “Dual Stack” apparaat

Een IPv6 adres ziet er als volgt uit:
2001:db81:85a3:08d3:1319:8a2e:0370:7344

De grote verschillen met een IPv4 adres (192.168.1.1) zijn:

- 8 octetten i.p.v. 4 octetten
- Octetten gescheiden door een dubbele punt (colon) i.p.v. een enkele punt
- 128 bits i.p.v. 32 bits (elk octet bestaat uit 16 bits i.p.v. 8 pits)
- Hexadecimale notatie i.p.v. decimale notatie

Doordat de getallen in een IPv6 adres hexadecimaal zijn i.p.v. decimaal kunnen ze 16 waardes i.p.v. 10 waardes bevatten. Door het gebruik van hexadecimale getallen worden de problemen voorkomen met getallen die uit 2 cijfers bestaan (10, 11, 12, 13, 14, 15 en 16) waardoor een octet ook meer dan 4 karakters lang kan worden en er niet altijd exact duidelijk is of 10110 nu 10-1-1-0 is of 1-0-11-0 of 1-0-1-10 is.

16 waardes voor ieder karakter in IPv6

Decimaal	Hexadecimaal	Binair
0	0	00000000
1	1	00000001
2	2	00000010
3	3	00000011
4	4	00000100
5	5	00000101
6	6	00000110
7	7	00000111
8	8	00001000
9	9	00001001
10	A	00001010
11	B	00001011
12	C	00001100
13	D	00001101
14	E	00001110
15	F	00001111
16	10	00010000
17	11	00010001
18	12	00010010
19	13	00010011
20	14	00010100

Het volgende hexadecimale IPv6 adres: 2001:db81:85a3:08d3:1319:8a2e:0370:7344 wordt door de computer binair gelezen en ziet er als volgt uit:

0010 0000 0000 0001:1101 1011 1000 0001:1000 0101 1010 0011:0000 1000 1101 0011:0001 0011 0001 1001:1000 1010 0010 1110:0000 0011 0111 0000:0111 0011 0100 0100

In decimale notitie is dit:
2001:131181:85103:08133:1319:810214:0370:7344

Bij de decimale notatie is niet duidelijk wat een tiental is en wat niet. Daarom wordt er bij een IPv6 adres gekozen voor hexadecimale notatie.

IPv6 en nullen:

Binnen IPv6 kunnen octetten die uit nullen bestaan 1 maal gegroepeerd worden door 2x een dubbele punt (colon).

Bijvoorbeeld:
2001:0b81:0000:0000:0000:0a2e:0000:7344

Kan geschreven worden waarbij de octetten samengevoegd zijn met een colon:
2001:0b81::0a2e:0000:7344

Ook mogen alle voorloopnullen binnen ieder octet weggelaten worden:
2001:b81:0000:0000:0000:a2e:0000:7344

En ieder octet met 4 nullen mag genoteerd worden als 1 nul. Dus het volledige IPv6 adres:
2001:0b81:0000:0000:0000:0a2e:0000:7344

Kan als volgt genoteerd worden:
2001:b81::a2e:0:7344

De opbouw van een IPv6 adres

Net als bij IPv4 is een gedeelte van het IPv6 adres gereserveerd voor het netwerk en heb je het andere gedeelte ter beschikking voor je hosts. Stel je het volgende IPv6 adres voor:
FE80:0212:34FF:FE56:7890:8a2e:0370:7344/64

De /64 is een CIDR notatie (Classless Inter-Domain Routing). Deze geeft aan dat de eerste 64 bits gebruikt worden om het netwerk aan te duiden (het netwerk gedeelte ofwel de prefix). Het volgende gedeelte is dus voor iedere hosts op het netwerk hetzelfde:
FE80:0212:34FF:FE56

Het laatste gedeelte is het hosts adres (Interface ID) voor de cliënts op het interne netwerk.
7890:8a2e:0370:7344

De prefix wordt dan als volgt geschreven (de host bits zijn nullen):
FE80:0212:34FF:FE56:0:0:0:0/64
of:
FE80:0212:34FF:FE56::/64

De prefix berekenen is gemakkelijk. Een octet bestaat uit 16 bits, elk hexadecimaal cijfer is 4 bits. Stel je een 40-bits prefix voor. Dat betekend 2 octetten (2x16 = 32) + 2 hexadecimale getallen (2x4 = 8).
De prefix van: FE80:0212:00FF:FE56:7890:8a2e:0370:7344/40 is dus:

FE80:0212:0000::/40
of
FE80:212::/40

IPv6 kent de “Global Routing Prefix” welke overeenkomt met het netwerk ID van IPv4. De Global Routing Prefix geeft het hele blok beschikbare IPv6 adressen weer.

Soorten IPv6 adressen:

Binnen IPv6 kennen we een aantal soorten IPv6 adressen. De volgende zijn de meest belangrijke varianten:

Unicast IPv6
Een Unicast adres is een host-to-host adres ofwel voor verkeer dat 1 op 1 gerouteerd moet worden. Er zijn een paar soorten Unicast adressen, namelijk:

Global Unicast IPv6
Deze komt overeen met het oude publieke IPv4 adres. Deze adressen zijn globaal uniek en routeerbaar over het internet. Global Unicast adressen zijn alle adressen binnen IPv6 welke niet voor een ander doeleinde gereserveerd zijn.

Link-Local Unicast IPv6
Ieder IPv6 apparaat beschikt over een Link-Local Unicast adres. Dit adres wordt gebruikt om binnen het eigen netwerk (subnet) te communiceren. Dit adres is niet routeerbaar en kan automatisch statisch ingesteld worden, via DHCPv6 of SLAAC. Deze adressen hebben altijd een 64-bits prefix welke begint met **FE80::/10** (eerste 10 bits) gevolgd door nullen. De prefix is dus FE8::/64 – FE9::/64 -- FEA::/64 of FEB::/64. Het netwerk ID kan op verschillende manieren geconfigureerd worden zoals b.v. de EUI-64 optie.

Cisco router maken automatisch een link-local aan op iedere interface die geconfigureerd is met een IPv6 unicast adres.

Loopback
Het loopback adres is het oude IPv4 “local” adres. Ieder device beschik over het loopback adres zodat hij pakketten aan zichzelf kan zenden. Je kunt je loopback adres dus ook altijd pingen. Het IPv6 loopback adres ziet er altijd als volgt uit:

::1/128

Ofwel:

0000:0000:0000:0000:0000:0000:0000:0001

Unspecified address:
Het unspecified adres kan alleen gebruikt worden als “source” adres in een IP pakket wanneer het apparaat geen geldig IPv6 adres heeft of wanneer het “source” adres irrelevant is. Een unspecified adres bestaat alleen uit nullen (dus **::0/128**).

Unique Local Address:
Het Unique Local Address is overeenkomstig met de IPv4 private adressen. Het is een privé adres welke gebruikt wordt voor lokale adressering binnen 1 of meerdere sites. Dit adres is niet routeerbaar over het internet. De Unique Local Address range is van:
FC00::/7 tot FDFF::/7

Daarnaast moet de beheerder een uniek 40-bits GlobalID kiezen (tesamen met FC / FD is dat een 48-bits prefix). De volgende 16 bits moeten voor het subnet veld gebruikt worden. De laatste 64-bits zijn voor de hosts.

IPv4 embedded:
Om Ipv4 langzaam over te laten gaan naar Ipv6. Deze adressen worden toegewezen aan apparaten die met zowel Ipv4 als Ipv6 overweg kunnen (ofwel Dual Stack apparaten). Deze adressen bestaan allemaal uit nullen met uitzondering van de laatste 32-bit die ingevuld worden met het 32-bits Ipv4 adres.

Ipv4:
101.44.61.32

Ipv6:
0:0:0:0:0:0:101.44.61.32 (ofwel: ::101.44.61.32)

Multicast Ipv6
Multicast is te vergelijken met het oude “broadcast” idee. Er bestaan 3 soorten multicast adressen:

All-nodes multicast
Verkeer naar de “all-nodes multicast” adressen gaat naar ieder Ipv6 apparaat op het netwerk. Deze range is als volgt: **FF02::1**

All-routers multicast
Multicast verkeer naar de “all-routers” groep gaat naar alle routers binnen het netwerk. Een router wordt lid van deze groep als hij Ipv6 geactiveerd heeft en RS (Router Solicitation) berichten kan ontvangen en verwerken. Deze range is als volgt: **FF02::2.** We kennen ook:
FF02::1:2 = Alle DHCPv6 en DHCPv6 relay agents
FF02::5 = All-OSPF
FF02::6 = All OSPF-DR (designated Routers)
FF02::A = All EIGRPc6 routers

Solicited node multicast
Dit is een multicast adres dat gebruikt wordt door het NDP (Neighbor Discovery Protocol) en wordt automatisch aangemaakt wanneer de global unicast of link-local unicast adressen worden toegewezen. Dit adres wordt gemaakt door de prefix **FF02:0:0:0:0:1:FF:/104** te combineren met de laatste 24 bits van het global unicast of link-local adres. De laatste 6 hex getallen (24 bits) vormen het solicited node multicast adres. Alle nodes met dezelfde laatste 6 hex getallen vallen in dezelfde groep en ontvangen dus gezamenlijk de pakketten die hier naartoe gestuurd worden.

Anycast Ipv6
Anycast is speciaal voor 1-to-many (van 1 naar een grote groep) communicatie. Denk hierbij b.v. aan b.v. videosharing. Er is geen speciaal adresschema voor Ipv6 Anycast adressen. Anycast is nieuw en heeft als voordeel dat het load sharing tussen routers ondersteund. Met Anycast kun je denken aan het opvragen van een video bij een video farm met servers over de hele wereld. Deze servers werken met anycast waardoor de gebruiker gestuurd wordt naar de server die de load het beste kan verwerken. Het maakt niet uit welke server dit is!

Makkelijk onthouden:

Type	**Eerste Hexadecimale getallen**
Global Unicast	Alle adressen, mits gereserveerd
Unique Local	FD
Multicast	FF00
Link-Local	FE80
Site-local address	FEC0
Global addres	2000
Loopback address	::1

Ezelsbrug (verzin gerust zelf iets….dit slaat helemaal nergens op ☺):
Loopback = eerste adres (::1)
Global address: Global = wereldwijd. We leven in de 21e eeuw (2xxx). Deze beginnen met 2000.
Link-local = Local = intern. Dit is "Forbidden External". Begint dus met FE. + 80
Site-local = Local = intern. Dit is "Forbidden External". Begint dus met FE. + C0
Unique-local = intern. Dit is intern maar uniek. Dus "Formidable Desirable". Begint met FD
Multicast = "Flow Foreward". Begint dus met FF + 00
Global Unicast = ALLE REST (mits gereserveerd)

Het verkrijgen van een IPv6 adres

Je kunt op verschillende manieren een IPv6 adres verkrijgen:

- Statisch (100% zelf verzinnen)
- EUI-64 (Gebaseerd op MAC adres)
- SLAAC (Stateless Address Auto Configuration)
- DHCPv6

Statisch:
Het statische IP adres is een IP adres welke je zelf 100% verzint. Je vult dus zelf 32 hexadecimale karakters in. Op Cisco doe je dit als volgt:

```
>enable
#configure router
()ipv6 unicast-routing                    <- Stel de router in om IPv6 te routeren
()interface fastethernet0/1
(-)ipv6 address 2001:DBB:1111:3::2/64
```

EUI-64
Het EUI-64 principe zorgt ervoor dat je zelf de (64-bits) prefix maakt en de router het 64-bits Interface ID erbij genereerd op basis van je MAC adres.

De EUI-64 regels zijn als volgt:

1. Neem Mac en deel het door de helft
2. Plaats FFFE tussen beide helften
3. Verander / invert het 7e bit (universal / local bit)

Als we deze regels volgen met MAC adres: 16123456789A dan zou de prefix als volgt worden gegenereerd.

1. 1612345 6789A
2. 1612345 FFFE 6789A
3. 16 = 0001 0110 – Het 7e bit veranderen we (in dit geval van 1 naar 0). Dan wordt het: 0001 0100. Nu staan de binaire waarde voor 14. De prefix wordt dan: 1412345FFFE6789A

Op Cisco stellen we dit als volgt in:

```
>enable
#configure router
()ipv6 unicast-routing                    <- Stel de router in om IPv6 te routeren
```

()interface fastethernet0/1
(-)ipv6 address 2001:DB8:1111:1::/64 eui-64 <- Stel hier de prefix in met toevoeging eui-64.

Als er een interface is die niet beschikt over een MAC adres (zoals bij serieel het geval is) dan gebruikt Cisco het MAC adres van de laagst genummerde router interface (FastEthernet0/0)

Neightbor Discovery Protocol – NDP

NDP is het protocol dat ervoor zorgdraagt dat hosts voorzien worden van een interface/unicast IPv6 adres, prefix length, default router en de DNS server. Hosts die geconfigureerd zijn om SLAAC te gebruiken zullen het NDP protocol gebruiken. Het NDP protocol werkt als volgt:

- Host verstuurd een NDP RS (Router Solicitation) bericht. Dit is een local scope Router Multicast bericht (FE02::2). Alle routers ontvangen dit bericht en kunnen antwoorden.

- Alle routers beantwoorden met een NDP RA (Router Advertisement) bericht waarin staat:
  - Link-local IPv6 adres van de router
  - Prefix van het lokale subnet
  - Prefixlengte van het lokale subnet

  *De router kan NDP RA ook ongevraagd (unsolicited) versturen. In dat geval worden ze naar het local-scope Multicast adres gestuurd i.p.v. naar het unicast adres van de host.

- De host gebruikt na het verkrijgen van de juiste netwerkinfo NDP NS/NA (Neighbor MAC Discovery) berichten om zijn “directe buren” (omringende hosts) te ontdekken. De host stuurt deze berichten naar het solicited-node multicast adres. NS = Neighbor Solicitation en NA = Neighbor Advertisement. De NA bevat het IP adres + MAC adres van de host

- Als de host een unicast IP adres wil gebruiken verstuurd deze een NDP DAD (Duplicate Address Detection) bericht (wat gewoon een NS pakket is met de vraag of hosts met het gewenste IP willen antwoorden). Op deze manier controleert de host of zijn gewenste IP al in gebruik is (zo ja dan krijgt deze antwoord en zo nee, dan niet).

DHCPv6
DHCP heeft een aantal voordelen t.o.v. SLAAC. Het enige nadeel is dat DHCP een server nodig heeft om alles administratief (voor elke host) bij te houden. SLAAC heeft geen server nodig.

DHCPv6 is niet de 6e versie van DHCP maar wordt zo aangegeven om te laten zien dat het bedoeld is voor IPv6 adressen. Het opvragen van een adres bij DHCPv6 gaat als volgt:

- **Solicit** - DHCP client stuurt een local LAN bericht om een DHCP server te zoeken
- Als de server zich in hetzelfde subnet bevindt kunnen direct gegevens worden uitgewisseld
- Als de DHCP server zich in een ander LAN bevindt dan zullen beide routers voorzien moeten worden van een DHCP Relay Agent om de cliënt met de DHCP server te laten communiceren
- **Advertise** - Server biedt vervolgens een unicast IP + prefix lengte en DNS server aan incl. de lease periode
- **Request** - De client geeft aan het adres te willen gebruiken
- **Reply** - De DHCP server registreerd de gegevens voor de client.
- DHCPv6 biedt (in tegenstelling tot DHCP) geen default gateway meer aan. De default router (zoals dat bij IPv6 heet) wordt gevonden door NDP te gebruiken.

Er zijn 2 type DHCP servers:

1. Statefull DHCPv6 server
   Deze server houdt bij welke cliënts een lease hebben van een specifiek IP adres hebben en hoe lang.

2. Stateless DHVPv6 server
   Deze server houdt geen tracking data van de cliënt bij maar deelt alleen bepaalde informatie uit zoals DNS settings. Een Stateless DHCPv6 server wordt vrijwel altijd gebruikt in combinatie met SLAAC.

Stel de interface in om via DHCPv6 het IPv6 adres te ontvangen:
>enable
#configure router
()interface fastethernet0/1
(-)ipv6 address dhcp

SLAAC (Stateless Address Auto Configuration)
SLAAC is een methode waarmee hosts hun eigen IP adres automatisch kunnen aanmaken incl. alle bijbehorende informatie zonder aanwezigheid van een (statefull) DHCP server. Een IP adres wordt niet aan de cliënt geleased zoals bij Statefull DHCPv6 maar de host configureert zijn eigen IP adres volgens de volgende stappen:

1. Gebruik NDP RA/RA berichten om de prefix van alle routers in het netwerk te leren. Op deze manier wordt de prefix, prefix lengte en default router gevonden
2. Maak nu het IPv6 adres compleet door een NetwerkID te genereren (statisch of middels EUI-64)
3. Alvorens de host het IPv6 adres gebruikt controleert hij de uniekheid door eerst een NDP DAD te sturen
4. Overige informatie zoals b.v. de DNS servers worden verkregen van een Stateless DHCP server

De SLAAC router stuurt periodiek een Router Advertisement (RA) bericht naar alle IPv6 apparaten op het netwerk. Cisco routers doen dit standaard iedere 200 seconden. Maar een IPv6 apparaat hoeft hier niet op te wachten en kan zelf ook een Router Sollicitation (RS) naar de router sturen. De router voorziet de cliënt dan van een Prefix, Prefix lengte (subnetmask) en Default Gateway. Hiervoor wordt het NDP (Network Discovery Protocol) gebruikt via ICMPv6 (Internet Comunication Protocol version 6).

Stel de interface in om via SLAAC het IPv6 adres te ontvangen:
>enable
#configure router
()interface fastethernet0/1
(-)ipv6 address autoconfig

IPv6 subnetting

Soms zal een beschikbaar IP blok onderverdeeld moeten worden in kleinere blokken (subnets). Subnetting met IPv6 is gemakkelijker dan met IPv4. Cisco hanteert de stelregel dat een uniek subnet nodig is voor ieder VLAN en iedere WAN verbinding (Serial, Frame Relay en EoMPLS).

Zorg er allereerst voor dat je je mindset veranderd als je gaat subnetten. Waar we bij IPv4 nog gingen rekenen hoeveel hosts we nodig hadden. Omdat een normaal host netwerk bij IPv6 64-bits lang is en dus miljarden hosts kan bevatten is dat geen probleem meer. Bij IPv6 kijken we hoe we onze beschikbare subnetten zo goed mogelijk kunnen verdelen.

Het wordt wel altijd aangeraden om 64 bits te reserveren voor de interface ID (hosts netwerk) omdat SLAAC en EUI-64 ook altijd 64 bits gebruiken.IPv6 bestaat net als IPv4 uit 2 delen, netwerk gedeelte en hosts gedeelte. Als we gaan subnetten maken we hier 3 gedeeltes van:

1 – Netwerk gedeelte (Global Routing Prefix)
2 – Subnet
3 – Hosts gedeelte

We zien hierboven een Global Unicast Ipv6 adres zoals deze uitgegeven kan worden door een provider. De eerste 3 octetten (48 bits) zijn vast. Dit is de site prefix. De laatste 64-bits (4 octetten) zijn gereserveerd voor de host netwerken. De 16 bits uit het 4e octet zijn gereserveerd voor het Subnet ID. Met deze 16 bits heb je 65535 mogelijke subnetten tot je beschikking. Je zou je subnetten dus kunnen nummeren met een logisch nummer.

Marketing = subnet 1000
Sales = subnet 2000
Directie = subnet 5000
etc.

Een IP adres van de afdeling marketing is dan gemakkelijk te herkennen aan het subnetmask. Deze ziet er b.v. als volgt uit:

FE80:0212:34FF:**1000**:7890:8a2e:0374:7288/64

WAN's

Leased Lines

- Ook wel genoemd Leased Circuit, Circuit, Serial Link, Serial Line, Point-to-Point Link, T1, WAN Link
- Foreward data tussen 2 routers (2 sites) – Vergelijking met crossover kabel
- Full Duplex
- Layer 1
- Ook wel private circuit genoemd (privé lijn)
- Kan voor telefonie, data en internet gebruikt worden
- Altijd actief (geen dail-in)
  HDLC & PPP Protocollen

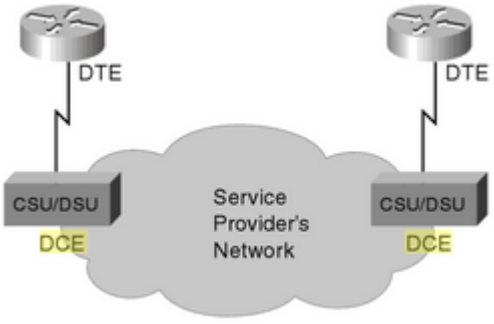
Om een leased line te creëren zijn een aantal componenten benodigd. Allereerst staat er een router bij de telecom aanbieder met een ingebouwde CSU/DSU (Channel Service Unit / Data Service Unit) of een seperate CSU/DSU met een korte kabel tussen router en CSU/DSU. Vervolgens gaat er een lange kabel naar de locatie van de klant alwaar deze ook met een CSU/DSU verbonden wordt welke weer met een router verbonden is. De CSU/DSU+Router noemen we CPE (Customer Premise Equipment) ofwel de gehuurde componenten. De CSU/DSU is een apparaat die het "cloaking" proces regelt. Het cloacking proces regelt fysiek de snelheid en timing waarover de seriële interface van de router bits over de seriële kabel verzend en ontvangt. De router is verbonden met de CSU/DSU als rol DTE of DCE.

DTE – Data Terminal Equipment

- End device (router)
- Serial connection
- Communiceert met DCE via crossed serial line (pin 2 en 3)
- Ontvangt en verzend als de DTE dit aangeeft
- Meestal aan kant van end-user

DCE - Data Circuit-terminating Equipment

- Modem
- Serial connection
- Communiceert met DTE via crossed serial line (pin 2 en 3)
- Ontvangt en verzend als de DCE dat aangeeft
- Meestal aan kant van provider (b.v. Frame Relay switch in Frame Relay Cloud)



DSL – Digital Subscribers Line

- Relatief korte afstanden t.o.v. leased lines
- Via telefoonkabel
- RJ11 poorten
- DSLAM (DSL Access Multiplexer) wordt gebruikt door provider om internet en voice signalen te splitsen
- Asymmetrisch (hogere download (max 24 Mbps) dan upload)

Dail Access & ISDN (Integrated Services Digital Network)

- Dail Access is analoog (digitaal signaal wordt door modum gemoduleerd naar analoog en bij de ISP weer terug naar digitaal. Max speed van dail access is 56 Kbps
- ISDN gebruikt digitale signalen waardoor er geen modulatie plaats hoeft te vinden. Ook ondersteund het 2 oproepen van 64 Kbps tegelijkertijd waardoor je kunt bellen en internetten tegelijkertijd of waarmee je door ze te bundelen kunt internetten met 128 Kbps.
- Symmetrische snelheid (Zelfde download snelheid als upload snelheid)

Kabel Internet

- Asymmetrisch
- Relatief korte afstanden
- Vaak sneller dan DSL

3G / 4G

- Werkt via radiosignalen (vanuit end-user device)

Satelliet

- Satellietverbindingen zijn speciaal voor afgelegen gebieden waar geen snelle internetverbinding te verkrijgen is
- Satellietverbindingen zijn doorgaans 10x sneller dan analoge modem verbindingen
- Upload snelheid is +/- 10% van de download snelheid

Frame Relay

- NBMA – Non Broadcast MultiAccess networks. Meer devices kunnen hierop aansluiten maar broadcasts kunnen in tegenstelling tot LAN netwerken niet verzonden worden.
- Connectie tussen DTE 1 en DTE 2 (over de frame relay cloud) heet een Permanent Virtual Circuit (PVC). Als er nog sprake is van een inbelverbinding en de connectie niet permanent is dan noemen we dit een SVC – Switched Virtual Circuit. Vergelijk deze VC's als een Point-to-Point connectie, dus een connectie tussen 2 netwerken. De snelheid waarmee bits over de VC kunnen gaan (volgens de overeenkomst met ISP) heet CIR – Commited Information Rate
- De lijn tussen de DTE en de DCE in frame relay cloud heet een "Access Link". De snelheid waarop deze clocked is noemen we AR – Access Rate
- Het frame relay adres welke in de header de VC identificeert waarover de frames getransporteerd moeten worden noemen we DLCI – Data Link Connection Identifier. De DLCI

moet uniek zijn tussen access-links (point-to-point en point-to-multipoint). Vaak wordt de DLCI gekozen door de ISP.

- Om de verbinding tussen een DCE en DTE te managen worden status berichten en keepalives tussen beide verzonden. Dit gebeurt door de LMI – Local Management Interface op de DTE (router buiten het Frame Relay netwerk). Deze berichten noemen we dan ook LMI berichten.
- Als alle frame relay sites met elkaar verbonden zijn noemen we dat een “full mesh frame relay” en zo niet dan heet het een “partial mesh frame relay”.

LMI berichten hebben 2 hoofdfuncties:

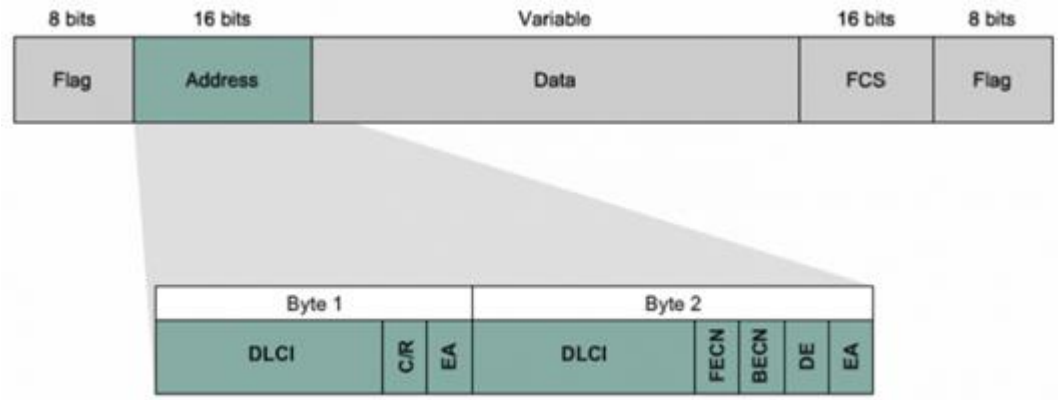
1. Keepalive functie toepassen tussen DTE & DCE
2. Signal om te controleren welke VC’s up & down zijn

Er zijn 3 soorten LMI status berichten, namelijk:

Type	LMI Type Parameter
Cisco	cisco
ANSI	ansi
ITU	Q933A

*Deze 3 LMI protocollen zijn niet met elkaar compatible.

De frame relay header ziet er als volgt uit:



Het DLCI veld in de header is om de PVC te identificeren. In de header staat dus geen source of destination informatie. Als Router A met DLCI 40 een pakket over de PVC van router B verzend zet de ISP in de frame relay cloud de DLCI van 40 naar de DLCI van router B.

IP Adressing Frame Relay:
Er zijn 3 IP adressing mogelijkheden:

1. Een subnet voor alle frame relay DTE’s. Point-to-mulitpoint. Dit wordt meestal niet gebruikt met een partial mesh
2. Een subnet per VC. Point-to-point. Dit wordt vaak gebruikt voor een partial mesh en wordt meestal gebouwd d.m.v. subinterfaces op de router
3. Hybide oplossing waarbij een gedeelte bestaat uit een subnet per DTE (point-to-mulitpoint) en een gedeelte uit een subnet per VCE (point-to-point)

Voor het configureren moet je minimaal 2 commando’s gebruiken, namelijk IP Address & Encapsulation. Er zijn echter veel meer opties. Het algemeen stappenplan voor het opzetten van een frame relay netwerk is als volgt:

1. Bepaal de frame relay sites, zorg dat er een access-link is en zet de juiste clock snelheid op de links.
2. Bepaal de VC's en zet hierop de juiste CIR (meestal geregeld door ISP)
3. Kies het LMI type
4. Kies IP subnetting schema
5. Kies of de ip adressen op de fysieke interface of op subinterfaces worden toegewezen (afhankelijk van point-topoint of point-to-multipoint)
6. Kies of je "cisco" of "IETF" encapsulatie gebruikt

Om layer 3 naar layer 2 te mappen wordt "mapping" gebruikt. Dit is vergelijkbaar met ARP in LAN netwerken. Met mapping kun je het layer 3 adres van de router mappen aan de DLCI van de andere router zodat bekend is welke DLCI gebruikt moet worden om die router te benaderen. Mapping wordt gebruikt in een multiaccess netwerk.

Inverse ARP – I-ARP:
Dit proces noemen we ook wel automatic mapping. Zodra een router online komt stuurt het een IARP bericht met zijn IP adres + DLCI in de header. De ontvangende router weet nu het IP + DLCI. Inverse ARP is automatisch enabled in multiaccess netwerken.

Static frame relay mapping:
Het nadeel van static mapping is dat mapping geconfigureerd moet worden voor elk layer 3 protocol dat erover gerouteerd wordt.

Sub interfaces:
Om frame relay over een sub interface te laten werken roep je de subinterface aan met een punt (serial0/0/0.1). De frame-relay encapsulation stel je nog steeds in op de hoofd interface. Op de subinterfaces stel je de IP adressen en DLCI info in.

Protocollen

HDLC - High-Level Data Link Control

- Voor Point to Point leased line (serial)
- HDLC is een connection orientend of connectionless protocol.

HDLC Frame:

1	1	1 - 2	2	Variable	4	1
Flag	Address	Control	Type Proprietary	Data	FCS	Flag

*Let op – het 2 byte lange "type" veld is een Cisco veld en hoort niet bij de ISO HDLC standaard.

MPLS (Multi Protocol Label Switching)

- Zelfde ideeen als ethernet en frame relay
- Klanten verbinden met MPLS cloud
- Data is prive tussen vertrouwde endpoints

- Routes IP packets between site (geen frame relay packets of bits)

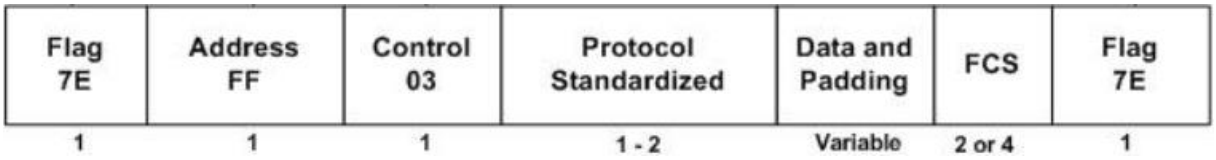
EoMLPS - Ethernet over MPLS (Multi Protocol Label Switching)

- Maakt het mogelijk om Ethernet pakketjes over de MPLS cloud te versturen
- Gebruikt bij Leased Lines en Circuit Switching
- Max 100 Mbps en 1 Gbps ethernet
- Client-side is ethernet interface en geen seriële interface

PPP - Point-to-Point Protocol

- Ook een data-link protocol voor Leased Lines, Circuit Switching en Breedband
- Pakketje hebben een header en een trailer
- Bedoeld voor synchrone en asynchrone verbindingen
- Multiple layer 3 protocollen worden ondersteund en kunnen worden aangegeven in protocol field in de header
- Authenticatie mogelijk (PAP / CHAP)
- Control Protocols voor protocollen op een bovenliggende laag

PPP frame



PPP Control Protocols:

Link Control Protocol – LCP:
Voor verschillende individuele data-link laag functies

Network Control Protocols – NCP:
Dit is een set van protocollen, 1 per netwerk laag protocol en biedt functies die gerelateerd zijn aan laag 3 protocollen.

Authenticatie:

PAP

- Partij B (welke geauthentiseerd moet worden) begint en toont zijn secret password in clear tekst.
- Partij A bevestigd de authenticatie met een “acknowledgement”

CHAP

- Veiliger dan PAP
- Partij A begint met de challenge (met random number voor de hash)
- Partij B verstuurd zijn wachtwoord gehashed (MD5)
- Bij akkoord stuurt partij A naar partij B een “accepted” melding (dus 3-way handshake)

*Als authenticatie (met PAP / CHAP) faalt dan blijft de interface in een “Up/Down” state. De volgende statussen zijn veelvoorkomende statussen:

Line Status	Protocols	Omschrijving
Admin down	Down	Interface shutdown
Down	Down	Layer 1 problem
Up	Down	Layer 2 problem
Up	Up	Layer 3 problem
Up	Down (both ends)	Foute encapsulation geconfigureerd (matched niet)
Up	Down (both ends)	Authentication failure
Up	Down (1 end)	Keepalive disabled

PPPoE - Point-to-Point over Ethernet

- Gebruikt bij Breedband
- Layer 2
- VCMUX / LLC encapsulation
- PPP frames encapsulated in Ethernet Frames
- Point-to-Point
- CHAP authenticatie mogelijk
- Gebruikt een (virtuele) dailer interface op de Cisco Router. Op deze interface moet een encapsulation (PPP) en IP adres geplaatst worden. Vervolgens moeten (als deze gebruikt worden) ook een CHAP username en password geplaatste worden (gegeven door provider) om te authenticeren. Tenslotte wordt de dailer interface gekoppeld aan de fysieke ethernet interface. De MTU moet op 1492 geplaatst worden i.p.v. op 1500 (default) om de PPPoE headers te kunnen dragen.

PPPoA – Point-to-Point over Asynchronous Transfer Mode (ATM)

- Gebruikt bij Breedband
- Layer 2
- VCMUX / LLC encapsulation

PVC – Permanent Virtual Circuit

- Vaste virtuele verbinding tussen 2 endpoints
- Vaste paden
- Gebruikt bij Frame Relay
- Pad kan veranderen maar de endpoints niet

SVC – Switched Virtual Circuit

- Vergelijkbaar met telefoonlijn (connectie op call-by-call basis)
- Gebruikers geven endpoint op waarmee ze willen verbinden
- Gebruikt bij Frame Relay

VPI/VCI - Virtual Path Identifier / Virtual Channel Identifier
Wordt gebruikt om de volgende bestemming van een cel te identificeren als deze door een reeks van ATM switches gaat, op weg naar zijn bestemming.

BGP – Border Gateway Protocol
Het Border Gateway Protocol (BGP) is het belangrijkste routeringsprotocol van het internet: het wordt gebruikt om verkeer tussen verschillende providers te kunnen routeren. Binnen het netwerk van een provider (een zogenaamd Autonoom Systeem of AS) kiest de provider voor een bepaald intra-routeringsprotocol zoals OSPF of Routing Information Protocol, maar om routes uit te wisselen met andere providers wordt exclusief gebruikgemaakt van BGP. Het is dus niet zo dat BGP het meest gebruikte routeringsprotocol is, maar zonder BGP zou er geen Internet zijn, maar slechts een verzameling losse netwerken die niet met elkaar (kunnen) communiceren.

BGP werkt door een tabel van IP-netwerken of 'prefixes' bij te houden die de netwerkbereikbaarheid tussen autonome systemen (AS) aangeeft. Het is beschreven als een path vector protocol. BGP gebruikt geen technische metrics, maar neemt routeringsbeslissingen gebaseerd op network policies of regels.

Troubleshooting / Network Monitoring

Er zijn diverse methodes om network devices te monitoren. In dit hoofdstuk zullen er een aantal besproken worden.

SNMP – Simple Network Management Protocol

- Het SNMP protocol praat met de Management Information Base (MIB) van een apparaat.
- Objecten in de MIB heten OID's (Object ID's)
- Application Layer (7) protocol
- SNMP kan uitgelezen worden door diverse application zoals Nagios en Cisco Prime
- GET berichten zijn berichten die de SNMP manager uitzend om informatie te achterhalen
- SET berichten zijn berichten waarmee de SNMP manager berichten in zijn database schrijft
- TRAPS zijn berichten die het apparaat (SNMP agent) zelf naar de SNMP manager stuurt

Er zijn 3 versies van SNMP:

SNMP v1

- Legacy protocol
- Onveilig
- Gebruikt community strings om toegang tot MIB objecten te authentiseren. Deze community strings zijn clear-tekst passwords en onveilig.

SNMP v2c

- Onveilig
- Efficiënter in het ophalen van grote hoeveelheden data t.o.v. V1
- Gebruikt community strings om toegang tot MIB objecten te authentiseren. Deze community strings zijn clear-tekst passwords en onveilig. Er zijn 2 soorten community strings:
    - RO – Read Only – Objecten kunnen gelezen maar niet gemodificeerd worden door SNMP
    - RW – Read-write – Objecten kunnen gelezen en gemodificeerd worden d.m.v. SNMP

SNMP v3

- Veel veiliger
- Message integrity (berichten zijn niet aangepast)
- Authentication mogelijkheden (aanmelden met gebruikersnaam en wachtwoord)
- Encryptie
- De 3 veiligheidslevels in SNMP v3 zijn:

Level name	Config keyword	Username / Password	Encryptie
noAuthNoPriv	Noauth	Username	Nee
authNoPriv	Auth	Hash (MD5 / SHA)	Nee
authPriv	priv	Hash (MD5 / SHA)	Ja

Syslog – System Message Logging

Er zijn speciale syslog servers die syslogberichten kunnen ontvangen, inventariseren en categoriseren en die alle informatie samenvoegen om deze op een mooie en duidelijke manier te presenteren. Zo worden baselines en calamiteiten snel zichtbaar.

Elk bericht heeft de volgende format (basis)

- Timestamp (datum + tijd). Let op dat standaard de tijd meegestuurd wordt sinds je Cisco device als laatste opgestart is (0:59) is dus bijna een uur sinds de laatste reboot en niet de melding van 1 minuut voor 1.
- Router Facility (welk onderdeel de melding op de router gerapporteerd heeft)
- Severity level (de ernstigheid)
- Message Mnemonic
- Description (omschrijving van de melding / log)
- Default Cisco level = 7 (alles)

Er zijn 8 soorten severity levels (0-7). 0 is het meest dringend (emergency) en 6 het minst dringen (informational). Level 7 is debugging informatie. Normaliter worden levels 0 tot 4 ingesteld om verstuurd te worden (de belangrijkste meldingen).

Netflow

Netflow wordt gebruikt om het netwerkverkeer te monitoren en om zo bottlenecks, verbruik, netwerk design, security e.d. te kunnen vinden. Netflow slaat TCP verkeer op met informatie over de flow / verkeersstroom, dus niet de exacte data en alle pakketjes die over de lijn gegaan zijn. Een netflow pakketje bevat de volgende velden:

- Source IP address (waar komt het vandaan)
- Destination IP address (waar moet het naartoe)
- Source poortnummer
- Destination poortnummer
- Layer 3 protocol type
- Type of Service (ToS) marking (QoS onderdeel)
- Input logical interface

Er zijn verschillende versies van netflow. Versie 1, 5, 6, 7 ,8 en 9, Versie 9 is niet backwards compattible met andere netflow versies maar heeft wel de meeste functies waaronder MPLS labels en IPv6 ondersteuning.

CDP – Cisco Discovery Protocol

- Cisco only
- Protocol om device informatie van neighbours (aangesloten apparaten) te achterhalen
- Schakel CDP altijd uit op poorten die dit niet gebruiken. Dit is een security issue.
- Default interval: 60 seconde

CDP kan de volgende informatie achterhalen:

- Device Identifier - Hostname
- Address List - Network & Data Link list
- Post Identifier - Interface van CDP apparaat waarmee verbonden

- Capabilities List - Device Type
- Platform - Model & OS

LLDP – Link Layer Discovery Protocol

- Vendor onafhankelijk
- Protocol om device informatie van neighbours (aangesloten apparaten) te achterhalen

Device management

Cisco IOS

- Cisco IOS = Cisco Internetworking Operating System
- Cisco IOS is 1 file

Cisco apparaten hebben verschillende geheugen typen voor verschillende doeleinden:

RAM

- Werkgeheugen
- Running Config

Flash

- Cisco IOS software
- Rewritable Permanent Storage
- Interne of Extene flashdrive of USB stick

ROM

- Bootstrap program
- ROMMON

NVRAM

- Startup config

Het kopiëren van verschillende configuratie files gaat als volgt:
COPY VAN NAAR

Startup-config > Running config
copy startup-config running-config

Running config > Startup-config
copy running-config startup-config

TFTP > Running config
copy tftp running-config

Running config > TFTP
copy running-config tftp

Running config > USB 1
copy running-config usbflash1

Na het kopiëren worden de originele files overschreven door de gekopieerde files. Behalve bij een copy naar de running-config in het RAM. In dat geval worden de configuraties samengevoegd (merged). Het verwijderen van de bestanden gaat als volgt:

Verwijder startup-config
#erase nvram
OUDER: write erase & erase startup-config

Updaten Cisco IOS / operating system:

1. Download nieuwe IOS image van Cisco
2. Plaats de image op een TFTP of FTP server of op een USB stick (als deze ondersteund wordt)
3. Copy de image naar het flash geheugen van de router (#copy tftp flash)
4. Bekijk of de image op het flashgeheugen staat (#show flash)
5. Voeg een “boot system” command toe aan de startup config om de juiste (nieuwe) image te laden
6. Reboot router
    a. Router voert POST (Power On Self-Test) uit
    b. Router kopieerd bootstrap van ROM naar RAM
    c. Bootstrap kiest de image die hij gaat laden (register value) en laad IOS / ROMMON
    d. IOS kiest nu de startup-config file in NVRAM en laad het in het RAM als running-config

ROMMON (ROM Monitor)

- Een separaat OS voor o.a. password recovery

Configuration Register

- Het register van de Cisco Router welke uitgelezen wordt alvorens IOS tijdens boot wordt gestart. Het register bevat informatie over de Cisco Router zoals connectiesnelheid (9600 bps als standaard).
- 16 bits (4 hex digits)
- config-register 0x2100 zorgt ervoor dat de router niet boot met IOS maar met ROMMON (dit wordt bepaald door het laatste hexadecimale bit. Als dit 1 was (0x2101) dan werd de eerste IOS image geladen die in het Flash geheugen gevonden wordt. Met 0x2102 wordt er eerst gekeken of de startup config een “boot system” command zoals “boot system flash %filename%” heeft. Zo niet dan wordt de eerste IOS file geladen die in de flash gevonden wordt.
- Register aanpassingen (na config-register) commando worden opgeslagen na het drukken op enter.

Password recovery

Cisco heeft meerdere manieren om een wachtwoord te resetten. Deze methodes verschillen per model. Globaal volgt password recovery de volgende procedure:

1. Haal alle flashdrives uit de router zodat bootstrap geen image files kan vinden. ROMMON wordt geladen
2. Zet het Cisco register op 0x2142 (confreg 0x2142)
3. Doe de flashdrive terug in de router en reboot hem (reset commando). Cisco laad nu de enable mode zonder enig wachtwoord
4. Copieer de juiste config terug naar het apparaat (#copy startup-config running-config)
5. Reset alle wachtwoorden
6. Zet de running-config terug naar de startup-config (#copy running-config startup-config)
7. Zet het register weer terug op normale waarde (2102) zodat bij een reboot niet ROMMON geladen wordt (config-reg 0x2102)

Cisco Licensing

Cisco heeft licensing modellen, een oud en een nieuw model.

Oude licensing model:

- 1 IOS file per apparaat / familie
- 1 IOS file per functie / mix van functies
- Er zijn 4 functies:
  - IP Base (basis / default)
  - Data
  - Voice
  - Security
- Grote updates worden “versions” genoemd en kleine updates “releases”
- Bij elke update worden er dus 7 nieuwe images per apparaat / familie gereleased

Nieuw licensing model:

- 1 IOS image met alle functies erin die wel of niet geactiveerd worden op basis van de licentie. Deze IOS file noemen we de “Universal IOS file”
- De volgende 4 feature sets (ook wel “technology-packages” genoemd) zijn er:
  - IPbase / ipbasek9
  - Data / datak9
  - Unified Communications / uck9
  - Security / securityk9

Handmatig activeren van een licentie / manual activation:

1. Koop een licentie bij een Cisco reseller = Product Activation Key (PAK)
2. Ga naar de Cisco Product License Registration Portal
3. Kopieer je UDI* en PAK in portal en ontvang de licentie (in file format) in de e-mail
4. Maak de licentie publiekelijk beschikbaar (HTTP / FTP / TFTP)
5. Log in op de router en voer uit “license install %location + filename%”
6. Reload de router

*De UDI van je apparaat is de Unique Device Identifier. Deze kun je opvragen met het commando:
#show license udi

De UDI bestaat uit 2 delen:

1. Product ID (PID)
2. Serial Number (SN)

Om de licentie in zijn geheel te tonen gebruik je het commando:
#show license

Automatisch licenties toekennen en activeren kan met de gratis Cisco software CLM (Cisco License Manager). Deze staat in contact met de Cisco Product License Registration Portal en met alle devices van het bedrijf.

Trail / Technology Evaluaties

- Technology Packages uitproberen zonder PAK
- Volgens “right to use” license
- 60 dagen trail, daarna nog actief maar mag niet meer gebruikt worden (volgens Right to Use licentie)

Het activeren van een evaluatie functie gaat als volgt:

()license boot module %type router% technology-package %type feature%

Dus bv.:

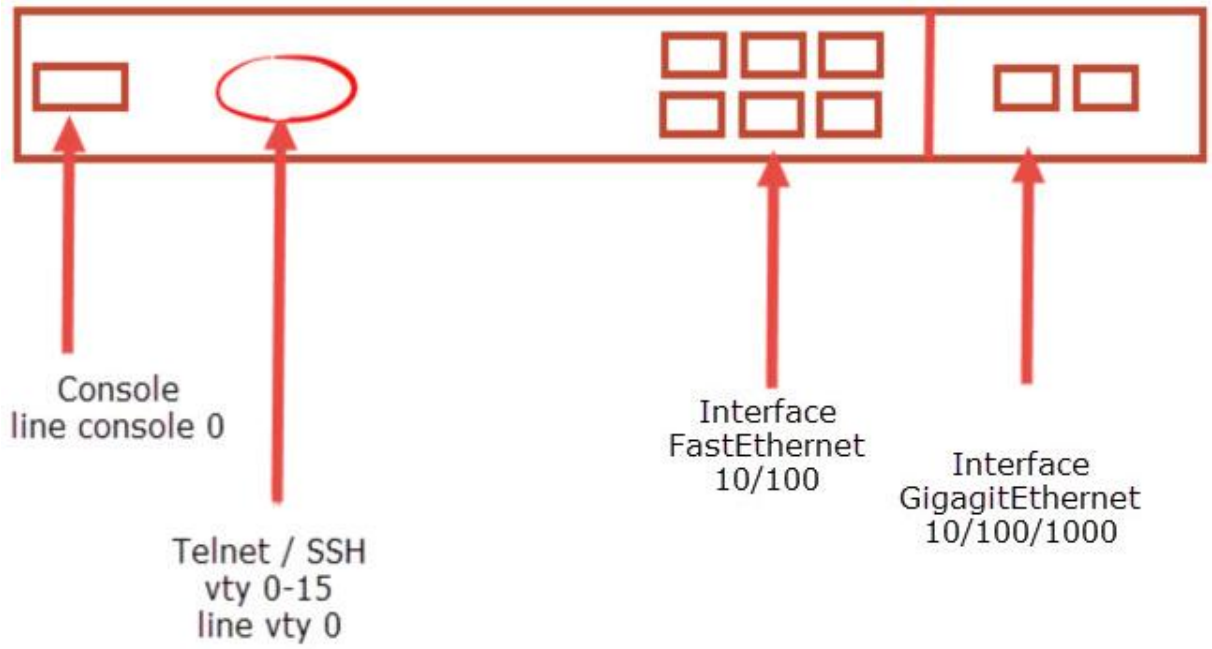
()license boot module c2900 technology-package securityk9

IOS staat voor Internetwork Operating System

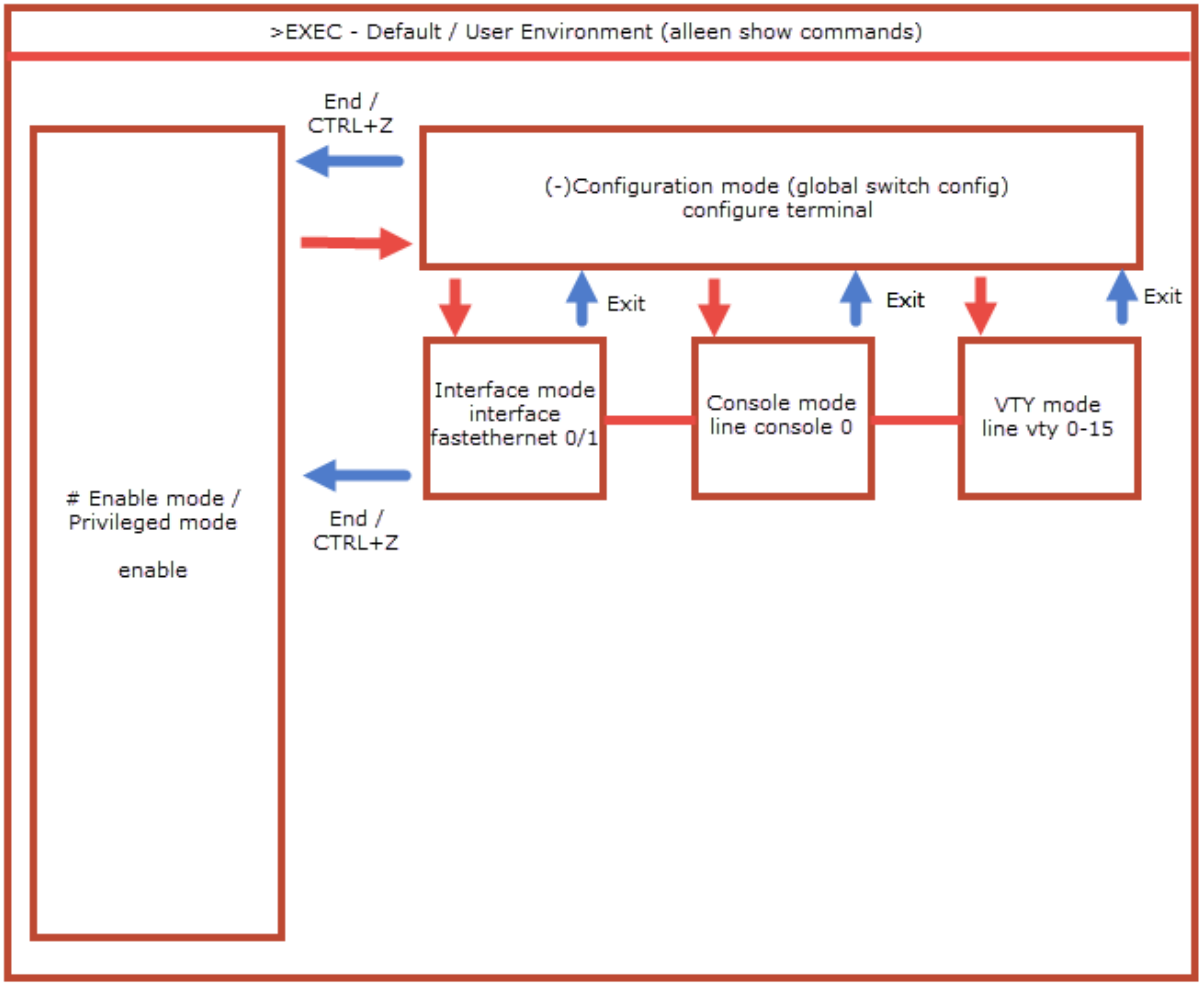
Console Serial Connection
Een console connection met een Cisco Switch maak je met een rollover kabel. Je stelt je terminal in op de volgende waardes:

Bits per Seconde: 9600
Flow Control: No Hardware Flow Control
8N1: (8-bit ASCII – No Parity Bits – 1 stop bit)

Cisco terminologie:



IOS levels



Show Commands

Switch informatie bekijken:
>show version

Config opslaan en overzetten

Opslaan van config:
#copy running-config startup-config

Config naar TFTP
#copy running-config TFTP

Config van TFTP
#copy TFTP running-config

NVRAM (startup-config) verwijderen
#erase nvram
#erase startup-config

Telnet en SSH

Setup Telnet op alle 16 vty poorten
>enable
#configure terminal
()enable secret password
()service password-encryption
()line vty 0 15
(-)password %wachtwoord%
(-)login

Setup SSH op alle 16 vty poorten (en disable telnet)

1. Config hostnaam:

>enable
#configure terminal
()hostname %hostnaam%

2. Config domeinnaam:

()ip domain-name %domeinnaam%

3. Maak een certificaat aan om pakketten te encrypten

()crypto key generate rsa
(gebruik 2048 bits en gebruik de hostname + domainname als naam b.v. cisco.cisco.com.

4. Gebruik alleen SSH versie 2

()ip ssh version 2

5. Configureer de VTY lijn voor SSH

()line vty 0 15
(-)login local
(-)transport input ssh

6. Maak een user aan om in te loggen

(-)username %gebruikersnaam% privilege 15 secret %wachtwoord%

7. Zet een timeout van 5 minuten op de inlogtijd
(-)exec-timeout 5

Setup console 0 en lijn vty 0-15 met default wachtwoorden
>enable
#configure terminal
()enable secret %wachtwoord% <-wachtwoord voor enable mode
()hostname %hostnaam% <-Hostnaam apparaat

()line console 0 <-Open sub-interface line 0
(-)password %wachtwoord% <-Zet wachtwoord voor line 0
(-)login <-Zorg ervoor dat er om het ww wordt gevraagd
(-)exit <-Exit de line 0 config
()line vty 0 15 <-Ga naar de config voor lijn VTY 0-15
(-)password %wachtwoord% <- Zet wachtwoord voor lijn vty 0-15
(-)login <-Zorg ervoor dat er om het ww wordt gevraagd
(-)end <-Terug naar enable mode
#

Credentials & secret credentials

Gebruik lokale credentials
Je kunt ook gebruik maken van lokaal opgeslagen gebruikersnamen en wachtwoorden. Hiervoor ga je als volgt te werk:
>enable
#username %gebruikersnaam% password %wachtwoord%
#configure terminal
()line vty 0 15
(-)login local

Beveiligen lokale credentials:
>enable
#username %gebruikersnaam% secret %wachtwoord%

Encrypt wachtwoorden zodat deze versleuteld in de console & config getoond worden.
Deze encryptie is nog relatief gemakkelijk te kraken:
>enable
#service password-encryption

Disable secret enable wachtwoord
>enable
#configure terminal
() no enable secret

Banners

3 soorten banners:

MOTD (Message of the Day) - Voor login (bij openen shell)
Login - Voor login, na MOTD
Exec - Na enable

Banner maken:
>enable
#configure terminal
()banner %type% %end character% (banner login #)

*Het End Character zorgt ervoor dat de banner creatie afgesloten wordt. Dit karakter mag je dus niet in de banner gebruiken. Verder zijn alle tekens en Enters toegestaan.

Commando history & notifications

Tijdelijk meer commando's (voor up en down arrows) opslaan voor ingelogde sessies:
>enable
#terminal history size %aantal%

Vaste commando cache aanpassen voor serial en VTY verbindingen:
>enable
#configure terminal
()line vty 1-15 <- kies je lijn / type
(-)history size %aantal%

Geen IOS meldingen (uitschakelen)
()no logging console

Alleen meldingen op juiste momenten (na commando's):
()logging synchronous

Switch IP

IP adres op switch plaatsen:
Het IP adres van de switch wordt op een virtuele NIC geplaatst (geen fysieke poort). Dit management IP kan maar op 1 VLAN gezet worden. Dit werkt als volgt:

Statisch:
>enable
#configure terminal
()interface vlan1
(-)ip address 192.168.1.240 255.255.255.0
(-)no shutdown
(-)exit
()ip default-gateway 192.168.1.1

Dynamisch (DHCP)
>enable
#configure terminal
()interface vlan1
(-)ip address dhcp
(-)no shutdown

IP adres info bekijken:
>enable
#show interface vlan1

DHCP info bekijken:
>enable
#show dhcp lease

Gateway bekijken:
>enable
#show ip default-gateway

Switch Interface Configureren

Algemeen:
>enable
#configure terminal
()inteface fastethernet 0/1 <- Kies de interface
OF
()inteface range fastethernet 0/1 – 0/10 <- Kies een interface range

Interface configuratie mogelijkheden:
(-)duplex %half/full% <- Duplex
(-)speed %10/100/1000% <- Snelheid
(-)description %omschrijving% <- Naam / titel

Info alle interfaces bekijken:
>enable
#show interface status

Laat de MAC tabel zien:
show mac address-table

Laat alleen dynamisch geleerde MAC adressen zien:
show mac address-table dynamic

Router interface commando's

Laat een overzicht zien van alle interfaces:
>enable
#show ip interface brief

Laat details van een interface zien:
>enable
#show interface serial 0/0/0

Zet andere clock-rate op een seriële lijn:
>enable
#interface serial 0/0/0
()clock rate 128000

Routes op een router

Routetabel laten zien:
>enable
#show ip route

Maak een statische route aan naar een ander subnet
>enable
#configure terminal
()ip route %netwerk id% %subnetmask% %next-hop router%
Voorbeeld: ()ip route 192.168.100.0 255.255.255.0 192.168.50.254

Maak een statische default route aan
>enable
#configure terminal
()ip route 0.0.0.0 0.0.0.0 %outgoing interface %
Voorbeeld: ()ip route 0.0.0.0 0.0.0.0 serial0/0/1

Router VLAN & Trunking

VLAN's bekijken:
>enable
#show vlans

Activeer 802.1Q trunking op een router voor VLAN 10 en het native LAN:
>enable
#interface gigabitethernet 0/0.10 <- Maak subinterface 10 aan op gigabitethernet 0/0
(-)encapsulation dot1q 10 <- Schakel 802.1Q encapsuation in voor VLAN 10
(-)ip address 192.168.10.254 255.255.255.0 <- Geef subinterface 10 een IP + Mask in juiste subnet
(-)exit
()ip address 192.168.1.254 255.255.255.0 <- Geef de fysieke interface een IP + Mask*

*Door het inschakelen van een IP + Mask op de fysieke interface wordt de fysieke interface gebruikt voor het native VLAN. Let erop dat je geen encapsulation configureerd op de fysieke interface. Je kunt je native VLAN ook over een subinterface laten lopen door deze aan te maken en te configureren met het commando:
(-)ip address 192.168.10.254 255.255.255.0 <- De interface moet een IP + Mask hebben
(-)encapsulation dot1q %VLAN nummer% native <- Activeer native VLAN X op subinterface

Layer 3 Switch Routing

Activeer de mogelijkheid om tussen VLAN 10 & 20 te routeren op een layer 3 switch:
>enable
#configure terminal
()sdm prefer lanbase-routing <- Activeer hardware support voor layer 3 routing
()reload <- Reload de switch (ook nodig om routing te activeren)
>enable
#configure terminal

()ip routing <-Activeer IPv4 routing
()interface vlan 10 <-Maak VLAN 10 aan waar naartoe gerouteerd kan worden
(-)ip address 192.168.10.240 255.255.255.0 <-Geef VLAN interface een IP + subnetmask (uniek)
(-)no shutdown <- Alleen als de switch de interface aanmaakt als shutdown
()interface vlan 20 <-Maak VLAN 20 aan waar naartoe gerouteerd kan worden
(-)ip address 192.168.20.240 255.255.255.0 <-Geef VLAN interface een IP + subnetmask (uniek)
(-)no shutdown <- Alleen als de switch de interface aanmaakt als shutdown

Geef een interface een 2e IP adres om tussen 2 subnets te routeren:
>enable
#configure terminal
()interface gigabitethernet 0/0
(-)ip address 192.168.3.254 255.255.255.0
(-)ip address 192.168.4.254 255.255.255.0 secondary <- Voeg toe als secondary addres

Port Security

Poort Security instellen:

>enable
#configure terminal
()inteface fastethernet 0/1
(-)switchport mode access <- Of trunk....
(-)switchport port-security <- Enables Port Security

Aantal MAC adressen vergroten:
(-)switchport port-security maximum %aantal%

Switchport Port-Security mode aanpassen:
(-)switchport port-security violation %protect / restrict / shutdown%

Geef een specifiek device toegang op de poort:
(-)switchport port-security mac-address %MAC address%

Zet de port-security poort in Sticky learning:
(-)switchport port-security mac-address sticky

VLAN's

Maak een VLAN aan en geef deze een naam:
>enable
#configure terminal
()vlan %VLAN ID% <- Maak een VLAN aan of ga in de config van een bestaand VLAN
(-)name %VLAN naam%

Maak interface 0/10 en 0/11 een access switchport en koppel deze aan VLAN:
>enable
#configure terminal
()interface range fastethernet 0/10 – 0/11

(-)switchport mode access
(-)switchport access vlan %VLAN ID% <- Als VLAN met dit ID niet bestaat wordt hij aangemaakt

Laat trunk info zien:
>enable
#show interfaces trunk

OSPF

Laat OSPF processen zien:
#show ip ospf

Laat de OSPF database zien:
#show ip ospf database

Laat alle OSPF neightbours zien:
#show ip ospf neighbor

Laat alle OSPF interfaces zien (inclusief area's en passieve interfaces – maar staat niet aangegeven dat passief is):
#show ip ospf interface brief

Laat alle OSPF interfaces zien incl. de passieve status
#show ip ospf interface

Stel een loopback interface in met interfacenummer 10 en IP 192.168.100.10:
()interface loopback10
(-)ip address 192.168.100.10 255.255.255.0

Activeer OSPF (2 interfaces + serial) in area 0
>enable
#configure terminal
()interface fastethernet 0/0
(-)ip address 192.168.150.0 255.255.255.0 <- Stel een interface in met een IP adres
(-)no shutdown <- Zet de interface in up modus
(-)exit
()interface fastethernet 0/1
(-)ip address 192.168.200.0 255.255.255.0 <- Stel een 2e interface in met een IP adres
(-)no shutdown <- Zet de interface in up modus
(-)exit
()interface serial 0/0/0
(-)ip address 10.20.0.254 255.255.0.0 <- Stel seriele interface in met een IP adres
(-)clock rate 64000 <- Verkregen van CSU
(-)bandwidth 64 <- Verkregen van CSU
(-)no shutdown
(-)exit
()router ospf 1 <- Activeer OSPF ID 1
(-)network 192.168.150.0 0.0.0.255 0 <- Include FE0/0 met wildcard (netwerk)
(-)network 192.168.200.0 0.0.0.255 0 <- Include FE0/1 met wildcard (netwerk)
(-)network 10.20.0.254 0.0.0.0 0 <- Include serial 0/0/0 met wildcard (1 IP)

Pas het router ID aan naar 1.0.0.0 voor OSPF proces 1

()router ospf 1
(-)router-id 1.0.0.0

Je hebt een router met 40 poorten maar alleen gigabitethernet 1/10 en 1/11 moeten OSPF enabled hebben:

>enable
#configure terminal
()router ospf 1 <- Activeer OSPF ID 1
(-)passive interface default <- Zet alle interfaces op passive OSPF
(-)no passive interface gigabitehternet1/10 <- Zet gigabitethernet 1/10 op OSPH actief
(-)no passive interface gigabitehternet1/11 <- Zet gigabitethernet 1/11 op OSPH actief

Als de router verbonden is met het internet zorg er dan voor dat deze router de default route publiceert naar andere OSPF devices:

>enable
#configure terminal
()ip route 0.0.0.0 0.0.0.0 serial0/0/1 <- Maak default route aan over serial0/0/1
()router ospf 1 <- Ga in OSPF ID 1 configuratie
(-)default-information originate <- Zorgt ervoor dat default route gepubliceerd wordt

Activeer multi-area OSPF waarbij we 2 LAN interfaces hebben die trunken naar andere routers

>enable
#configure terminal
()interface gigabitethernet0/1
(-)encapsulation dot1q <- Activeer trunking
(-)ip address 192.168.1.254 255.255.255.0 <- Zet IP op interface
(-)exit
()interface gigabitethernet0/2
(-)encapsulation dot1q <- Activeer trunking
(-)ip address 192.168.2.254 255.255.255.0 <- Zet IP op interface
(-)exit
()interface gigabitethernet0/10
(-)ip address 192.168.10.254 255.255.255.0 <- Zet IP op interface
(-)exit
()interface gigabitethernet0/11
(-)ip address 192.168.11.254 255.255.255.0 <- Zet IP op interface
(-)exit
()router ospf 1 <- Maak of activeer OSPF proces 1
(-)network 192.168.1.254 0.0.0.0 area 0 <- Zet specifiek netwerk in area 0
(-)network 192.168.2.254 0.0.0.0 area 0 <- Zet specifiek netwerk in area 0
(-)network 192.168.10.254 0.0.0.0 area 1 <- Zet specifiek netwerk in area 1
(-)network 192.168.11.254 0.0.0.0 area 2 <- Zet specifiek netwerk in area 2
(-)router-id 1.1.1.1 <- Zet een handmatig RID
(-)passive-interface gigabitethernet0/1 <- Verstuur geen OSPF over de trunk
(-)passive-interface gigabitethernet0/2 <- Verstuur geen OSPF over de trunk

Verander de cost van een interface naar 10:
()interface fastethernet0/0
(-)ip ospf cost 10

OSPFv3

Laat OSPFv3 processen zien:
#show ipv6 ospf

Laat de OSPFv3 database zien:
#show ipv6 ospf database

Laat alle OSPFv3 neightbours zien:
#show ipv6 ospf neighbor

Laat door OSPFv3 geleerde routes zien:
#show ipv6 route ospf

Laat zien op welke interfaces OSPF3 actief is
#show ipv6 ospf interface brief
OF
#show ipv6 ospf protocols

Activeer OSPFv3 (2 interfaces + serial) in area 0
>enable
#configure terminal
()ipv6 unicast-routing
()interface fastethernet 0/0
(-)ipv6 address 2001:db8:1111:4::1/64 <- Stel een interface in met een IP adres
(-)no shutdown <- Zet de interface in up modus
(-)exit
()interface fastethernet 0/1
(-)ipv6 address 2001:db8:1111:5::1/64 <- Stel een 2e interface in met een IP adres
(-)no shutdown <- Zet de interface in up modus
(-)exit
()interface serial 0/0/0
(-)ipv6 address 2001:db8:1111:1::1/64 <- Stel seriele interface in met een IP adres
(-)clock rate 64000 <- Verkregen van CSU
(-)bandwidth 64 <- Verkregen van CSU
(-)no shutdown
(-)exit
()ipv6 router ospf 1 <- Activeer OSPF ID 1
(-)router-id 1.1.1.1 <- Stel router ID in
(-)interface fastethernet 0/0
(-)ipv6 ospf 1 area 0 <- Zet de interface in de juiste area
(-)interface fastethernet 0/1
(-)ipv6 ospf 1 area 0 <- Zet de interface in de juiste area
(-)interface serial 0/0/0
(-)ipv6 ospf 1 area 0 <- Zet de interface in de juiste area

EIGRP

Bekijk alle EIGRP interfaces
#show ip eigrp interfaces detail

Bekijk de EIGRP Topologie
#show ip eigrp topology

Bekijk EIGRP Neighbors:
#show ip eigrp neighbors

Bekijk de EIGRP routes (aangegeven in routetabel met code D)
#show ip route eigrp

Stel EIGRP Router ID (RID) in op 10.10.100.1
()eigrp route-id 10.10.100.1

Verander de waardes van een interface zodat EIGRP een andere successor route en FS route kiest:
>enable
#configure terminal
()interface serial 0/0/0
(-)bandwidth 1500 <- Verlaag bandwidth om de metric te verhogen

Beter is om de interfaces in te stellen op de actuele bandwidth, verander dus de delay:
>enable
#configure terminal
()interface serial 0/0/0
(-)delay 123 <- Verlaag delay naar 1230 microseconds (123 sec)

Verander de helo interval naar 20 seconde:
>enable
#configure terminal
()ip helo-interval eigrp 1 20 <- 20 seconde helo voor EIGRP 1

Activeer EIGRP (2 interfaces + serial):
>enable
#configure terminal
()interface fastethernet 0/0
(-)ipv6 address 192.168.10.10 <- Stel een interface in met een IP adres
(-)no shutdown <- Zet de interface in up modus
(-)exit
()interface fastethernet 0/1
(-)ipv6 address 192.168.20.10 <- Stel een 2e interface in met een IP adres
(-)no shutdown <- Zet de interface in up modus
(-)exit
()interface serial 0/0/0
(-)ipv6 address 192.168.100.10 <- Stel seriele interface in met een IP adres

(-)clock rate 64000 <- Verkregen van CSU
(-)bandwidth 64 <- Verkregen van CSU
(-)no shutdown
(-)exit
()router eigrp 1 <- Start EIGRP proces met Autonomous System Nr
(-)network 192.168.10.0 0.0.0.255 <-Activeer EIGRP op alle 192.168.10.x interfaces
(-)network 192.168.20.0 0.0.0.255 <-Activeer EIGRP op alle 192.168.20.x interfaces
(-)network 192.168.100.0 0.0.0.255 <-Activeer EIGRP op alle 192.168.100.x interfaces

DHCP

Laat alle DHCP leases zien:
#show ip dhcp binding

Laat alle DHCP pool informatie zien:
#show ip dhcp pool %poolname%

Laat DHCP server statistieken zien:
#show ip dhcp server statistics

Stel een DHCP server "IP Helper" in waarbij de host verbonden is met router interface fastethernet0/3 (192.168.1.254) en de DHCP server (192.168.10.1) verbonden is met fastethernet0/9 (192.168.10.254)
>enable
#configure terminal
()interface fastethernet0/3
(-)ip helper-address 192.168.10.1

Stel een DHCP pool 192.168.150.50-100 in op de router 192.168.150.1 en exclude 192.168.150.60-70:
>enable
#configure terminal
()ip dhcp exclude-address 192.168.150.60 192.168.150.70 <- Exclude adres range
()ip dhcp exclude-address 192.168.150.1 192.168.150.49 <- Exclude adres range
()ip dhcp exclude-address 192.168.150.101 192.168.150.254 <- Exclude adres range
()ip dhcp pool DHCPPool1 <- Maak DHCPPool1
(-)network 192.168.150.0 255.255.255.0 <- Stel pool adres in op netwerk
(-)default-router 192.168.150.1 <- Stel default router in
(-)dns-server 192.168.150.1 8.8.8.8 <- Stel DNS servers in
(-)lease 8 4 30 < Zet lease op 8 dagen, 4 uur, 30 min
(-)domain-name mijnnetwerk.nl <- Stel DNS domeinnaam in
(-)exit
()interface fastethernet0/3
(-)ip helper-address 192.168.168.150.1 <- Zet IP helper naar interne DHCP

DNS

Stel een router in als DNS server om te forewarden naar 8.8.8.8 met 1 statisch adres:
>enable
#configure terminal
()ip domain-lookup <- Enables DNS
()ip name-server 8.8.8.8 <- Zet foreward adres
()ip host mijnnaamisrouter.com 192.168.150.1 <- Zet statisch adres

Access Control Lists - ACL

Laat alle Access Control Lists zien
#show ip access-lists

Troubleshoot een ACL
()access-list 1 permit 192.168.1.1 log

Gebruik een standaard numbered ACL om 1 IP te whitelisten
()access-list 1 permit 192.168.1.1

Gebruik een standaard numbered ACL om 1 subnet te whitelisten
>enable
#configure terminal
()access-list 1 permit 192.168.1.0 0.0.0.255
()interface serial 0/0/0
(-)ip access-groep 1 in

Edit named ACL en verwijder lijn 5 en voeg een nieuwe regel toe op lijn 100
()ip access-list extended Default_Deny <- Enter (of maak) de Extended Named list “Default_Deny”
(-)do show ip access-list Default_Deny <- Laat de sequence numbers zien van de individuele lijnen
(-)no 5 <- Verwijder lijn / regel 5
(-)100 deny host 192.168.1.1 192.168.2.0 0.0.0.255 any <- Voeg een nieuwe lijn toe op positie 100

Network Address Translation – NAT

Bekijk NAT mappings:
#show ip nat translations

Bekijk NAT statistieken:
#show ip nat statistics

Schakel statische NAT in voor 1 host op 1 interface
>enable
#configure terminal
()interface FastEthernet0/1 <- Open interface voor activatie NAT
(-)ip nat inside <-Schakel interface in om mee te doen met NAT op inside netwerk
(-)ip nat outside <-Schakel interface in om mee te doen met NAT op outside netwerk
(-)ip nat source static 192.168.1.1 200.1.1.10 <- Map IP 192.x.x.x statisch aan extern IP 200.x.x.x

Schalel dynamic NAT in op 1 interface
>enable
#configure terminal
()interface FastEthernet0/1 <- Open interface voor activatie NAT
(-)ip nat inside <-Schakel interface in om mee te doen met NAT op inside netwerk
(-)ip nat outside <-Schakel interface in om mee te doen met NAT op outside netwerk
(-)exit
()ip nat pool MijnNAT 200.1.1.10 200.1.1.15 255.255.255.250

<- Maak de NAT pool "MijnNAT" met 6 publieke IP's. De opgegeven range moet in hetzelfde (opgegeven) subnetmask vallen

()ip nat inside source list 1 pool MijnNAT <- Maak NAT mappings gebaseerd op hosts die overeenkomen op ACL 1 voor pakketjes die binnenkomen op de inside interface. Geef deze hosts een inside global adres uit de pool genaamd "MijnNAT".

Schalel NAT Overload (PAT) in (1-op-1)
>enable
#configure terminal
()interface FastEthernet0/1 <- Open interface voor activatie NAT
(-)ip nat inside <-Schakel interface in om mee te doen met NAT op inside netwerk
(-)ip nat outside <-Schakel interface in om mee te doen met NAT op outside netwerk
(-)exit
()ip nat inside source list 1 interface serial0/0/0 overload
<- Maak NAT mappings gebasseerd inside hosts die overeenkomen op ACL 1 voor pakketjes die binnenkomen op de inside interface. Map deze hosts aan het global address van serial 0/0/0

IPv6

Maak NDP neighbor tabel leeg
()clear ipv6 neighbor

Bekijk NDP neighbor tabel:
#show ipv6 neightbors

Bekijk neighbor ipv6 routers
#show ipv6 routers

Laat alle IPv6 settings zien van de interfaces
#show ipv6 route

Laat alle IPv6 local routes (host IP's) zien van de interfaces
#show ipv6 route local

Laat alle IPv6 static routes zien van de interfaces
#show ipv6 route static

Maak een statisch IPv6 adres aan:

>enable
#configure router
()ipv6 unicast-routing <- Stel de router in om IPv6 te routeren
()interface fastethernet0/1
(-)ipv6 address 2001:DBB:1111:3::2/64

Maak een statische IPv6 route aan:
>enable
#configure router
()ipv6 route 2001:db8:1111:2::/64 s0/0/0 <- Route - Prefix length - Outgoing interface

Maak een statische IPv6 route aan waarbij de volgende hop een link-local adres is:
>enable
#configure router
()ipv6 route 2001:db8:1111:2::/64 s0/0/0 FE80::FF:FE00:2
<- Route - Prefix length - Outgoing interface - Next Hop Link Local IPv6

Maak een statische default route aan
>enable
#configure router
()ipv6 route ::/0 s0/0/0 <- Default Route - Prefix length - Outgoing interface

Maak een EUI-64 adres aan:
>enable
#configure router
()ipv6 unicast-routing <- Stel de router in om IPv6 te routeren
()interface fastethernet0/1
(-)ipv6 address 2001:DB8:1111:1::/64 eui-64 <- Stel hier de prefix in met toevoeging eui-64.

Stel de interface in om via DHCPv6 het IPv6 adres te ontvangen:
>enable
#configure router
()interface fastethernet0/1
(-)ipv6 address dhcp

Stel een inteface in om DHCP te relayen
>enable
#configure router
()interface fastethernet0/1
(-)ipv6 dhcp relay destination 2001:DB8:1111:3::8

Stel de interface in om via SLAAC het IPv6 adres te ontvangen:
>enable
#configure router
()interface fastethernet0/1
(-)ipv6 address autoconfig

Spanning Tree

Bekijk spanning tree events:
#debug spanning-tree events

Laat spanning-tree informatie van VLAN 10 zien:
#show spanning-tree vlan 10

Laat spanning-tree bridge informatie zien van VLAN 10:
#show spanning-tree vlan 10 bridge

Laat de root bridge van VLAN 10 zien:
#show spanning-tree vlan 10 root

Laat de etherchannel configuratie zien:
#show etherchannel summary

Laat de etherchannel configuratie zien van channel 1:
#show etherchannel 1 summary

Stel port priority van 112 in op een interface
(-)spanning-tree vlan 10 port-priority 112

First Hop Redundancy Protocol – FHRP

Bekijk de (brief) status van HSRP (Hot Standby Router Protocol):
#show standby brief

Bekijk de (brief) status van GLBP (Gateway Load Balancing Protocol):
#show glbp brief

Configureer HSRP :
>enable
#configure router

()interface gigabitethernet0/0	<- Kies interface (verbonden met netwerk)
(-)ip address 192.168.1.200 255.255.255.0	<- Geef interface een IP
(-)standby version 2	<- Gebruik HSRP versie 2
(-)standby 1 ip 192.168.1.254	<- HSRP groep 1 met virtual IP (in range van interface)
(-)standby 1 priority 110	<- HSRP prioriteit (hoogste = primair, default = 100)
(-)standby 1 name failover-groep	<- Zet “failover-groep” als groepsnaam - niet verplicht

Configureer GLBP:
>enable
#configure router

()interface gigabitethernet0/0	<- Kies interface (verbonden met netwerk)
(-)ip address 192.168.1.200 255.255.255.0	<- Geef interface een IP
(-)glbp 1 ip 192.168.1.254	<- GLBP groep 1 met virtual IP (in range van interface)

(-)glbp 1 priority 110 <- GLBP prioriteit (hoogste = primair, default = 100)
(-)glbp 1 name failover-groep <- Zet “failover-groep” als groepsnaam - niet verplicht

Virtual Private Network – VPN

Laat informatie van tunnel 1 zien:
#show interfaces tunnel1

Maak een GRE tunnel (configureer 1e router) en routeer verkeer statisch:
>enable
#configure terminal
()interface serial0/0/1 <- Geef serial poort een IP
(-)ip address 10.0.0.1
(-)exit
()interface tunnel 1 <- Maak een virtuele tunnel interface nummer 1
(-)ip address 192.168.1.254 255.255.255.0 <- Geef de tunnel interface een intern IP adres
(-)tunnel source serial0/0/1 <- Tunnel start van interface serial0/0/1 (10.0.0.1)
(-)tunnel destination 10.0.0.2 <- Tunnel moet verbinden met ip 10.0.0.2
(-)tunnel mode gre <- Zet tunnel in GRE modus (default modus)
(-)exit
()ip route 192.168.2.0 255.255.255.0 10.0.0.1 <- Maak statische route voor 192.168.2.x netwerk over de tunnel

Maak een GRE tunnel (configureer 2e router) en routeer verkeer OSPF:
>enable
#configure terminal
()interface serial0/0/1 <- Geef serial poort een IP
(-)ip address 10.0.0.2
(-)exit
()interface tunnel 1 <- Maak een virtuele tunnel interface nummer 1
(-)ip address 192.168.2.254 255.255.255.0 <- Geef de tunnel interface een intern IP adres
(-)tunnel source serial0/0/1 <- Tunnel start van interface serial0/0/1 (10.0.0.1)
(-)tunnel destination 10.0.0.1 <- Tunnel moet verbinden met ip 10.0.0.1
(-)tunnel mode gre <- Zet tunnel in GRE modus (default modus)
(-)exit
()router ospf 1 <- Activeer OSPF ID 1
(-)network 10.0.0.0 0.0.0.255 area 0 <- Activeer OSPF op subnet seriale interfaces

Leased Lines HDLC / PPP + PPPOE

Debug PAP / CHAP:
#debug ppp authentication

Bekijk of je te maken hebt met de DCE of DTE kant van de kabel:
#show controllers serial 0/0/0

Configureer een serial interface met HDLC
>enable

#configure terminal
()serial 0/0/0
(-)no shutdown
(-)ip address 10.146.182.12
(-)encapsulation hdlc
(-)clock rate 2000000 <- Als dit de kant van de DCE kabel is
(-)bandwidth 1544 <-In Kbps
(-)description <- Niet verplicht, mogelijkheid om beschrijving te plaatsen

Configureer PPP met CHAP authenticatie:
>enable
#configure terminal
()serial 0/0/0
(-)ip address 10.146.182.12
(-)no shutdown
(-)encapsulation ppp
(-)clock rate 2000000 <- Als dit de kant van de DCE kabel is
(-)exit
()hostname %hostname% <- Dit is de username voor de andere router
()username %gebruikersnaam% password %wachtwoord% <- Zelfde op beide routers
()ppp authentication chap serial 0/0/0

Configureer PPPoE
>enable
#configure terminal
()interface dialer 1 <- Maak virtuele dialer interface
(-)encapsulation ppp <- Zet PPP encapsulation
(-)ip address negotiated <- Stel IP in om van de host te verkrijgen
(-)ppp chap hostname %gebruikersnaam% <- Stel je PPP gebruikersnaam in
(-)ppp chap password %wachtwoord% <- Stel je wachtwoord in
(-)mtu 1492 <- Stel afwijkende MTU size van 1492 in
(-)dialer pool 1 <- Maak interface lid van een dialer pool
(-)exit
()interface gigabitethernet0/1 <- Ga naar fysieke interface (outlet connected) interf.
(-)no ip address <- Verwijder huidige (als bestaande) IP informatie
(-)pppoe-client dial-pool-number 1 <- Stel in dat dial pool 1 gebruikt moet worden

Frame Relay

Laat PVC status + DLCI zien:
#show frame-relay pvc

Laat mappings zien:
#show frame-relay map

Maak een statische mapping aan:
(-)frame-relay map ip 199.1.1.1 51 broadcast <- Voor broadcast & multicast verkeer

Zet Frame Relay op met IETF encapsulatie en waarbij de LMI het type ANSI is:

```
>enable
#configure terminal
()interface serial 0/0/0
(-)encapsulation frame relay
(-)ip address 199.160.10.10 255.255.255.0
(-)frame-relay lmi-type ansi                <- Dit disables autosense
(-)frame-relay map ip 199.160.10.10 53 ietf <- 53 = DLSI van ander netwerk
```

Zet Frame Relay op met een subinterface:

```
>enable
#configure terminal
()interface serial 0/0/0
(-)encapsulation frame relay
(-)interface serial 0/0/0.2 point-to-point  <- Of point-to-multipoint
(--)ip address 199.160.10.10 255.255.255.0
(--)frame-relay interface-dlci 52
```

Troubleshooting

Configureer SNMP v2:

```
>enable
#configure terminal
()ip access-list standard SNMP_Restrict     <- Maak access-list aan
(-)permit host 192.168.1.30                 <- Allow host op ACL
(-)exit
()snmp-server community %wachtwoord% ro  SNMP_Restrict
                                            <- Configureer SNMP v2c read only + ACL
()snmp-server-location %locatie%            <- Beschrijf de locatie
()snmp-server-contact %contactinfo%         <- Beschrijf contactinformatie
```

Configureer Syslog om alleen berichten te versturen met level 0-4:

```
>enable
#configure terminal
()logging console                           <- Router logt naar de console (0-7) = default
()logging buffered                          <- Buffer logberichten (tijdelijk bewaren) =
default
()logging 192.168.1.100                     <- Definieer de logging server
()logging trap 4                            <- Stuur alleen berichten TOT level 4 (0-4)
```

Bekijk Netflow cache op de router:

```
#show ip cache flow
```

Bekijk de monitoring flow op de interfaces (ingress en egress):

```
#show ip flow interface
```

Configureer Netflow:
>enable
#configure terminal
()Interface gigabitethernet0/1
(-)ip flow ingress <- Monitored pakketjes die de interface in gaan
(-)ip flow egress <- Monitored pakketjes die de interface uit gaan
(-)exit
()ip flow-export destination 192.168.1.100 <- Waar wordt de netflow data naartoe gestuurd
()ip flow-export version 9 <- Welke versie van netflow wordt er gebruikt (1,5,7,8,9)
()ip flow-export source loopback 0
<- Gebruik loopback 0 als source van pakketten die naar collector gestuurd zijn

Gebruik CDP om host info te achterhalen van je neighbors:
show cdp neighbors

Gebruik CDP om uitgebreide host info te achterhalen van je neighbors:
show cdp neighbors detail

Gebruik CDP om gedetailleerde info van 1 CDP neighbor te achterhalen:
show cdp entry %neightborname%

Schakel CDP uit op 1 poort:
(-)no cdp

Schakel CDP in zijn geheel uit:
()no cdp run

Help

Neem onderstaande info zeker mee tijdens het examen. Gebruik de eerste 10 minuten intro om onderstaande info op te schrijven zodat je hier gedurende het examen naar terug kunt pakken.

Meest gebruikte show commando's:

- show ip interface brief
- show ip route
- show interfaces
- show version
- show ip protocols
- show protocols
- show arp
- show run
- show vlan
- show interface status
- show access-list
- show cdp neighbor detail
- show interface trunk
- show ip ospf neighbor
- show ip eigrp neighbor

OSI layers:

Nummer		Naam		Ezelsbrug
7	-	Application	-	All
6	-	Presentation	-	People
5	-	Session	-	Seem
4	-	Transport	-	To
3	-	Network	-	Need
2	-	Data	-	Data
1	-	Physical	-	Protoection

2 Commando's

Gebruik een standaard numbered ACL om 1 subnet (inbound) te whitelisten

```
>enable
#configure terminal
()access-list 1 permit 192.168.1.0 0.0.0.255
()interface serial 0/0/0
(-)ip access-groep 1 in
```

NAT aanmaken

```
>enable
#configure terminal
()interface serial0/0/0
(-)ip nat outside
(-)exit
()access-list 100 remark == [Control NAT Service]==
()access-list 100 permit ip 192.168.0.0 0.0.0.255 any
()ip nat pool MyPool 80.134.12.11 80.134.12.18 subnet 255.255.255.248
()ip nat inside source list 100 pool MyPool overload
```