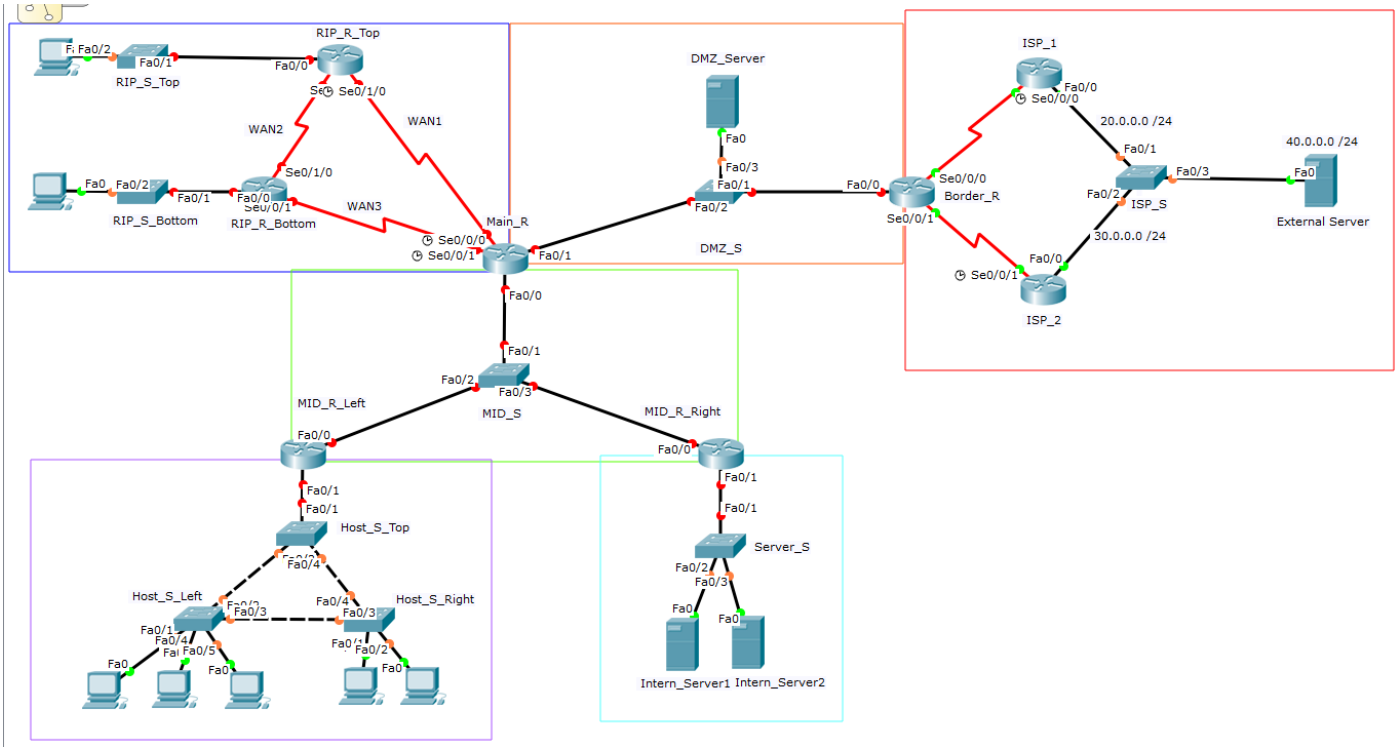
Voorbeeldexamen Network advanced

Onderstaand is een examenachtige oefening (puur te indicatie).

Pas wel op:

- Onderstaand examen is een grote oefening als voorbereiding op het examen. De concepten van VLSM, VLAN's, InterVLAN routing, DHCP, security, statische en dynamische routes komen in deze oefening aan bod. De andere concepten (STP, Etherchannel, FHRP) zullen ook op het examen aan bod komen. Maar deze opgave is een goede oefening. Dit document is de uitleg van het examen en dit dient samen met de packet tracer file gebruikt te worden. In de packet tracer file kan je je progress zien, net zoals op het examen.
- Jullie examen zal twee oefeningen bevatten: configureeroefening (zoals onderstaande opgave, maar dan een kortere versie) + troubleshootoefening (zoals er verschillende te vinden zijn in de Cisco course, en ook tijdens de lessen gemaakt). Die troubleshootoefeningen zijn om jullie begrip van de theorie aan de praktijk te koppelen.

De netwerktopologie van de opgave:



Het examennetwerk bestaat uit vijf interne netwerken (RIP-, MID-, Host-, Server-, en DMZ-netwerk), verbonden met twee externe ISP's.

Het ISP-gedeelte (rode rechthoek) behoeft geen verdere configuraties. Dus ISP_1, ISP_2, ISP_S en de External Server zijn allemaal al correct geconfigureerd.

Ieder device heeft ook al een hostname gekregen, zodat je perfect weet op welk device je configuraties aan het invoeren bent.

Voor de serial links zal er steeds gewerkt worden met een clock rate van 64kbps.

Voor zowel het RIP-, als het Host-netwerk zal er een VLSM-berekening moeten gebeuren voor de IP-adressen. Voor de andere netwerken worden de IP-adressen en subnetmaskers gegeven.

Indien er ergens een paswoord nodig is, zal dit steeds 'cisco' zijn (zonder de aanhalingstekens). Ook zal er zorg moeten gedragen worden dat je steeds paswoorden op een zo veilig mogelijke manier gaat configureren.

Voor de SSH-connecties zal er ook een lokale gebruiker moeten geconfigureerd worden: 'admin' (zonder de aanhalingstekens). Gebruik ook een 2048 bit RSA-sleutel, in het domein 'examen.com'.

Aangezien we voor ieder device een SSH-toegang gaan moeten configureren, mag je een SSH-script maken in notepad. Dit is het enige waarvoor je notepad mag gebruiken!

1 RIP-netwerk (blauw)

1.1 VLSM

Het RIP-netwerk bestaat uit vijf subnetten (RIP_Top, RIP_Bottom, WAN1, WAN2, WAN3), die zo optimaal mogelijk via VLSM moeten berekend worden. Voor RIP_Top en RIP_Bottom is de default gateway het 1ste vrije IP-adres, de PC krijgt het 2de vrije IP, en de switch krijgt het laatste vrije IP-adres van de range. De drie WAN subnetten zijn even groot, daarom wordt eerst WAN1 toebedeeld, daarna WAN2, en vervolgens WAN3.

- Start IP: 10.0.0.0
- Aantal hosts RIP_Top: 100
- Aantal hosts RIP_Bottom: 50
- Aantal hosts WAN1: 2
- Aantal hosts WAN2: 2
- Aantal hosts WAN3: 2

Maak a.d.h.v. bovenstaande specificaties een zo optimaal mogelijke VLSM-verdeling voor de subnetten, en vul onderstaande items in. Deze items staan niet expliciet op punten (wel bij de implementatie ervan in de packet tracer file), en is enkel voor jullie als hulp tijdens de configuraties.

10.0.0.0	Network-ID	Mask	Broadcast
RIP_Top (100 hosts)			
RIP_Bottom (50 hosts)			
WAN1 (2hosts)			
WAN2 (2hosts)			
WAN3 (2hosts)			

	IP-adres	Subnetmasker	Default gateway
Switch RIP_S_Top			
PC in RIP_Top			
Switch RIP_S_Bottom			
PC in RIP_Bottom			
WAN1 Main_R S0/0/0: (1ste IP)			-
RIP_R_Top S0/0/0: (2de IP)			-

WAN2 RIP_R_Top S0/1/0: (1ste IP)			-
RIP_R_Bottom S0/1/0: (2de IP)			-
WAN3 Main_R S0/0/1: (1ste IP)			-
RIP_R_Bottom S0/0/1: (2de IP)			-

Manual Summarization RIP-netwerk

Bereken ook al een optimale samenvatting van het RIP-netwerk (de vijf subnetten die je net bij de VLSM van RIP hebt berekend)

- Deze samenvatting is later nodig voor de PAT-translaties (zie deel DMZ)
- Optimale samenvatting:

1.2 Routers van het RIP-netwerk:

- **Main_R:**
  - Interfaces:
    - Interface S0/0/0
      - Verbonden met RIP_R_Top
      - Configureer IP settings volgens de VLSM-berekeningen, DCE
    - Interface S0/0/1
      - Verbonden met RIP_R_Bottom
      - Configureer IP settings volgens de VLSM-berekeningen, DCE
    - Interface Fa0/0
      - Verbonden met MID_S
      - Deze interface wordt bij het MID-gedeelte geconfigureerd
    - Interface Fa0/1
      - Verbonden met DMZ_S
      - Deze interface wordt bij het DMZ-gedeelte geconfigureerd
  - Default Route
    - Configureer een default route op deze router, naar de Fa0/0 interface van de Border_R, en gebruik makend van de IP notatie (dus niet via de exit-interface).
      - IP-adres van Fa0/0 interface op Border_R: 10.10.0.2 /24
- **RIP_R_Top:**
  - Interfaces:

        - Interface S0/0/0
            - Verbonden met Main_R
            - Configureer IP settings volgens de VLSM-berekeningen, DTE
        - Interface S0/1/0
            - Verbonden met RIP_R_Bottom
            - Configureer IP settings volgens de VLSM-berekeningen, DCE
        - Interface Fa0/0
            - Verbonden met RIP_S_Top
            - Configureer IP settings volgens de VLSM-berekeningen

- **RIP_R_Bottom:**
    - <u>Interfaces:</u>
        - Interface S0/0/1
            - Verbonden met Main_R
            - Configureer IP settings volgens de VLSM-berekeningen, DTE
        - Interface S0/1/0
            - Verbonden met RIP_R_Top
            - Configureer IP settings volgens de VLSM-berekeningen, DTE
        - Interface Fa0/0
            - Verbonden met RIP_S_Bottom
            - Configureer IP settings volgens de VLSM-berekeningen

- **Main_R, RIP_R_Top en RIP_R_Bottom:**
    - <u>RIPv2</u>
        - Configureer RIPv2 op deze drie routers
        - Alle verbonden netwerken van het RIP-netwerk worden aan de RIP-buren doorgegeven.
        - Zorg er voor dat er geen RIP-updates over de Fa0/0 interface worden verstuurd, maar dat dit netwerk wel aan de RIP-buren wordt bekend gemaakt
        - Zorg dat de default route via RIP aan de RIP-buren wordt doorgegeven
    - <u>SSH</u>
        - Configureer alle nodige paswoorden en SSH settings (op alle beschikbare VTY-lines), zodat de gebruiker ‘admin’ via SSH kan inloggen op de router. Disable ook Telnet toegang.

1.3 Switches van het RIP-netwerk

- **RIP_S_Top**
    - <u>IP settings</u>
        - Configureer IP settings volgens de VLSM-berekeningen. Gebruik de default VLAN als SVI
    - <u>SSH</u>

        - Configureer alle nodige paswoorden en SSH settings (op alle beschikbare VTY lines), zodat de gebruiker ‘admin’ via SSH kan inloggen op de switch. Disable ook Telnet toegang.
    - MAC filtering
        - Zorg voor sticky MAC filtering op de fa0/2 interface naar de PC. Gebruik de default settings

- **RIP_S_Bottom**
    - IP settings
        - Configureer IP settings volgens de VLSM-berekeningen. Gebruik de default VLAN als SVI
    - SSH
        - Configureer alle nodige paswoorden en SSH settings (op alle beschikbare VTY lines), zodat de gebruiker ‘admin’ via SSH kan inloggen op de switch. Disable ook Telnet toegang.
    - MAC filtering
        - Zorg voor sticky MAC filtering op de fa0/2 interface naar de PC. Gebruik de default settings

1.4 PC’s van het RIP-netwerk

- **De 2 PCs van het RIP netwerk**
    - IP settings
        - Configureer IP settings volgens de VLSM-berekeningen.
    - Check SSH connectiviteit
        - Via de 2 PCs zou je SSH connectiviteit moeten hebben tot alle devices van het RIP-netwerk

2 Host netwerk (purper)

2.1 VLSM

Het Host netwerk bestaat uit drie subnetten (VLAN10 - Studenten, VLAN20 – Docenten, VLAN30 - Management), die zo optimaal mogelijk via VLSM moeten berekend worden.

De default gateway van iedere VLAN is het 1ste vrije IP-adres uit de range. Voor de VLAN met de switches in: de Host_S_Top switch krijgt het 2de vrije IP-adres, de Host_S_Left het 3de vrije IP-adres, en de Host_S_Right het 4de vrije IP-adres.

De PCs gaan via DHCP hun IP-adres krijgen. Deze DHCP-pools gaan in het MID-netwerk geconfigureerd worden, nml. op de Main_R.

- Start IP: 192.168.0.0
- Aantal hosts VLAN10 - Studenten: 200
- Aantal hosts VLAN20 - Docenten: 50
- Aantal hosts VLAN30 - Management: 20

Maak a.d.h.v. bovenstaande specificaties een zo optimaal mogelijke VLSM-verdeling voor de subnetten, en vul onderstaande items in. Deze items staan niet expliciet op punten (wel bij de implementatie ervan in de packet tracer file), en is enkel voor jullie als hulp tijdens de configuraties.

10.0.0.0	Network-ID	Subnetmasker	Default gateway
VLAN 10 - Studenten			
VLAN 20 - Docenten			
VLAN 20 - Management			

	IP-adres	Subnetmasker	Default gateway
Switch Host_S_Top			
Switch Host_S_Left			
Switch Host_S_Right			

Manual Summarization Host netwerk

Bereken ook al een optimale samenvatting van het Hostnetwerk (de drie VLAN's die je net hebt berekend)

- Deze samenvatting gaan we later immers nodig hebben voor PAT-translaties (zie deel DMZ)
- Optimale samenvatting:

2.2 Router van het Host netwerk

- **MID_R_Left**
  - Interfaces
    - Interface Fa0/0
      - Verbonden met MID_S
      - Deze interface wordt bij het MID-gedeelte geconfigureerd
    - Interface Fa0/1
      - Verbonden met Host_S_Top
      - Gebruik het router-on-a-stick principe op deze interface om de default gateways van de 3 VLANs te maken
        - Gebruik het nummer van de VLAN om de subinterface te maken (bv VLAN10 krijgt de subinterface 10)
        - Gebruik de IP settings uit uw VLSM-berekeningen voor het Host netwerk
        - VLAN30 is de Management VLAN, maar zal ook de native VLAN zijn
        - Configureer de subinterfaces om als DHCP Relay te dienen, en de DHCP requests door te sturen naar de Fa0/0 interface (172.16.0.1) van de Main_R
  - MID
    - De configuratie wordt hieronder in het MID- gedeelte gedaan.
  - SSH
    - Configureer alle nodige paswoorden en SSH settings (op alle beschikbare VTY lines), zodat de gebruiker 'admin' via SSH kan inloggen op de router. Disable ook Telnet toegang.

2.3 Switchen van het Host netwerk

- **Op de drie switchen (Host_S_Top, Host_S_Left, Host_S_Right)**
  - VLANs
    - Maak de drie VLAN's aan, met de juiste naam:
      - VLAN10, naam: Studenten
      - VLAN20, naam: Docenten
      - VLAN30, naam: Management
  - IP Settings
    - Configuur de juiste VLAN (SVI) met de IP Settings die je in de VLSM hebt uitgerekend voor de switches uit het Host netwerk.
  - Access en Trunk ports
    - Maak de juiste interfaces access / trunk
      - Expliciet trunk maken, en niet laten afhangen van DTP
      - VLAN30 is de native VLAN
      - Filter iedere trunk zodat ze enkel berichten van VLAN10, VLAN20, en VLAN30 doorlaten
      - Om te controleren welke interfaces access of trunk zijn, en eventueel behoren tot welke VLAN: zie het deel Interfaces hier net onder
  - Interfaces
    - Host_S_Top
      - via Fa0/1 verbonden met MID_R_Left

- via Fa0/2 verbonden met Host_S_Left
- via Fa0/4 verbonden met Host_S_Right
- Zorg dat alle niet gebruikte interfaces uitstaan

- Host_S_Left
  - Via Fa0/2 verbonden met Host_S_Top
  - Via Fa0/3 verbonden met Host_S_Right
  - Via Fa0/1 verbonden met PC uit VLAN10, Studenten
  - Via Fa0/4 verbonden met PC uit VLAN20, Docenten
  - Via Fa0/5 verbonden met PC uit VLAN30, Management
  - Zorg dat alle niet gebruikte interfaces uitstaan
- Host_S_Right
  - Via Fa0/3 verbonden met Host_S_Left
  - Via Fa0/4 verbonden met Host_S_Top
  - Via Fa0/1 verbonden met PC uit VLAN10, Studenten
  - Via Fa0/2 verbonden met PC uit VLAN20, Docenten
  - Zorg dat alle niet gebruikte interfaces uitstaan

- SSH
  - Configureer alle nodige paswoorden en SSH settings (op alle beschikbare VTY lines), zodat de gebruiker 'admin' via SSH kan inloggen op de alle switches. Disable ook Telnet toegang.

2.4 PC's van het Host netwerk

Nadat je in het MID-netwerk de DHCP-pools hebt geconfigureerd voor de VLAN's (zie hieronder bij deel MID), zal iedere PC via DHCP zijn IP settings krijgen.

Dan kan je ook pas de connectiviteit gaan testen.

3 Server Netwerk (licht blauw)

3.1 Router van het Servernetwerk

- **MID_R_Right**
  - Interfaces
    - Interface Fa0/0
      - Verbonden met MID_S
        - Deze interface wordt in het MID-gedeelte verder geconfigureerd
    - Interface Fa0/1
      - Verbonden met Server_S
      - Configureer volgende IP Settings
        - 192.168.10.1 /24
  - MID
    - De configuratie wordt hieronder in het MID- gedeelte gedaan.
  - SSH
    - Configureer alle nodige paswoorden en SSH settings (op alle beschikbare VTY lines), zodat de gebruiker 'admin' via SSH kan inloggen op de router. Disable ook Telnet toegang.

3.2 Switch van het Server netwerk

- **Server_S**
  - IP Settings
    - Deze switch gebruikt de default settings qua VLANs, access en trunks ports.
    - Configureer wel de correcte IP Settings.
      - Het IP-adres van de switch is 192.168.10.254 /24.
  - Interfaces (niet te configureren)
    - Interface Fa0/1
      - Verbonden met MID_R_Right
    - Interface Fa0/2
      - Verbonden met Intern_Server1
    - Interface Fa0/3
      - Verbonden met Intern_Server2
  - SSH
    - Configureer alle nodige paswoorden en SSH settings (op alle beschikbare VTY lines), zodat de gebruiker 'admin' via SSH kan inloggen op de router. Disable ook Telnet toegang.

3.3 Servers van het Server netwerk

- **Intern_Server1**
  - Configureer deze server met zijn IP Settings, met een IP-adres van 192.168.10.2
- **Intern_Server2**
  - Configureer deze server met zijn IP Settings, met een IP-adres van 192.168.10.3

4 MID-netwerk (groen)

4.1 Routers van het MID-netwerk

- **Main_R**
    - Interfaces
        - Serial interfaces
            - Deze zijn al geconfigureerd in het RIP-gedeelte
        - Interface Fa0/0
            - Verbonden met MID_S
            - Configureer volgende IP Settings:
                - 172.16.0.1 /29
        - Interface Fa0/1
            - Verbonden met DMZ_S
            - Deze interface wordt bij het DMZ-gedeelte geconfigureerd
    - Static Routing
        - Configureer statische routes op deze router zodat alles werkt
        - Zorg dat de RIP-instelling blijft werken
    - DHCP
        - Configureer de drie DHCP-pools van het Host netwerk op deze router.
        - Gebruik hiervoor de VLSM settings van het host netwerk
        - Gebruik als naam voor de DHCP-pools: DHCP_VLAN10, DHCP_VLAN20, DHCP_VLAN30
        - Zorg er met één commando voor dat de al gebruikte IP-adressen van het management VLAN (gateway en drie Host switches) niet worden uitgedeeld aan hosts
        - Zorg ervoor dat ook de andere IP-adressen die al gebruikt zijn niet worden uitgedeeld
    - SSH
        - SSH-connectiviteit naar deze router heb je al bij het RIP-gedeelte geconfigureerd

- **MID_Left**
    - Interfaces
        - Interface Fa0/0
            - Verbonden met MID_S
            - Configureer volgende IP Settings:
                - 172.16.0.2 /29
        - Interface Fa0/1
            - Verbonden met Host_S_Top
            - Deze interface is reeds bij het Host gedeelte geconfigureerd
    - Static Routing
        - Configureer statische routes op deze router zodat alles werkt
    - SSH

        - SSH-connectiviteit heb je al bij het Host gedeelte geconfigureerd

- **MID_Right**
    - Interfaces
        - Interface Fa0/0
            - Verbonden met MID_S
            - Configureer volgende IP Settings:
                - 172.16.0.3 /29
        - Interface Fa0/1
            - Verbonden met Server_S
            - Deze interface is reeds bij het Server gedeelte geconfigureerd
    - Static Routing
        - Configureer statische routes op deze router zodat alles werkt
    - SSH
        - Configureer alle nodige paswoorden en SSH settings (op alle beschikbare VTY lines), zodat de gebruiker 'admin' via SSH kan inloggen op de router. Disable ook Telnet toegang.

4.2 Switch van het MID-netwerk

- **MID_S**
    - IP settings
        - Configureer volgende IP settings: (gebruik de default VLAN als SVI)
            - IP 172.16.0.4 /29
            - Default gateway is de Fa0/0 interface van Main_R (172.16.0.1)
    - SSH
        - Configureer alle nodige paswoorden en SSH settings (op alle beschikbare VTY lines), zodat de gebruiker 'admin' via SSH kan inloggen op de switch. Disable ook Telnet toegang.

4.3 Tussentijdse connectiviteitstesten

In principe zou nu alles correct geconfigureerd moeten zijn in het RIP, het MID, het Host, en het Server netwerk. Hoewel de connectie tussen het Hostnetwerk, en het RIP-netwerk nog niet volledig zal werken, omdat de bepaalde routes nog niet actief zijn (het is nodig ook het DMZ gedeelte te doen).

Normaal zou je nu vanuit iedere PC in het Hostnetwerk een SSH-connectie moeten kunnen leggen naar iedere router of switch in het Host-, MID-, en Servernetwerk.

Ook zou iedere PC in het Hostnetwerk moeten kunnen surfen naar de IP-adressen van de interne servers (192.168.10.2 en 192.168.10.3).

Best kan je al enkele van deze connectiviteitstesten uitvoeren om te controleren of je al ergens grote fouten hebt gemaakt.

5 DMZ netwerk (oranje)

5.1 Routers van het DMZ netwerk

- **Main_R**
    - Interfaces
        - De serial interfaces zijn al geconfigureerd in het RIP-netwerk
        - De Fa0/0 interface is al geconfigureerd in het MID-netwerk
        - Interface Fa0/1
            - Verbonden met DMZ_S
            - Configureer de IP settings
                - IP-adres 10.10.0.1 /24
    - DHCP

      Dit is al geconfigureerd in het MID-netwerk
    - SSH
        - De SSH-configuratie is al gebeurd in het RIP-netwerk
- **Border_R**
    - Interfaces
        - Interface Fa0/0
            - Verbonden met DMZ_S
            - IP Settings: 10.10.0.2 /24
        - Interface S0/0/0
            - De IP settings zijn al voorgeconfigureerd (IP 20.0.0.1 /24), en behoeft geen verder configuratie
            - Deze interface zal nog wel de externe bron moeten worden voor de Static NAT vertaling van de DMZ_Server (zie item Static NAT hieronder).
        - Interface S0/0/1
            - Deze interface is al volledig voorgeconfigureerd (IP 30.0.0.1 /24), en behoeft geen verdere configuraties.
    - Default Route
        - Configureer een default route naar ISP_1. Gebruik hiervoor de exit-interface notatie.
    - Floating Default Route
        - Configureer een floating default route (met een AD van 20) naar ISP_2. Gebruik hiervoor de exit-interface notatie.
    - Static Routes
        - Configureer de nodige statische routes naar de niet gekende netwerken. Doe dit via het next-hop adres

5.2 Switch van het DMZ netwerk

- **DMZ_S**
    - IP settings
        - Configureer volgende IP settings: (gebruik de default VLAN als SVI)

        - IP 10.10.0.254 /24
        - Default gateway is de Fa0/1 interface (10.10.0.1) van Main_R
    - SSH
        - Configureer alle nodige paswoorden en SSH settings (op alle beschikbare VTY lines), zodat de gebruiker 'admin' via SSH kan inloggen op de switch. Disable ook Telnet toegang.

5.3 Server van het DMZ netwerk

- **DMZ_Server**
    - Configureer deze server met een IP-adres van 10.10.0.3 /24, en gebruik de Fa0/1 interface (10.10.0.1) van de Main_R als default gateway.
    - Deze server zal ook extern bereikbaar zijn via het IP 20.0.0.2 (zoals hierboven bij Static NAT geconfigureerd).

6 ISP netwerk(en) (rood)

Deze netwerken zijn al volledig geconfigureerd. De connectie naar ISP1 is via het 20.0.0.0 /24 netwerk, en de connectie naar ISP2 is via het 30.0.0.0 /24 netwerk.

De externe server heeft het IP-adres van 40.0.0.3.

6.1 Finale Connectiviteitstesten

In principe is nu gans het examennetwerk geconfigureerd, en zouden onderstaande connectiviteitstesten moeten lukken:

Vanuit iedere PC (zowel in het Host netwerk, als het RIP netwerk)

- Surfen naar alle servers:
    - Interne Servers (192.168.10.2 en 192.168.10.3)
    - DMZ Server (10.10.0.3)
    - Externe Server (40.0.0.3) – check de vertaling naar een extern IP
- SSH connectie leggen naar gelijk welk device in het examennetwerk (buiten dan het ISP netwerk)
    - Externe Server kan surfen naar de DMZ Server via het extern bereikbare IP (20.0.0.3)