

LÆS HELE CASEN IGENNEM FØRST

Afvikles i ugerne 2, 3, 5, 6, 7 og 8 (d. 10. januar – 25. februar) (OS III fra d. 7. - 18. marts)

Resume:

Denne 5½ ugers case består af følgende fag: 16857 Serverteknologi I, 16861 Netværk II og 16862 Serverautomatisering I. Valgfaget Operativsystemer III (gælder ikke for EUV 2 elever), afvikles i ugerne 10–11.

Learn:

På hold betegnelsen "22M2HIT01–10.2" under "H2 Case - Servertek, Netværk II og ServerAut" vil du finde alle relevante filer, Casen som PDF, PowerPoints og øvrige materialer som omhandler casen (alle 3 fag)

Udstyr:

1 server til virtualisering, mindst 2 fysiske PC'ere, 3 routere og 2 switche. Patch kabler, strømkabler mm.

Software:

Windows Server 2022 standard Evaluation, Windows 10/11 Enterprise Evaluation og VMWare vSphere Hypervisor 7 (ESXi), pfSense

Følgende filer og documentation finder du på Learn:

- MS produkter kan hentes på: <https://azureforeducation.microsoft.com/devtools>
- VMware vSphere Hypervisor 7.0 (ESXi) og VMware Workstation 16
- pfSense FireWall
- Øvrigt dokumentation, casen og intro

Ellers har jeg en USB med det hele på.

Arbejd i 2-3 mands grupper (gerne 4 grupper á 3 og 2 grupper på 2)

Casen løses i 2-3 mandsgrupper. Gruppen afslutter casen med et PowerPoint fremvisning for klassen, hvor casens mest interessante emner rundes – taletid fordeles ligeligt mellem gruppens medlemmer (15-20 min i alt)

Alle PowerShell (PS) kommando linjer og scripts dokumenteres undervejs og sendes slutteligt til pi@sde.dk

(dokumentationen af PowerShell skal bestå af korte beskrivelser til kommandoerne og scripts)

Ydermere skal konfigurationerne af de 3 routere også sendes til pi@sde.dk – de må gerne lægges sammen med PS dokumentationen.

Dan grupper efter Præstationsstandarder (se næste side):

I skal danne grupper efter nedenstående præstationsniveauer. Der skal afgives karakterer i alle 3 (4) fag, derfor skal gruppen tidligt i forløbet være enig i, hvilke niveauer de følgende 2 fag, **Serverteknologi I og Serverautomatisering I**, skal afvikles på. Karaktergivningen i Netværk II foregår lidt anderledes, da der både er teori og praktik, som en del af bedømmelsen. Det er teorien, som sætter udgangspunktet for niveauet (se side 12) og sammen med den praktiske del bestemmer karakteren. Derfor kan man individuelt vælge niveau i gruppen i Netværk II. Valgfaget Operativsystemer III bedømmes gruppevis for jer som ikke er afkortet i uddannelsen (EUV 2)

Præstationsstandarder for Rutineret-, Avanceret- og Ekspertniveau

Rutineret niveau.

Eleven kan planlægge og gennemføre en opgave eller aktivitet eller løse et problem i en *rutinemæssig eller kendt situation* og omgivelse, alene og i samarbejde med andre. På dette niveau lægges vægt på den personlige kompetence til *selvstændigt* at sætte sig ind i mere komplicerede problemstillinger og til at kommunikere med andre om løsningen heraf. Yderligere lægges vægt på fleksibilitet og omstillingsevne.

Avanceret niveau.

Eleven kan vurdere et problem, kan planlægge, løse og gennemføre en opgave eller aktivitet eller løse et problem også i *ikke-rutinesituationer – alene eller i samarbejde med andre* – under hensyn til opgavens art. På dette niveau lægges vægt på den personlige kompetence til at tage *selvstændigt ansvar* og vise initiativ samt kompetence til selv at formulere og løse faglige og sociale opgaver og problemer. Yderligere lægges vægt på kvalitetssans og kreativitet.

Ekspertniveau

Eleven kan løse *komplekse arbejdsopgaver* og kan *argumentere* for valgte løsninger af opståede problemer. Der lægges vægt på evnen til at kunne bruge allerede opnåede kompetencer i en ny kontekst, på evnen til at arbejde med overblik og deltage i arbejdspladsens innovative processer. På dette niveau lægges vægt på den personlige kompetence til målrettet at kunne planlægge, tilrettelægge, udføre og evaluere arbejdsprocesserne således, at kvaliteten i processen og resultatet sikres. Desuden lægges vægt på, at eleven kan *vurdere og begrunde* behovet for forbedringer af arbejdsprocesser, samt på at eleven kan kommunikere om sin faglighed i alle relevante sammenhænge.

Bedømmelse:

Du bliver bedømt ud fra din selvstændighedsgrad, dokumentation, scriptløsninger, fremlæggelse og kompetencer som ligger i (-eller ud over) fagets beskrevne mål.

Det anbefales, at grupperne sammensættes i enighed om hvilket Niveau der arbejdes ud fra.

Sidst i casen er bedømmelsespunkterne uddybet.

Casebeskrivelse:

Et nyt firmanetværk i Odense og Aarhus skal implementeres, bestående af en Server 2022 Domain Controller (som Core) indeholdende DHCP scope til 2 Netværk, 2 Server 2022 Member servere og Windows 10 klient(er). Der oprettes 3 selvvalgte afdelinger, hver med mindst én Security Gruppe og 5 brugere. På de 2 Member servere sættes en ekstra harddisk (Drev D). Der oprettes en delt mappe til hver afdeling på Server 2.

En stor del af dette administreres med PowerShell (CMDLet) eller PowerShell ISE.

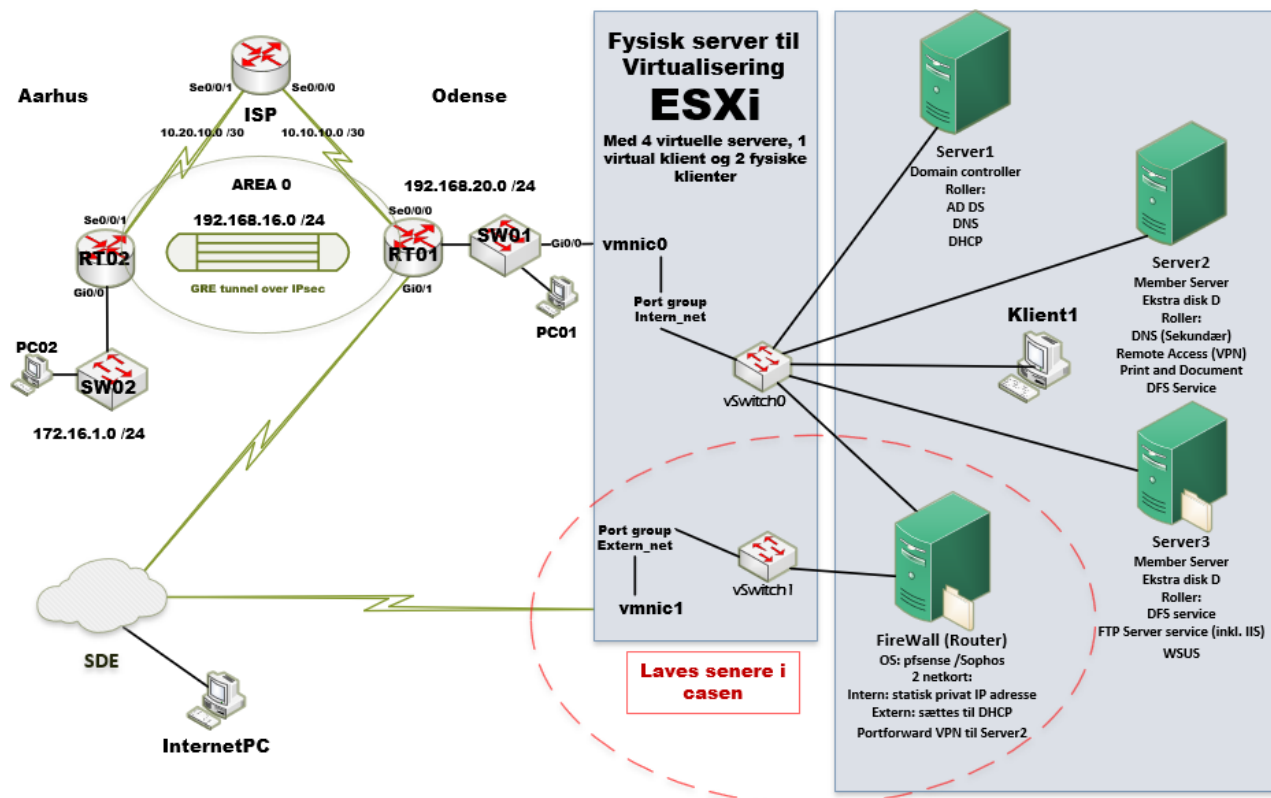
Firmaet vil gerne forberede sig på en overgang til IPv6, så der er aftalt en IPv6 løsning med deres ISP (linjen mellem Odense og Aarhus), så der kan oprettes "duel stack" både i Odense og Aarhus.

I første omgang skal de ansatte kunne tilgå Internettet via en NAT/PAT opsætning på RT01 samt kunne tilgå firmanetværkets Interne Webserver (Server3) fra Internettet via en portforward/statisk NAT på router, RT01. Senere vil NAT delen på RT01 blive erstattet med en FireWall, hvorfra de ansatte nu skal kunne tilgå Internettet samt hele firmaets lokalnet via en VPN opkobling fra Internettet.

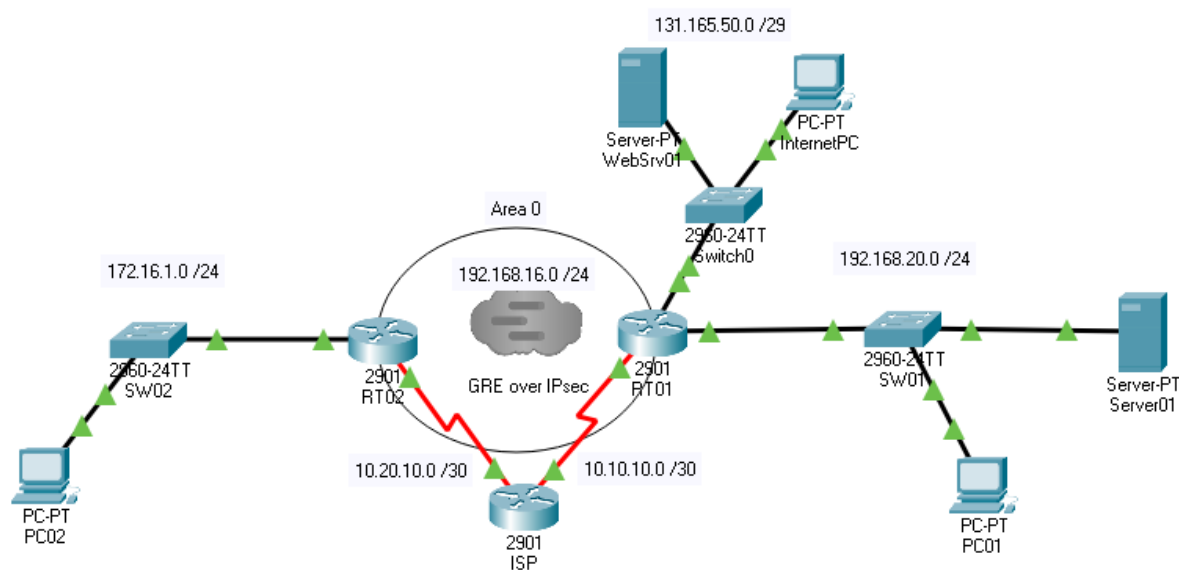
Firmaets hovedsæde i Odense vil gerne have en billig men sikker opkobling til firmaets Aarhus afdeling. Da begge lokationer har en "Internet" opkobling via en ISP udbyder, skal de blot bindes sammen med en GRE tunnel med IPsec, således dynamisk routing også kan udveksles mellem RT01 og RT02.

Case topologien:

Topologi 1 (Rutineret / Avanceret / Ekspert):



Topologi 2 er et eksempel på, at man kan bygge netværks delen op i Packet Tracer, før det implementeres i et "rigtigt" miljø.



Del 1:

Lav som det første en IP-Plan, hvori alle statiske IP adresser og Server- klient navne optræder (skal godkendes af lærer inden du fortsætter)

Eksempel på en IPv4-Plan – der må gerne bruges andre private IP-subnets.

Odense IP-Subnet: 192.168.20.0 /24 (255.255.255.0)					
Enhedsnavn	IP-adresse	Subnet Mask	Default Gateway	DNS	Kommentar
RT01 Gi0/0	192.168.20.1	255.255.255.0	N/A	N/A	
RT01 Gi0/1	DHCP fra SDE	DHCP fra SDE	DHCP fra SDE	DHCP fra SDE	NAT/PAT
SW01	192.168.20.?	255.255.255.0	192.168.20.1	N/A	
FW01 (Int)	192.168.20.?	255.255.255.0	N/A	192.168.20.?	fra Del 8
FW01 (Ext)	DHCP fra SDE	DHCP fra SDE	DHCP fra SDE	DHCP fra SDE	fra Del 8
ESXi01	192.168.20.?	255.255.255.0	192.168.20.1	192.168.20.?	
DCSrv01	192.168.20.?	255.255.255.0	192.168.20.1	192.168.20.?	
MemSrv01	192.168.20.?	255.255.255.0	192.168.20.1	192.168.20.?	
MemSrv02	192.168.20.?	255.255.255.0	192.168.20.1	192.168.20.?	

Aarhus IP-Subnet: 172.16.1.0 /24 (255.255.255.0)					
Enhedsnavn	IP-adresse	Subnet Mask	Default Gateway	DNS	Kommentar
RT02 Gi0/0	172.16.1.1	255.255.255.0	N/A		
SW02	172.16.1.?	255.255.255.0	172.16.1.?		
Klient Scope	172.16.1.100 - 150	255.255.255.0	172.16.1.?	192.168.1.?	

WAN IP-Subnet (RT01 og 02) – GRE tunnel IP-Subnet: 192.168.16.0 /24					
Enhedsnavn	IP-adresse	Subnet Mask	Default Gateway	DNS	Kommentar
RT01 Se0/0/0	10.10.10.1	255.255.255.252	N/A	N/A	AREA 0
RT02 Se0/0/1	10.20.10.1	255.255.255.252	N/A	N/A	AREA 0
ISP Router					
ISP Se0/0/0	Beregn selv	255.255.255.252	N/A	N/A	
ISP Se0/0/1	Beregn selv	255.255.255.252	N/A	N/A	

Eksempel på Ipv6-Plan – der må gerne bruges andre Global Prefix Subnets.

Odense – Global prefix subnet: 2001:db8:acad:20::/64					
Enhedsnavn	Global Unicast	Link-Local	Default Gateway	DNS	Kommentar
RT01 Gi0/0	2001:db8:acad:20::1	FE80::1	N/A	N/A	
RT01 Gi0/1	Ikke mulig				
SW01	Ikke mulig				
FW01 (int)	2001:db8:acad:20::?	Auto	N/A	N/A	fra Del 8
FW01 (ext)	Ikke muligt				
ESXi01	2001:db8:acad:20::?	Auto	FE80::1	2001:db8:acad:20::?/?	
DCSrv01	2001:db8:acad:20::?	Auto	FE80::1	2001:db8:acad:20::?/?	
MemSrv01	2001:db8:acad:20::?	Auto	FE80::1	2001:db8:acad:20::?/?	
MemSrv02	2001:db8:acad:20::?	Auto	FE80::1	2001:db8:acad:20::?/?	
Ekstra Server					
Klient01	DHCPv6	Auto	Auto	DHCPv6	

Aarhus – Global prefix subnet: 2001:db8:acad:50::/64					
Enhedsnavn	Global Unicast	Link-Local	Default Gateway	DNS	Kommentar
RT02 Gi0/0	2001:db8:acad:50::1	FE80::1	N/A	N/A	
SW02	Ikke mulig				
Klient02	DHCPv6	Auto	Auto	DHVPv6	

WAN (RT01 og RT02 – GRE tunnel Global Prefix Subnet: 2001:db8:acad:16::/64					
Enhedsnavn	Global Unicast	Link-Local	Default Gateway	DNS	Kommentar
RT01 Se0/0/0	2001:db8:acad:11::1	FE80::1	N/A	N/A	AREA 0
RT02 Se0/0/1	2001:db8:acad:12::1	FE80::?	N/A	N/A	AREA 0
ISP Router					
ISP Se0/0/0	2001:db8:acad:11::?	FE80::?	N/A	N/A	
ISP Se0/0/1	2001:db8:acad:12::?	FE80::2	N/A	N/A	

Du skal som minimum implementere IPv6 på Odense siden. Hvis du arbejder i Ekspert niveau skal IPv6 implementeres i hele topologien

Del 2:

NB: rækkefølgen på nedenstående punkter i Del 2/3 og Del 4 er ligegyldig....

På EXSi serveren installeres 3 virtuelle Server 2022 – **Server 1** skal være en Core Server.

Vælg "Windows Server Standard Evaluation"

Operating system	Architecture	Date modified
Windows Server 2022 Standard Evaluation	x64	8/7/2021
Windows Server 2022 Standard Evaluation (Desktop Experien...	x64	8/7/2021
Windows Server 2022 Datacenter Evaluation	x64	8/7/2021
Windows Server 2022 Datacenter Evaluation (Desktop Experi...	x64	8/7/2021

Sørg for at alle serverne og klienter bliver installeret med dansk time format og keyboard:

Language to install: English (United States)

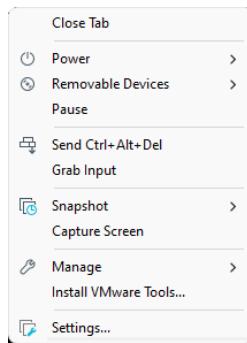
Time and currency format: Danish (Denmark)

Keyboard or input method: Danish

Ydermere skal MS serverne og klienter time synkroniseres (kræver VMWare Tools installeret) op mod ESXi serveren, som igen time synkroniserer til en NTP server på internettet, f.eks.: 0.dk.pool.ntp.org
ESXi serveren skal dog have Internet adgang før den kan tidssync'e.

Installering af VMWare Tools på en Core kan bla. gøres som følger:

Tryk på
"Install VMWare Tools"
Gå til Core serveren og
skriv i command:
PS D:> cmd og <return>
Og vælg og kørs:
D:\>setup64.exe



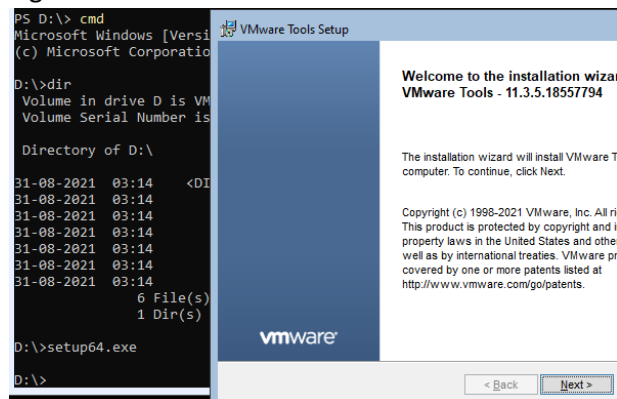
```
D:\>dir
Volume in drive D is VMware Tools
Volume Serial Number is E873-7BAF

Directory of D:\

31-08-2021  03:14    <DIR>          Program Files
31-08-2021  03:14                770.208 VMwareToolsUpgrader.exe
31-08-2021  03:14                55.802 autorun.ico
31-08-2021  03:14                100 autorun.inf
31-08-2021  03:14                2.797 manifest.txt
31-08-2021  03:14            45.456.976 setup.exe
31-08-2021  03:14            98.676.160 setup64.exe
               6 File(s)      144.962.043 bytes
               1 Dir(s)         0 bytes free

D:\>setup64.exe
```

Og VMWare Tools installation starter:



Derudover benyttes de fysiske skolePC'er som klienter (du kan med fordel installere en Virtuel PC til bla. PowerShell afvikling). **Server1** skal være AD DS, DNS og DHCP Server og **Server2** og **Server3** skal være member servere (ikke DC) i det samme domæne. **Klient1** skal også være medlem af dette domæne. (se topologi 1). **Server2** og **Server3** skal være på samme net som det interne netkort. Vælg selv statiske IP-adresser og subnetmaske lokal netværket. På **Server2** og **3** skal der være 2 harddiske (C og D). Tilføj derfor en ekstra virtuel harddisk. For at kunne bruge bogstavet D til den ekstra harddisk, flyttes drevbogstavet for DVD til et bogstav senere i alfabetet (f.eks. Z)

Alle servere, Firewall, routere og switche skal have et sigende navn og en statisk IP adresse, f.eks. kan navngivningen være: RT01, SW01, DCSrv01, FW01, MemSrv01, Klient01 osv osv....

Microsoft domain navngivningen på Server1 (DC server) må ikke bestå af et servernavn, så lav en fiktivt firmanavn eller brug gruppemedlemmernes initialer, f.eks: PI.local, MYDOM.local osv osv. **Navngivning af servere/klient, tildeling af statisk IP, installering af roller, Promote DC, konfigurerung af DHCP Scope, Options og indmelding af Klient/server i domain sker i PowerShell.**

- 1) Konfigurer Raid på Server – hvilke Raid level kan bruges med 4 diske (raid 0,1,5,6 eller 10)?
- 2) Forbind Servers netkort til en enkelt Switch, indtil det endelige netværk er på plads
- 3) Forbind 2-3 PC'er til samme switch, som skal bruges ved oprettelse, installation og konfiguration af serverne. Alle i gruppen kan hver især lave noget på ESXi serveren.
- 4) Installer VMWare vSphere Hypervisor (ESXi) fra en bootable USB
- 5) Konfigurer ESXi med en statisk IP, GW og DNS ud fra IP-planen
- 6) Tilgå ESXi manager med en browser fra klient; login: root
- 7) Upload ISO til Datastore
- 8) Opret og grundinstaller 3 Virtuelle servere, Server 1 **SKAL** være en "Core" som minimum.
- 9) Opret og installer 1 Virtual klient

10) På hver server og klient udføres følgende i PowerShell eller PowerShell ISE

(Start altid Powershell og Powershell ISE som "Run as administrator")

- a. Konfigurer statisk IP, Default gateway og DNS; PS:>New-netipaddress -Interface... Og PS:>SetDnsClientServerAddress -Interface....
(skriv evt. Get-NetIPConfiguration for oplysninger til Interface)
 - b. Navngiv servere og klienter inkl. genstart; PS:>Rename-Computer -....
- 11) Klargør Klient, så denne kan administrere AD via Tools (hvis du ikke kører det fra server)
- a. Installer RSAT, kør: Get-WindowsCapability -Name RSAT* -online |
 - b. Installer Windows Admin Center (manuelt eller med PS)
 - c. Fra klient til Server1 installeres rollen "AD DS" inkl. ManagementTools; PS:> Install-WindowsFeature -Name AD-.....
 - d. Fra klient overtages Server1 med PS:>Enter-PSSession – hvor man får en PS prompt på Server1 (husk at slå Remote management til på server); Promote Server1 som et nyt "Forest" med et sigende domain navn og inkl. DNS, f.eks. SDEDOM.local; PS:>Install-ADDSForest -Domain..... (HUSK DNS)
 - e. Når AD server er i luften, oprettet en ServerAdmin (f.eks. SrvAdm) bruger i stedet for Administrator; PS:>New-Aduser -name.... Server admin brugeren skal som minimum være medlem af gruppen "Domain Admins"; PS:>Add-ADGroupMember -Identity SG_??... Serveradmin bruges fremadrettet til at logge ind på serverne.
 - f. Fra klient til Server1; installer Rollen "DHCP server" inkl. ManagementTools; PS:>Install-WindowsFeature -Name
 - g. Fra klient til Server1; Der oprettes et klient scope i DHCP; PS:>Add-DhcpServer4Scope -Name
 - h. Fra klient til Server1; Der oprettes Option 003, 006 og 015 for DNS og Router oplysninger (default gateway) i DHCP; PS:>Set-DhcpServer4OptionValue -DNS....
 - i. Klientens statisk IP sættes til at modtage en dynamisk IP adresse fra den nyoprettede DHCP server. Tjek med IPCONFIG /all
 - j. Klienten meldes ind i det nyoprettede Domain, f.eks.: SDEDOM.local; PS:>Add-Computer -Domain-Name
 - k. Server 2 og 3 meldes også ind i det nye domain.
 - l. Der isættes 1 ny virtual disk på Server 2 og 3
 - m. CDrom drev D flyttes til andet drev, f.eks. Z
 - n. Den nye disk initialiseres og formateres som drev D (MEGET gerne med PS)

Del 3 (Frivilligt om der bruges PS):

Der skal være både en DNS Forward Lookup Zone (FLZ) og Reverse Lookup Zone (RLZ) for dit domæne. Opret derfor en RLZ for dit domæne på **Server1**. Installer derefter en DNS Server på **Server2**, og opret en Secondary Zone af dit DNS-domain på den, både FLZ og RLZ. Vær sikker på, at **Server2** er med på listen over navneservere, og at der er vist 2 "Name Server (NS)" records i din DNS-server.

Forklar/diskuter følgende med din lærer:

Hvad er FLZ og RLZ, og hvad anvendes de til?

Hvad indeholder "_msdcs"-zonen og hvilken vigtig betydning har denne zone?

Hvilke forskelle er der på en "Active Directory Integrated DNS-zone" og en "Secondary DNS-zone"?

Del 4 - Netværk II

Routerne og switchene skal nu konfigureres iflg. topologi 1 (2) og i overensstemmelse med CCNA3v7 teorien.

Tjek om Router bruger "factory-default setting" 0x2102, Skriv i prompt RT01#show version og kig nederst. Hvis den står til 0x2142 bliver startup configurationen sprunget over. Skriv derfor:

RT01 (config)#config-register 0x2102 -> gem og genstart

Switchen skal bruge 0xF ellers brug også SW01 (config)#config-register 0xF

- 1) Forbind det fysiske netværksudstyr, server og PC'er. Bemærk at det er de "blå" serielle kabler som forbinder RT01 og RT02 til RT03. Dokumenter gerne hvilke porte / Interfaces der bruges til at forbinde de enkelte enheder.
- 2) Konfigurer Routerne og Switchene med standard opsætninger, såsom RT/SW Name, Domain name, no ip domain lookup, enable secret password, MOTD banner, lokal administrativ bruger, SSH, generelt kryptering af clear tekst, management IP og gateway adresse på Vlan 1 på Switchene, description på porte og interfaces. Der henvises til Netværk I (CCNA2v7) kapitel 1.
- 3) Sæt statiske IP adresser på routerne, ifg. IP-planen
- 4) Ping test mellem RT01 og RT03 samt RT03 og RT02 – hvis ok, gå videre.
- 5) Opret statisk route fra R1 til R2 og omvendt, f.eks. fra RT01 # ip route 10.20.10.1 255.255.255.255 10.10.10.2, sæt også en statisk route op på RT02 og ping test mellem RT01 og RT02 – hvis ok, gå videre.
- 6) Konfigurer GRE tunnel over IPsec (arbejder du i ekspert niveau, skal du også gå all in med IPv6)
GRE over IPsec links (vent evt. med IPsec til efter OSPF konfigurationen)
Læs Netacad CCNA3v7, kap 8 VPN and IPsec Concepts – der er oplæg fra læreren
HUSK hvis Securityk9 modulet ikke er enableret på Routeren, tjek med "show version", så VPN IPsec kan bruges, skriv følgende:
#license boot module c2900 technology-package securityk9
<https://blog.router-switch.com/2012/09/how-to-configure-gre-over-an-ipsec-tunnel-on-routers/> (God og hurtig vejledning til GRE over IPsec)
<https://community.cisco.com/t5/security-documents/how-to-configure-gre-over-an-ipsec-tunnel-on-routers/ta-p/3111314> (God og hurtig vejledning til GRE over IPsec med lidt forklaring)

Test af ISAKMP:

- **show crypto isakmp sa**
Nedenstående vises (kun et eksempel):
Pv4 Crypto ISAKMP SA
dst src state conn-id slot status
203.0.0.6 203.0.0.2 QM_IDLE 1001 0 ACTIVE
IPv6 Crypto ISAKMP SA

Test af IPsec:

- **show crypto ipsec sa**

Nedenstående vises (kun et eksempel):

interface: Serial0/0

Crypto map tag: IPSEC_MAP, local addr 203.0.0.2

protected vrf: (none)

local ident (addr/mask/prot/port): (203.0.0.2/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (203.0.0.6/255.255.255.255/47/0)

current_peer 203.0.0.6 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4

#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0

- 7) Konfigurer Single-Area OSPFv2 mellem RT01 og RT02 (brug GRE IP adresserne som kendt Netværk)
Læs Netacad CCNA3v7, kap 1 og 2 – der er oplæg fra læreren
<https://networklessons.com/uncategorized/gre-ipsec-hub-remote-sites> (lidt OSPF med GRE over IPsec)
- 8) Konfigurer NAT/PAT, Access-list på RT01, så alle kan tilgå Internettet
Læs Netacad CCNA3v7, kap 6 (6.6 - PAT) og kap 5 ACL – der er oplæg fra læreren
- 9) Konfigurer en statisk NAT, så InternetPC kan tilgå Webserveren (Server3)
Læs Netacad CCNA3v7, kap 6 (6.4 Static NAT) – der er oplæg fra læreren
- 10) Konfigurer RT02 med en "IP helper-address" som peger på DHCP serveren.
- 11) Sæt en ACL op på RT01, RT02, SW01 og SW02, hvor det kun er 192.168.1.x Odense netværket som må tilgå Line VTY vis SSH.
Læs Netacad CCNA3v7, kap 5 (5.3 ACL) – der er oplæg fra læreren
- 12) De fysiske PC01 og PC02 skal modtage en dynamisk IP adresse DHCP serveren. Test om de kan tilgå Internettet. Ellers benyt fejlfinding, sæt statisk på en af klienterne på ping rundt i topologien, tjek om IP route (OSPF) virker på Routerne, med "show ip route", Tjek om default gateway er korrekt.
Læs Netacad CCNA3v7, kap 12 Network Troubleshooting

Del 5:

Installér mindst 3 OU'er (afdelinger), hvorunder grupper og brugere oprettes, med PowerShell

Husk start altid Powershell og Powershell ISE som "Run as administrator"

- 1) Opret 3 OU'er med selvvalgte navne via en CMDlet/ISE prompt (New-AD.....)
- 2) Opret en Security Group i hver OU via en CMDlet/ISE prompt (New-AD.....)
- 3) Opret en import.CSV fil. Indsæt 15 nye brugere fordelt ligeligt over de 3 OU'er i import.CSV filen og tilret den yderligere til Import, begræns evt. til de felter, der kun skal importeres. Brugere skal importeres i de OU'er, som de tilhører.
Eksempel på Import CSV:
Givenname,Surname,Displayname,Samaccountname,office,userprincipalname,ou
Peter,Iversen,Peter Iversen,pi,IT,pi@MYDOM.local,"OU=IT,DC=MYDOM,DC=local"
- 4) Lav et Import script med ISE editoren, som importerer de 15 nye brugere (behøver du at slette de 3 bestående brugere?) Brugere skal også tilknyttes OU'ens Security Group

Del 6:

Download og installér den seneste version af Wireshark på **Server3** eller **Klient**. Der skal installeres FTP server på **Server3** – det sker under "Roles and Features". Opret en mappe på D drevet med navnet "FtpData" på **Server3** og forbind FTP site i IIS'en til denne. Opret et par tekstdokumenter i mappen. Test først om du kan se en almindelig Ftp opkobling mellem **Klient1** og **Server3** i Wireshark. Hvilken port er Ftp? Skriv i en browser på klienten: **ftp://server3** eller i en CMD: **ftp server3** og du får et login billede. (FireWall på **Server3** kan drille)

Hent inspiration fra dette link: <https://www.avoiderrors.net/install-configure-ftp-server-server-2016/>

Del 7:

Nu skal du kryptere al FTP kommunikation på lokal nettet til **Server3** på Ftp porten med IPSec (Internet Protocol Security). Følg gerne vejledningen i "FTP-IPSec.pdf". Test om krypteringen virker med Wireshark med en Ftp forbindelse fra **Klient1** til **Server3**. Under fanebladet "Protocol" stod der "Ftp" da du testede den almindelige Ftp opkobling, hvad står der nu? Og hvad står det for? Hvorfor er det vigtigt at kryptere Ftp trafik med IPSec i et åbent netværk?

Del 8:

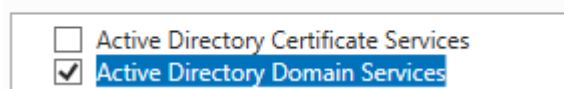
Der installeres en FireWall til erstatning af NAT/PAT router løsningen:

- 1) Opret virtual Switch og PortGroup til Internettet. Det gennemgår læreren.
- 2) Opret og installer 1 FireWall (evt. pfsense) med 2 netkort, et til lokal netværket, et til Internet (SDE)
- 3) Nedlæg NAT/PAT på RT01
- 4) Opret "default statisk route" på RT01 til at pege på FireWall's interne IP adresse.

På FireWall oprettes en portforward (PPTP) til VPN serveren (Server2). Skift derefter **Klient1** netkortet til den "PortGroup" i VMware som er connectet til FW's yderside eller sæt en fysisk klient på SDE nettet. Installér en RAS/VPN-server på **Server2** og konfigurer den som VPN-server i "Remote Access Server". Du skal nu oprette en VPN-forbindelse fra **InternetPC** til **Firewall's** eksterne netkort. Spørg hvis du er i tvivl, det kan være lidt besværligt. Test forbindelsen ved at pinge **Server1** fra **InternetPC**. RSAT på klient kan ikke håndtere RAS (Remote Access) administration, så en workaround er at installere "AD Tools" på den Server2:

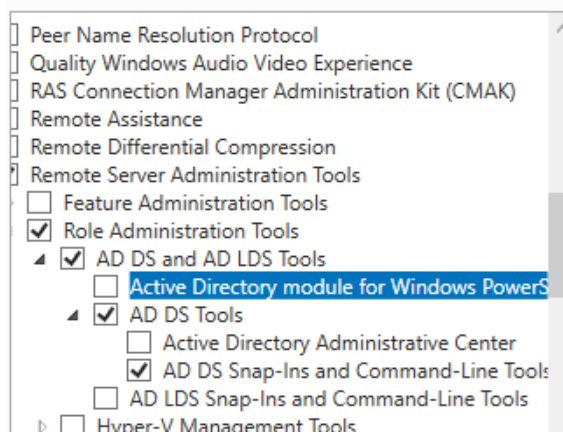
- 1) Gå i "Manage" -> "Add Roles and Features" og vælg "Active Directory Domain Services"

Roles



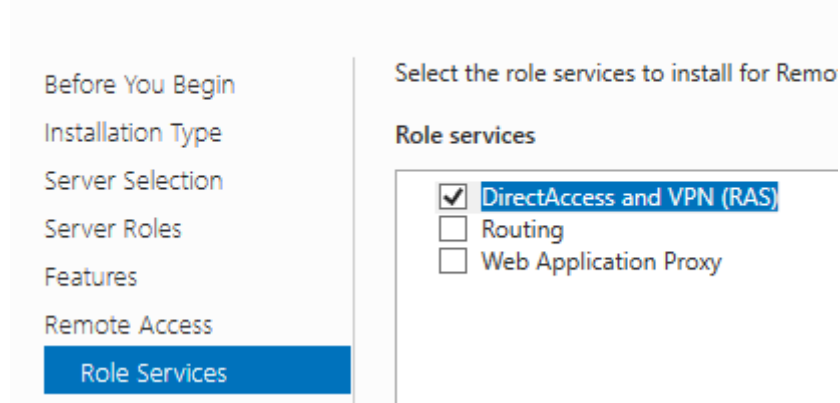
- 2) Og tilpas "Features" som nedestående:

Features



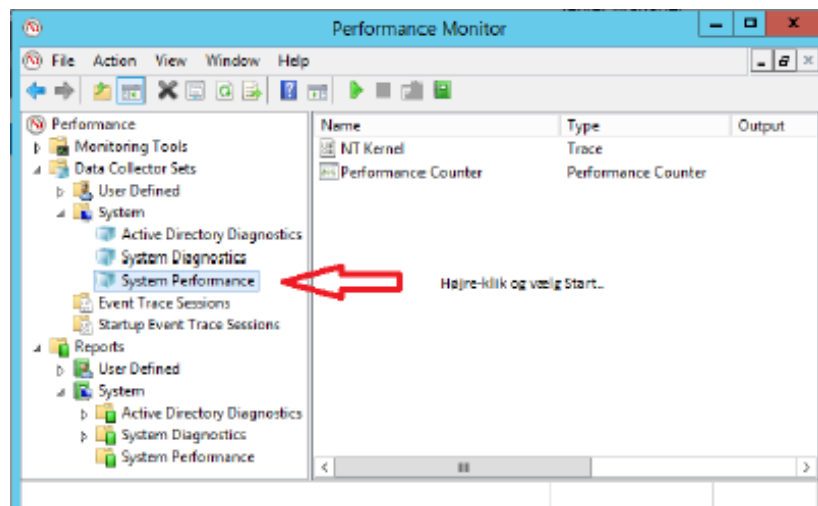
Der installeres efterfølgende Roles "Remote Access" og der tilvælges kun følgende:

Select role services



Del 9:

Start Performance Monitor på **Server1** og lad den køre 1 minut. Se efter om der er advarsler, og hvis der er advarsler, så undersøg hvad de betyder. Vis også log reporten.



Del 10:

Opret en mappe på drev D på **Server3**, og del den med alle godkendte brugere i domænet (Authenticated Users/Domain Users). Konfigurer en Disk Quota på 1GB pr. bruger på drev D. De må ikke kunne overskride denne quota. Udover at vise hvordan du sætter Disk Quota op på drev D, så skal du også vise, hvordan du kan sætte Quota på en mappe (folder) – det gør du ved at installere en Roles med forkortelsen FSRM.

Den Quota du sætter på et drev (partition/volume), gælder det pr. bruger eller pr. volume (drev)?
Gælder der det samme, når du sætter Quota på en mappe med FSRM?

Del 11:

Det kan være svært at finde rundt i et stort firmas mange delte mapper. Derfor anvender man DFS (Distributed File System) til at organisere disse delte mapper fra en fælles rod. Du skal tilføje "DFS Namespaces" og "DFS Replication" rollen på både **Server2** og **Server3** i Add Roles and Features. Følg vejledningen i "DFS Step by Step.docx". DFS roden skal oprettes på **Server1**. Mapperne som oprettes i DFS manageren skal ligge på **server 2 og 3's** drev. Brug gerne andre navne end i "step by step" dokumentationen – brug dog D drevet i stedet for C til mapperne og HUSK DFSRoot serveren (Namespace) skal ligge på **Server1's** C drev !!!!

Del 12:

Næste øvelse er "Backup og Restore" med Windows Server Backup på **Server3** – Installer rollen Windows Server Backup på **Server3**, tag kun backup af d drevet, gem backuppen på et share på **Server2**. Slet nogle filer/mapper på **Server3** og gendan det igen fra din backup.

Del 13: (dit udgangspunkt er én fysisk printer bundet op med én port tilsluttet Printer 1 og Printer 2)

Installer rollen "Print and Document Services" på **Server2**. Start "Print management" og opret en **Printer1** (BrugerPrinter) og **Printer2** (AdminPrinter). Alle brugere i domænet skal automatisk tildeles **Printer1** som deres standardprinter ved hjælp af en "BrugerPrinter GPO". Administratorerne skal tildeles **Printer2**, som er forbundet til samme "port" som printer1, ved hjælp af en "Admin Printer GPO". Sæt prioriteten til 1 for **Printer1** og til 99 for **Printer2**. **Printer2** skal altid være default printer for administratorerne, uanset hvilken computer der logges på.

Del 14:

Installér WSUS (Windows Software Update Service) på **Server3**. Hent et par opdateringer til din klient fra Windows Update, gem dem lokalt på harddisken, og godkend dem. Kontroller at de bliver installeret. Husk når GPO'en oprettes til Update delen, skal stien have et portnummer på. Prøv selv at finde det nummer, eksempel på URL stien: <http://WSUSservernavnet.?.local:<portnummer>>

Del 15:

Opret et script i ISE som opretter mapper og shares, knyttet til Security Group på **Server2**'s d-drev

- Der skal oprettes mapper (New-Item) som hedder det samme som de 3 OU'er der er oprette i AD'en, f.eks. PS C:\New-Item -Path "D:\IT" -ItemType.....
- Mapperne skal shares, f.eks. PS C:\New-Smbshare -Name "SG_IT" -Path "D:\IT" - FullAccess tilknyttet Security Groups, med full access på sharingen
- I Security (NTFS) skal mapperne enten have R/W eller modify på tilknyttet Security Groups.

f.eks.

```
$acl = Get-Acl \\Mem01\IT
```

```
$AccessRule = New-Object  
System.Security.AccessControl.FileSystemAccessRule('SG_IT', 'Modify', 'Con  
tainerInherit, ObjectInherit', 'None', 'Allow')
```

```
$acl.SetAccessRule($AccessRule)
```

```
$acl | Set-Acl \\Mem01\IT
```

Fjern "everyone" fra IT mappens sharing; PS:>Revoke -SmbShareAccess -Name IT

Afprøv på klienten om alt virker som det skal 😊

Del 16:

Afdelingsmapperne (fra pkt. 13) drevmappes ved brug af GPO

Opret et fælles drev på **Server2** og del det ud på klienterne med GPO, så alle afdelinger kan tilgå det.

Opret et "homedrev" for hver bruger under Users -> Profile. Del (share) først en Homemappe på

Server2 En slutbruger vil nu have 3 drev til rådighed. (det er frivilligt om du vil lave dette pkt. med PS)

Del 17:

Når man sidder som IT-Supporter, så kan der komme mange opkald fra slutbrugerne, som bla. lyder:

- a) Jeg får ikke mit afdelingsdrev
- b) Jeg kan ikke komme på UVM hjemmesiden
- c) Jeg kan kun logge på min PC, men ellers virker ingenting
- d) Jeg kan ikke printe
- e) Jeg får ikke mine drev
- f) Jeg kan ikke komme på firmaets intraside

Til fejlfindingseksamen på H3 bliver du bedømt på din strukturering og systematiske tilgang til fejlscenariet.

- 1) Du tjekker rigtigheden i fejlen på klientens PC
- 2) Fokuser ikke kun på problemet, men også på hvad der virker på klienten
- 3) Tjek "ipconfig /all" fra en CMD prompt
 - a. Får du en apipa (169.xx.xx.xx) adresse, sæt en statisk IP på Klient og ping helt "lavpraktisk" til bla. router interface, servere og internet. Virker ping, tjek DHCP services (både på klient og Server), om DHCP scope er deaktiveret, virker ping ikke, tjek router/switch.
 - b. Får du en "rigtig" adresse, tjek videre. Er der DHCP options som står forkert, så du ikke kan komme på internettet eller DNS servicen på Server som er stoppet.
- 4) Får du ikke et drev, tjek GPO
- 5) Får du et drev men kan ikke tilgå det, tjek mappe rettigheder på **Server2**
I stifinder på Klient tjek evt. rettigheder/shares ud med [\\Server2](#)
- 6) Virker det interne net, men ikke internettet, tjek for korrekt DNS, DNS services eller Firewall.
- 7) Virker printer ikke, tjek printerport eller security i print manager.

Du skal fejlfinde sammen med din gruppe!!

Fejlfindings proceduren er:

- 1) Opret en log
- 2) Send et gruppe medlem uden for døren
- 3) Generer en fejl, og før fejlbeskrivelsen ind i loggen, som det første.
- 4) Skriv navn på fejlsøger i loggen
- 5) Før log under hele fejlfindingsforløbet (nu gør han/hun det, nu gør han/hun det osv osv.)
- 6) Brug max 15 min. – giv gerne små hints til fejlsøger, hvis han/hun er gået i stå.
- 7) Hvert gruppe medlem skal mindst 3 gange (gerne flere) igennem et fejlfindingsscenario.
- 8) HUSK at genstarte klient PC, som det sidste inden fejlsøger kommer til.
- 9) Sluttelig sendes loggen til Peter på pi@sde.dk

Del 18:

Valgfag: Operativsystemer III – gælder kun "ikke afkortede"

Det vender jeg tilbage med de sidste 2 uger i jeres skoleforløb 😊

Eksempler på PowerShell kommandoer:

Hjælp i ISE:

Hvis man skal have hjælp til f.eks: Get-ADUser skal man stille cursoren i kommandoen og trykke på "F1" og hjælpen vil poppe op i et vindue. Hvis man vil have hjælp online, hvergang der trykkes "F1", så går man i "Tools" -> "Options" -> "General Settings" og fjerner fluebenet i "Use local help content instead of online content"

Generalt CmdLet og ISE:

PS C:\get-service - <brug "tab"> for at vise diverse optional f.eks. -Computername
[[betyder at f.eks. -Name er required hvor kun én [typisk er Optional.

Kilder

Powershell

Disk Management:

<https://4sysops.com/archives/managing-disks-with-powershell/>

Ændring af Drev-bogstav for CD-rom drev:

<https://www.kittell.net/code/powershell-change-windows-cd-dvd-drive-letter/>

Redigering af Disk-Partition:

<https://docs.microsoft.com/en-us/powershell/module/storage/set-partition?view=windowsserver2019-ps>

DNS Add-primary FLZ, RLZ

<https://docs.microsoft.com/en-us/powershell/module/dnsserver/add-dnsserverprimaryzone?view=windowsserver2019-ps>

<https://www.readandexecute.com/how-to/server-2016/dns/configure-reverse-lookup-zone-with-powershell-windows-server-core-2016/>

DNS Add-secondary FLZ

<https://docs.microsoft.com/en-us/powershell/module/dnsserver/add-dnsserversecondaryzone?view=windowsserver2019-ps>

Hvordan man laver en ny liste variabel i Powershell:

<https://www.varonis.com/blog/powershell-array/#Fundamentals>

<https://stackoverflow.com/questions/26289293/powershell-add-multiple-dns-servers-to-new-dhcp-scope>

Eksportering af brugere i AD gennem Powershell:

<https://networkproguide.com/powershell-export-active-directory-users-to-csv/>

Alternativ:

<https://c-nergy.be/blog/?p=4709>

Hent enkelt AD-bruger:

<https://adamtheautomator.com/get-aduser/>

Sæt AD-bruger oplysninger:

https://www.reddit.com/r/PowerShell/comments/shx9p/user_powershell_to_change_ad_users_first_name/

Concatenering af Powershell værdier:

<https://www.educba.com/powershell-concatenate-string/>

Lidt om Powershell Variabler:

<https://4sysops.com/archives/the-powershell-variable-naming-value-data-type/>

Ny sharing på folder:

<https://docs.microsoft.com/en-us/powershell/module/smbshare/new-smbshare?view=windowsserver2019-ps>

Til at sætte statisk Ipv6 adresse på core server:

<https://docs.microsoft.com/en-us/powershell/module/nettcpip/set-netipaddress?view=windowsserver2019-ps>

16857 – Serverteknologi I
16861 – Netværk II
16862 – Serverautomatisering I
Valgfag: 1551 - Operativsystemer III

Tidsplan for den 5. uge

- 1) **Senest mandag d. 21. februar 2022 inden kl. 15.15 skal følgende være færdigt**
 - PowerShell dokumentationen, fejllogs og Konfigurationerne af routerne (én pr. gruppe) tilsendt til PI@sde.dk i DOC og PDF format (MEGET gerne før 😊)
- 2) **Senest tirsdag d. 22. februar 2022 kl. 15.15 skal følgende være færdigt:**
 - Casebedømmelse af hver gruppe
- 3) **Senest onsdag d. 23. februar 2022 inden midnat skal følgende være færdigt**
 - **For Rutineret** "Modules 6 – 8: WAN Concepts Exam" i "Module Group Exams" med minimum bestået 50 %.
 - **For Avanceret** "Modules 6 – 8: WAN Concepts Exam" i "Module Group Exams" plus 2 selvvalgte "Modules Exams" med minimum bestået 50 %.
 - **For Ekspert** Alle 5 "Modules Exams" i "Module Group Exams" med minimum bestået 50 % i hver og Final Exam med minimum bestået 50 %.
- 4) **Torsdag d. 24. februar 2022 fra kl. 08.10 - 12.00** bruges til at forberede gruppe præsentationen for klassen til torsdag eftermiddag. Jeg læser fejllogs og genlæser PowerShell dokumentationer om formiddagen i lokale 43.
- 5) **Torsdag d. 24. februar 2022 fra kl. 12.00 til 15.15** skal grupperne fremlægge projektet for klassen på PowerPoint. Brug ca. 15 - 20 min. og del fremlægningen ligeligt imellem jer.
- 6) **Fredag d. 25. februar 2022** ryddes der "måske" op, afhængig af om I fortsætter med OS III. Netværksudstyr og server nulstilles og afmonteres fra Rackskabene. Datakabler rulles pænt sammen, rackmøtrikker og skruer lægges tilbage i æsken. Derefter fri 😊

16857 – Serverteknologi I
16861 – Netværk II
16862 – Serverautomatisering I
Valgfag: 1551 - Operativsystemer III

TEORI (estimeret 2-5 dage):

NETVÆRK II (CCNA3v7)

Rutineret:

Eleven skal tage "Modules 6 – 8: WAN Concepts Exam" i "Module Group Exams" med minimum bestået 50 %.

Avanceret:

Eleven skal mindst tage "Modules 6 – 8: WAN Concepts Exam" i "Module Group Exams" plus 2 selvvalgte "Modules Exams" med minimum bestået 50 % i hver.

Ekspert:

Eleven skal tage alle 5 "Modules Exams" i "Module Group Exams" med minimum bestået 50 % i hver.
Eleven skal tage Final Exam med minimum bestået 50 %.

De enkelte "Modules" har fra 56 spørgsmål til 75.

Cisco CCNA bedømmelsesplan for den teoretiske del (Academy):

Procent:	Karakter:
0 – 25	-3
25 – 49	00
50 – 59	02
60 – 69	4
70 – 79	7
80 – 89	10
90 – 100	12

Denne karakter er en delkarakter, som bliver lagt sammen med den praktiske del. Gennemsnittet giver den endelige karakter i Netværk II. Bemærk: Den praktiske evaluering vægter en smule mere end den teoretiske.

16857 – Serverteknologi I
16861 – Netværk II
16862 – Serverautomatisering I
Valgfag: 1551 - Operativsystemer III

Læringsmål:

16857 Serverteknologi I, 16861 Netværk II og 16862 Serverautomatisering I er en del af en 4½ ugers case

Nedenstående læringsmål gælder for alle 3 fag...

- Du skal kunne planlægge et mindre firmanetværk:
 - Du skal kunne lave en netværkstopologi
 - Du skal kende til, beregne og implementere et IPv4 subnet
 - Du skal kende til, beregne og implementere et IPv6 subnet
 - Du skal kunne implementere standard sikkerheds regler på routere og switche
 - Du skal kunne forklare, forstå og implementere statisk routing
 - Du skal kunne forklare, forstå og implementere dynamiske routing protokoller, såsom OSPF og EIGRP
 - Du skal kunne forklare, forstå og implementere GRE over IPSec
 - Du skal kunne forklare, forstå og implementere statisk og dynamisk NAT/PAT
 - Du skal kunne forklare, forstå og implementere Access List (ACL)
 - Du skal kunne installere, opgradere, konfigurere og anvende et serveroperativsystem, herunder foretage bruger-og ressourceadministration samt installation og konfiguration af værktøjer og sikkerhed.
 - Du skal kunne installere, opgradere, konfigurere, administrere og vedligeholde netværksservere, herunder foretage fejlsøgning og fejlretning.
 - Du skal kunne installere og opsætte forskellige former for backup.
 - Du skal grundlæggende kunne anvende Powershell til fjernadministration af servere, installering og implementering af roller og applikationer, administration af bruger database, importering/exportering af brugere samt oprette og administrere en filstruktur sikkerhedsmæssigt korrekt
 - Du skal kunne anvende PowerShell i både CMDLets kommandoen og ISE editoren, forstå og anvende kommandoer samt kunne benytte dig af hjælpefunktionerne.

16857 – Serverteknologi I
16861 – Netværk II
16862 – Serverautomatisering I

Valgfag: 1551 - Operativsystemer III

I bedømmelsen af casen skal du vise og kunne forklare om følgende:

- 1) **Topologi, IP-Plan for IPv4 & v6**
- 2) **Opbygningen af den virtuelle host (ESXi), f.eks. Raid, Datastore**
 - a. Visning af de virtuelle servere
 - b. Visning af de fysiske klienter
 - c. Visning af en eller flere administrative klienter (bla. med RSAT og Windows Admin Center)
- 3) **DC server**
 - a. Visning af navngivning og statisk IPv4 og v6
 - b. Visning af AD strukturen
 - c. Visning af DNS (primær og sekundær)
 - d. Visning af DHCP (IPv4 og v6 scope til både Odense og Aarhus))
 - e. Visning af Remote Access (RAS/VPN)
 - f. Visning af GPO opsætninger, såsom WSUS og IPSec
- 4) **Member servere**
 - a. Visning af navngivning og statisk IPv4 og v6 samt ekstra drev d.
 - b. Visning af DFS (virker det fra en klient?)
 - c. Visning af FTP server (ikke krypteret / krypteret via Wireshark)
 - d. Visning af VPN – fra "Internet PC"
 - e. Visning af WSUS (styring af update via GPO og administration af WSUS)
- 5) **FireWall**
 - a. Visning af navngivning og statisk IPv4 og v6
 - b. Visning af "Forward rules"
- 6) **Route:**
 - a. Statiske IP adresser (IPv4 og v6)
 - b. Standard login sikkerhed med bla. SSH
 - c. NAT/PAT – adgang til "internettet"
 - d. Statisk NAT – adgang fra "internet PC" til Webserver (server 3)
 - e. Statisk routing
 - f. Dynamisk routing (OSPF) – mellem Odense og Aarhus
 - g. GRE over IPSec – mellem Odense og Aarhus
- 7) **Switch:**
 - a. Remote opsætning (SSH, IP, default gateway