

# 16858 Serveradministration- og sikkerhed, 16852 Netværk I og 16852 Computerteknologi

Opdateret af EL, d. 06.04.21

Varighed: 6 uger (uge 16 til og med uge 21 (til og med 28.05.21))

Version 9

**LÆS ALT IGENNEM FØR START!!!**

## Resume:

Denne 6 ugers case består af følgende fag: 16858 Serveradministration og sikkerhed, 16864 Netværk I og 16864 Computerteknologi.

## Udstyr:

1 server til virtualisering, mindst 2 fysiske PC'ere, 2 routere, 1 Access point (trådløs router) og 3 switche. Patch kabler, strømkabler mm.

## Software:

Windows Server 2016 standard Evaluation, Windows 10 Enterprise Evaluation og VMWare vSphere Hypervisor 7 (ESXi), pfSense/Sophos, FreeNas

Følgende ISO filer og documentation finder du på **USB sticks**, som jeg har til udlån !

- MS produkter, kan dog også hentes på: <https://azureforeducation.microsoft.com/devtools>
- VMware vSphere Hypervisor 7.0 (ESXi) og VMWare Workstation 15
- pfSense og Sophos FireWall's
- FreeNas
- Øvrigt dokumentation, casen og intro

## Arbejd i 2-3 mands grupper

Sidst i case forløbet (6. ugen) afleveres der én gruppe systemdokumentation og hver gruppe præsenterer deres projekt for resten af klassen i form af en PowerPoint præsentation på ca. 12-15 min, hvor hvert gruppemedlem deles ligeligt om præsentationen.

## Dan grupper efter Præstationsstandarder (se næste side):

I skal danne grupper efter nedenstående præstationsniveauer. Der skal afgives karakterer i alle 3 fag, men Computerteknologi og Serveradministration & sikkerhed hænger uhjælpelig sammen og evalueres som et fag og én karakter (dog 2 karakterer i LUDUS). Derfor skal gruppen tidligt i forløbet være enig i, hvilke niveauer de 2 fag skal afvikles på. Karaktergivningen i Netværk I foregår lidt anderledes, da der både er teori og praktik, som en del af bedømmelsen. Det er teorien, som sætter niveauet (se side 12) og den praktiske del er med til at bestemme karakteren. Derfor kan man individuelt vælge niveau i gruppen i Netværk I.

# 16858 Serveradministration- og sikkerhed, 16852 Netværk I og 16852 Computerteknologi

Opdateret af EL, d. 06.04.21

Varighed: 6 uger (uge 16 til og med uge 21 (til og med 28.05.21))

Version 9

## 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.

### Case:

2 revisionsfirmaer, Munkebjerg Revision og Skibhus Revision, i Odense tænker på at blive fusioneret. Inden dette bliver en realitet, vil de starte med at samarbejde omkring administrationen og revisorerne. I

Munkebjerg er der ansat 12 revisorer og 3 i administrationen og i Skibhus 9 revisorer og 2 i administrationen (find selv på navnene). Som udgangspunkt (fase 1) skal de have hvert deres eget selvstændige IT-system, en Windows Server 2016 domain controller, en fil- og print server. Der skal yderligere implementeres sikkerhed på såvel Microsoft miljøet som netværksudstyret.

Dit team skal udføre arbejdet for de 2 revisionsfirmaer, som i første omgang drejer sig om at opbygge hver deres netværk. En Cisco Router med 2 Gbit interfaces skal "binde" de 2 lokationer sammen.

Se "Topologi for fase 1"

Efter et halvårs tid med samarbejde på tværs af de 2 firmaer skal fusionen gennemføres (fase 2). Da Munkebjerg Revision har rigelig plads på deres lokation, lukker Skibhus Revision deres afdeling og flytter til Munkebjerg med mandskab og IT-udstyr. Skibhus domænet nedlægges og deres Servere og Klienter meldes i stedet ind i Munkebjerg domænet. Deres "gamle" DC server oprettes i Munkebjerg domænet, således der er 2 ligestillede Domain Controllere.

Samtidig ønskes der en fælles gruppe politik, hvor bla. baggrund, password kriterier, login standard, distribution af applikationer og printere administreres centralt (fra en GPO).

Der vil være en Fil- og print server tilovers fra Skibhus, så den laves om til en WSUS server (Microsoft update)

# 16858 Serveradministration- og sikkerhed, 16852 Netværk I og 16852 Computerteknologi

Opdateret af EL, d. 06.04.21

Varighed: 6 uger (uge 16 til og med uge 21 (til og med 28.05.21))

Version 9

Netværket skal også segmenteres i VLANs, hvor der tages højde for den højeste sikkerhed på switche og routere samt laves redundant i form af HSRP, Etherchannel og STP. Der skal være WI-FI adgang med et Access point, hvor sikkerheden er sat højest. Slutteligt opsættes en FireWall som giver firmaet internetadgang og beskytter fra ubudne gæster ude fra den store verden....

Revisionsfirmaerne skal have udleveret en systemdokumentation for "Fase 2" på IT-systemet ved afslutningen af projektet, som bl.a. omfatter forside, indholdsfortegnelse, kravsspecifikation, topologi, ip-plan, brugermatrix, tidsplan, dagbog, fejllog og skærmdumps af installation, opsætning, implementering og konfiguration af IT-løsningens teknologier med en kort beskrivelse til. (lav evt. skærmdumps løbende under projektet)

## Fase 1 (estimeret 6 dage):

- 1) Udarbejd en projektplan for fase 1, hvorunder kravsspecifikation, IP plan, navngivning af domain, server- og klienter, netværkstopologi og en ca. tidsplan indgår. Projektplanen skal godkendes af revisionsfirmaerne (læreren), inden den praktiske del af projektet igangsættes.  
Opret også en dagbog som hver dag udfyldes samt en fejllog hvor udfordringer/fejl og løsninger løbende noteres med et ID nummer (incident/solution).  
Munkebjerg Revision har IP Netværks ID: 192.168.20.x /24 og Skibhus har: 172.16.20.x /24  
Både Munkebjerg Revision og Skibhus Revision afvikles på samme fysiske Server med ESXi dog adskilt med 2 virtuelle switche (vSwitch0 og 1) som hver er tilknyttet sit eget fysiske interface – det skal jeg nok introducere nærmere, men det er en spændende løsning 😊
- 2) Konfigurer en Cisco Router til kommunikation mellem de 2 domæner, den første brugbare IP-adresse i hvert IP-subnet benyttes statisk på routerens Gigabit interfaces.
- 3) Der skal sættes 1 fysisk switch på hver af ESXi serverens netkort, hvorpå du tilslutter en fysisk Klient PC.  
Konfigurer også de helt basale sikkerhedsfunktioner, såsom enable-, console og telnet/SSH passwords og banner.  
[Læs CCNA2v7, kapitel 1, på Cisco Academy, for grundkonfiguration af Router samt ide oplæg til IP planlægningen. Der vil være oplæg fra læreren til kap. 1 samt en refresh på IPv4 og v6.](#)
- 4) Under hvert revisionsfirma installeres følgende virtuelle servere på ESXi serveren: 1 Domain controller og 1 fil- og print server samt en fysisk PC (brug den eksisterende skole PC). Der ønskes nyeste OS i form af Windows Server 2016 standard og Windows 10. Brug sigende server- og klient navne, f.eks. MunkDC1, MunkFil1, SkibDC1, SkibFilPrt, SKKlient eller andet... De 2 domæneskove/forest skal også være sigene og forskellige, f.eks. Munkebjerg.local, Skibhus.local, MU.local, SK.local eller andet. Husk også at server- og klient navne skal være forskellige i de 2 domæner og der må ikke indgå et servernavn i domænenavnet.  
Serverne skal tildeles statiske IP adresser og klienter tildeles dynamiske fra DHCP server. Se "Topologi for fase 1"  
DC skal indeholde rollerne: AD DS, DNS, DHCP  
Opret en serveradmin bruger på DC serveren, f.eks. SrvAdm, i stedet for Domain Administrator brugeren, og brug den fremadrettede på alle serverne (kopier Administrator brugeren)  
- Active Directory teknologien uddybes her, hvis der er ønske om det:  
<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/ad-ds-getting-started>  
Fil- og print server skal indeholde: en ekstra HD (drev d) til brugernes data, Print Services og evt. "File Server Ressource Manager" som en del af File and Storage Services

# 16858 Serveradministration- og sikkerhed, 16852 Netværk I og 16852 Computerteknologi

Opdateret af EL, d. 06.04.21

Varighed: 6 uger (uge 16 til og med uge 21 (til og med 28.05.21))

Version 9

## 5) Lav Trust mellem de 2 domæner (Two-way Forest-wide Trust)

- Se evt. <https://tech.iot-it.no/microsoft-windows-setup-two-way-forest-trust/>

**NB:** for at du kan oprette en trust mellem 2 domæner, skal du indsætte en "Conditional Forwarders" i DNS Manager, hvor det ene domain peger på det andet og vice versa.

AD- og filstrukturen oprettes som vist i "Forest-Trust diagram for fase 1"

2 brugere (vælg selv navnene) oprettes i hver OU på hvert sit domain, som har medlemskab af en Global Security Group. På Skibhus skal Global Security Group for Revision, både fra Munkebjerg og Skibhus, være medlem af en Local Security Group. Administrations afdelingerne benytter direkte Global Security Group.

Revisionsmappen på Skibhus shares med Local Security Group, som vist i diagrammet.

Administrationsmappen på Skibhus shares med Global Security Group fra både Munkebjerg og Skibhus. Husk også at sættes NTFS/Security rettigheder på nævnte grupper.

Kan I se fordele/ulempes ved de 2 måder at dele rettigheder på?

Brugere på Munkebjerg domænet skal nu kunne tilgå de shares på Skibhus domænet som de har fået rettigheder til. Aftest dette på en Munkebjerg klient og skriv `\\SKFilSrv01.skibhus.local` i øverste felt i en stifinder. Du skal gerne kunne tilgå de mapper dine rettigheder er til.

Vis evt. hvordan man kan differentiere share rettighederne mellem domænerne, hvor Skibhus evt. har flere rettigheder end Munkebjerg!!!!

**Avanceret/Ekspert:** spejlvend, således at Skibhus.local kan få fat i de relevante mapper på Munkebjerg.local

- 6) Der afholdes et statusmøde, hvor Munkebjerg revision (lærer) skal godkende projektet indtil videre, holdt op mod projektplanen. Teknologierne vises og forklares og 1. del af systemdokumentationen gennemgås.  
Fase 1 er estimeret til 6 dage

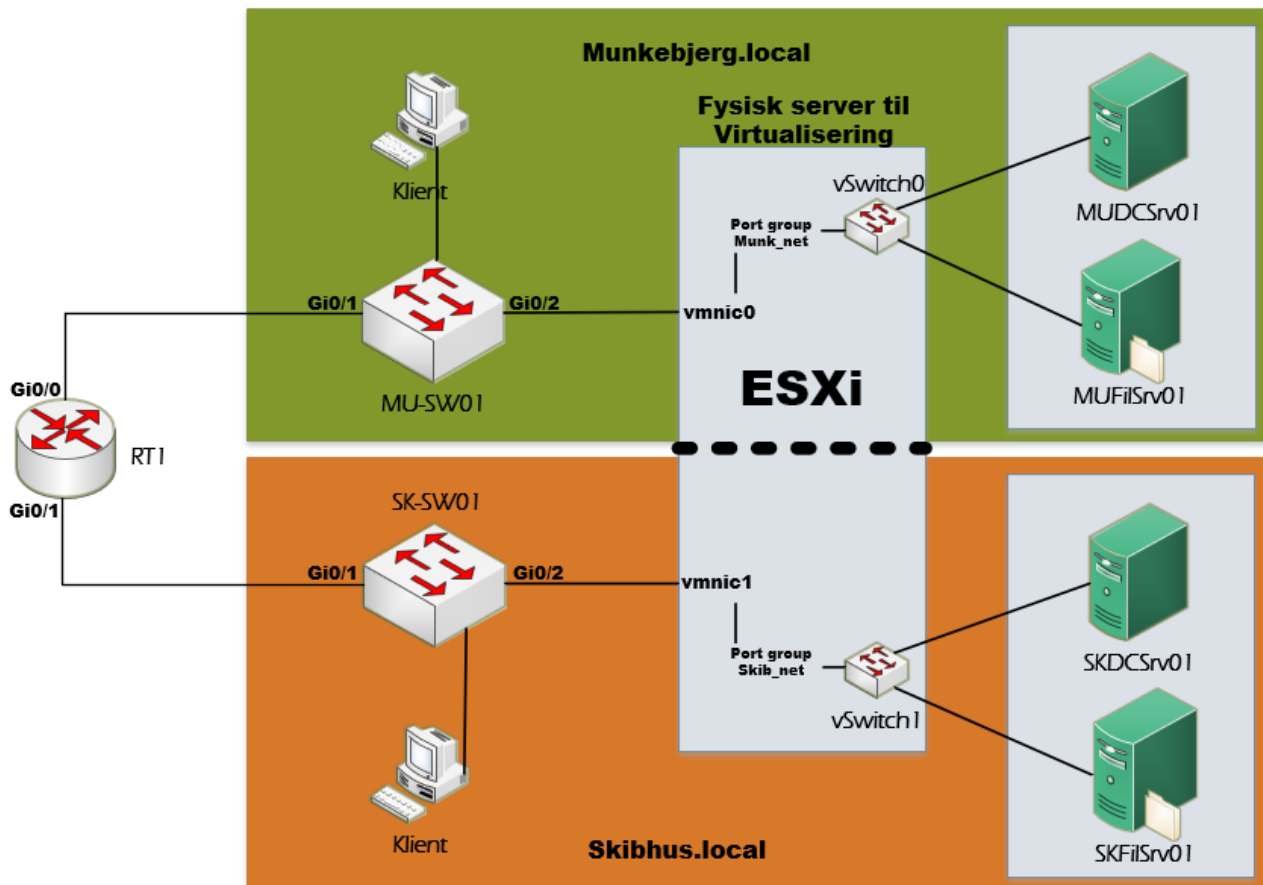
# 16858 Serveradministration- og sikkerhed, 16852 Netværk I og 16852 Computerteknologi

Opdateret af EL, d. 06.04.21

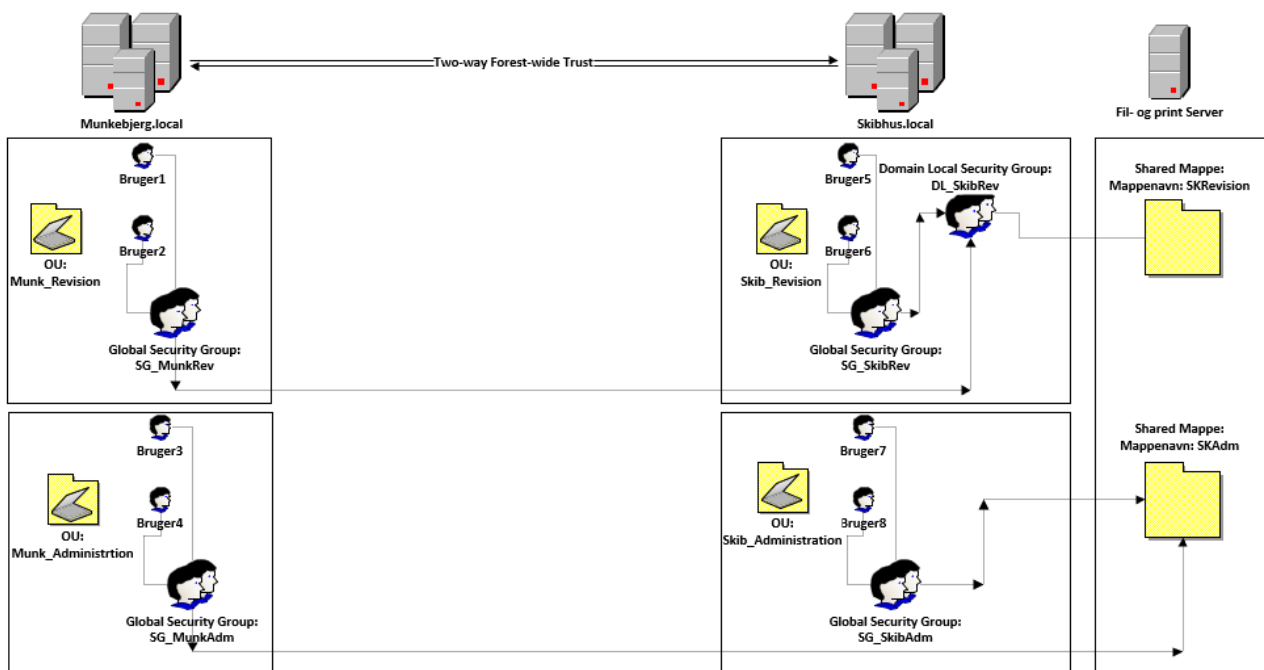
Varighed: 6 uger (uge 16 til og med uge 21 (til og med 28.05.21))

Version 9

## Topologi for fase 1:



## Forest-Trust diagram for fase 1:



# 16858 Serveradministration- og sikkerhed, 16852 Netværk I og 16852 Computerteknologi

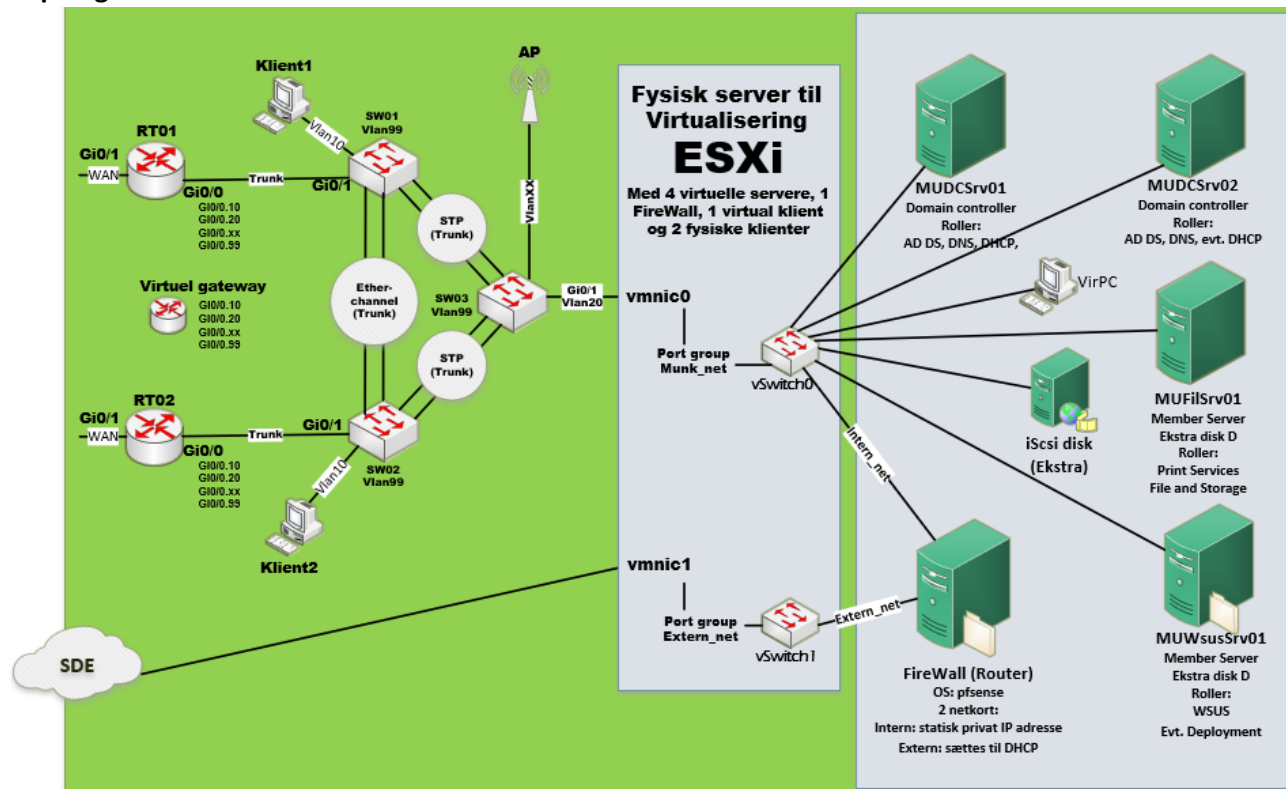
Opdateret af EL, d. 06.04.21

Varighed: 6 uger (uge 16 til og med uge 21 (til og med 28.05.21))

Version 9

## Fase 2 (estimeret 16 dage)

### Topologi for fase 2:



- 7) Udarbejd en projektplan for fase 2, hvorunder en ny kravsspecifikation, bruger matrix, IP-plan, ændringer i navngivning af server- og klienter, netværkstopologi, og en ca. tidsplan indgår. Projektplanen skal godkendes af revisionsfirmaerne (læreren), inden den praktiske del af projektet igangsættes. **NB: Kom gerne med andre udfordrende løsningsforslag!!!** Fortsæt med dagbog og fejllog registreringen.

Eksempel på IP-Plan:

VLAN 20					
Server netværk IP-Subnet: 192.168.20.0 /24 (255.255.255.0)					
Enhedsnavn	IP-adresse	Subnet Mask	Default Gateway (Virtuel GW)	DNS	Virtuel gateway
RT01 Gi0/0.20	192.168.20.2	255.255.255.0	N/A	N/A	192.168.20.1
RT02 Gi0/0.20	192.168.20.3	255.255.255.0	N/A	N/A	192.168.20.1
FW01	192.168.20.4	255.255.255.0	N/A	N/A	N/A
ESXi01	192.168.20.5	255.255.255.0	192.168.20.1	192.168.20.10/11	N/A
MUDCSrv01	192.168.20.10	255.255.255.0	192.168.20.1	192.168.20.10/11	N/A
MUDCSrv02	192.168.20.11	255.255.255.0	192.168.20.1	192.168.20.10/11	N/A
MUFilSrv01	192.168.20.12	255.255.255.0	192.168.20.1	192.168.20.10/11	N/A
MUWsusSrv01	192.168.20.13	255.255.255.0	192.168.20.1	192.168.20.10/11	N/A

# 16858 Serveradministration- og sikkerhed, 16852 Netværk I og 16852 Computerteknologi

Opdateret af EL, d. 06.04.21

Varighed: 6 uger (uge 16 til og med uge 21 (til og med 28.05.21))

Version 9

VLAN 10					
<b>Klient netværk IP-Subnet: 192.168.10.0 /24 (255.255.255.0)</b>					
Enhedsnavn	IP-adresse	Subnet Mask	Default Gateway (Virtuel GW)	DNS	Virtuel gateway
RT01 Gi0/0.10	192.168.10.2	255.255.255.0	N/A	N/A	192.168.10.1
RT02 Gi0/0.10	192.168.10.3	255.255.255.0	N/A	N/A	192.168.10.1
Klient1 & 2	DHCP	DHCP	DHCP	DHCP	N/A

VLAN XX (opret og beregn selv)					
<b>WI-FI netværk IP-Subnet: 192.168.xx.0 /24 (255.255.255.0)</b>					
Enhedsnavn	IP-adresse	Subnet Mask	Default Gateway (Virtuel GW)	DNS	Virtuel gateway
RT01 Gi0/0.xx			N/A	N/A	
RT02 Gi0/0.xx			N/A	N/A	
AP					
Klient1 & 2	DHCP	DHCP	DHCP	DHCP	N/A

VLAN 99					
<b>Management netværk IP-Subnet: 192.168.99.0 /24 (255.255.255.0)</b>					
Enhedsnavn	IP-adresse	Subnet Mask	Default Gateway (Virtuel GW)	DNS	Virtuel gateway
RT01 Gi0/0.99	192.168.99.2	255.255.255.0	N/A	N/A	192.168.99.1
RT02 Gi0/0.99	192.168.99.3	255.255.255.0	N/A	N/A	192.168.99.1
SW01	192.168.99.4	255.255.255.0	192.168.99.1	N/A	N/A
SW02	192.168.99.5	255.255.255.0	192.168.99.1	N/A	N/A
SW03	192.168.99.6	255.255.255.0	192.168.99.1	N/A	N/A

WAN (RT01 og RT02 Gi0/1)					
<b>WAN Subnet (RT01 og 02): 10.10.10.0 /30 (255.255.255.252) – beregn selv det der mangler</b>					
Enhedsnavn	IP-adresse	Subnet Mask	Default Gateway	DNS	Virtuel gateway
RT01 Gi0/1 WAN		255.255.255.252	N/A	N/A	N/A
RT02 Gi0/1 WAN			N/A	N/A	N/A

- 8) Nu skal Skibhus domænet nedlægges og meldes ind i Munkebjerg domænet. Inden det dog sker, skal følgende klargøres:
- Brugerne på Skibhus skal oprettes i Munkebjerg  
**Eksport:** eksporter brugerne fra Skibhus domænet og importer i Munkebjerg domænet med PowerShell. Importer evt. brugerne i én OU, opret "homefolder" i et hug og flyt derefter brugerne ud i de respektive OU'er.  
**Hints:**  
<https://emeneye.wordpress.com/2013/02/28/importing-users-into-active-directory-from-a-csv-file-using-powershell/>  
<https://gallery.technet.microsoft.com/scriptcenter/Powershell-script-to-5edcdaea>
  - Meld Klient og Fil- og printer server ud af Skibhus domænet. Husk at have en lokal administrator bruger ellers kan du ikke logge på efter en genstart.



# 16858 Serveradministration- og sikkerhed, 16852 Netværk I og 16852 Computerteknologi

Opdateret af EL, d. 06.04.21

Varighed: 6 uger (uge 16 til og med uge 21 (til og med 28.05.21))

Version 9

- c. Slet trust og conditionel forwarders på de 2 domæner.
  - d. Nedlæg (Demote) Skibhus domænet – Vælg "Remove Roles and Features" -> Fjern makingen i "Active Directory Domain Services" og "Remove" – Der bliver gjort opmærksomt på, at der skal køres en "Demote" først, som fjerner AD'et, klik med genvejs linket til "Demote". Efter en genstart fjernes DNS og DHCP fra Skibhus serveren. Bibehold AD DS rollen, som skal bruges senere, når den skal "Promotes" ind i Munkebjerg.local domænet.
- 9) Netværket, som det er nu, skal omkonfigureres, se Topologi for fase 2. VLAN, EtherChannel, STP og Subinterfaces skal konfigureres på henholdsvis SW01, SW02, SW03 og RT01, RT02.
- 10) Netværks ID: 192.168.xx.0 /24 subnettes i 3. oktav (xx) til brug i hvert af følgende VLAN:
- VLAN 10** er til Klienterne med Subnet ID: 192.168.10.0 /24 og IPv6 Subnet Prefix 2001:db8:acad:10::/64 og Link-Local FE80::1
- VLAN 20** er til serverne, DC-, Fil og WSUS serverne med IPv4 Subnet ID: 192.168.20.0 /24 og IPv6 Subnet Prefix 2001:db8:acad:20::/64 og Link-Local FE80::1 – Husk serverne skal have statiske IP adresser.
- VLAN ??** er til WLAN (Wi-Fi), vælg selv Vlan ID og IPv4 Subnet-ID, f.eks.: 192.168.xx.0 /24
- VLAN 99** er management, som bruges til at remote overtage switchene.
- Subnet ID: 192.168.99.0 /24.
- NB: Brug gerne andre IPv4 og v6 adresser!!
- Læs CCNA2v7, Switch Configuration kapitel 1, VLANs kapitel 3, EtherChannel kapitel 6 og skimme STP Operations kapitel 5. Der vil være oplæg fra læreren.
- 11) Begge Routere skal fungere som en "Router on the stick", hvor det ene hovedinterface (Gi0/0) skal håndtere flere IP-Subnets og Vlan's i form af subinterfaces. Med 2 "ens" routere, som kun adskiller sig med Hostname og IP adresser, skal der konfigureres en "Hot Stand-by Router Protocol, HSRP" løsning mellem de 2 routere, hvor RT01 er den "Active" og RT02 er "Passiv"
- HSRP behøves ikke at sættes op med IPv6 men "**Ekspert**" må gerne forsøge. Se følgende link: <https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/113216-ipv6-hsrp-00.html>
- IP adresserne på begge routers Gi0/1 går til en "fiktiv" lokation. IP adresserne skal blot kunne pinges.
- Læs CCNA2v7, Inter-VLAN Routing (SubInterface) kapitel 4, FHRP Concepts (HSRP) kapitel 9
- Der vil være oplæg fra læreren.
- Eks. på HSRP og SubInt (IPv4): <https://petri.com/forums/topic/hsrp-on-sub-interface-issue>
- 12) Opsæt og konfigurer Access point i overensstemmelse med din IP-plan. Brug Linksys AC1000 trådløs router, deaktiver DHCP servicen og brug kun den indbyggede switch (ethernet 1 – 4) til at connecte til RT01 med. Konfigurer sikkerhed på Wi-Fi. Hvad er WEP vs. WPA vs WPA2 vs WPA3 (AES/TKIP), SSID, Trådløs MAC-filter? Har Linksys AC1000 den nyeste teknologi (f.eks. Båndbredde G/N/AC og kryptering)? Læs om WLAN i CCNA2v7 kapitel 12 og 13
- Linksys: connect PC til ethernet 1-4 med adressen: 192.168.1.1 i en web browser og med password: admin.
- PC'en kan stå til at modtage en DHCP eller have en statisk IP i Subnet-ID 192.168.1.0 /24
- Ændr AP'ens statiske IP i forhold til IP-planen. Deaktiver DHCP-server på Lokal netværket.
- Opret en Static Routing på AP til de private adresser på lokalnetværkets Vlan10, 20 og 99.
- Der skal kunne pinges fra AP til DC server og omvendt.



# 16858 Serveradministration- og sikkerhed, 16852 Netværk I og 16852 Computerteknologi

Opdateret af EL, d. 06.04.21

Varighed: 6 uger (uge 16 til og med uge 21 (til og med 28.05.21))

Version 9

- 13) Flyt de nedlagte servere fra Skibhus til Munkebjerg (ændr "Port group" til Munk\_net), tilret dem med sigende navne og statiske IP-adresser iflg. den nye IP-plan. Tilføj den nedlagte domæne server til den bestående som ekstra domænecontroller. Brug den fungerende DC server som DNS. Den skal også gøres til ekstra GC-server (Global Catalog).

**Forklar hvad en GC-server er, hvor man kan se det er en GC'er, og hvorfor det er en fordel at der er flere GC-servere i domænet? Vis også, hvordan man selv bestemmer, hvornår AD-replikeringen mellem domaincontrollere i samme domain finder sted.**

Den nye DC2 server skal fungere som primary DNS (på lige fod med DC1).

- 14) Omkonfigurer DHCP scopet til Klient netværket på VLAN 10 samt lav et ny scope til WI-FI netværket.

**Avanceret/Ekspert:** Lav DHCP Split-Scope eller failover på DCSrv02:

<https://newhelptech.wordpress.com/2017/06/29/step-by-step-dhcp-failover-in-windows-server-2016/>

- 15) Installer en PFSense FireWall:

I ESXi Virtual machine opsætning bruges:

Other / FreeBSD 12 or later versions (64-bit)

**Husk** "Add" 2 interfaces, hvor det ene (em0) forbindes til portgroup "Munk\_net" og det andet (em1) forbindes til enten den bestående portgroup "Skib\_net" eller lav en ny som evt. hedder "Extern\_net" (går til SDE nettet)

Web adgang:

https:ipadressen

Login: admin / Password: pfsense

- 16) Opret en Default Static Route på RT01 og RT02 til Firewall'ens Interne IP adresse.

Læs CCNA2v7, Static Routes kapitel 15, 15.3 - Der vil være oplæg fra læreren.

- 17) **Spring over:** Opret en Static Route på RT01 og RT02 fra netværket på RT 01 Gi0/1 til de private adresser på lokalnetværkets Vlan10, 20, xx og 99, hvor backup server er forbundet. Der skal kunne pinges fra backup server til DC server og omvendt.

Læs CCNA2v7, Static Routes kapitel 15, 15.2 - Der vil være oplæg fra læreren.

- 18) Opret drevmapping via GPO, hvor hver afdeling har deres eget drev, hver bruger et personligt drev (mappet enten fra "Profile" på brugeren el. fra en GPO) og et fælles drev hvor alle brugere kan tilgå, i henhold til jeres brugermatrix... Tjek fra klienten at brugerne kun kan komme ind i de mapper de har rettigheder til iflg. brugermatrixen.



## SIKKERHED:

- 19) SSH forbindelsen til router og switcher er på plads, ellers konfigureres den (CCNA2v7 Kap 1, 1.3.4)
- 20) Access portene på switchene sikres med Port-security konfiguration. Læs CCNA2v7, Switch Security Configuration kapitel 11. Forstå de forskellige Secure MAC adresse typer.
- 21) På domæne controlleren stilles der krav om, at brugernes password skal være sikre, så de skal mindst være på 10 karakterer, indeholde tal, store og små bogstaver samt tegn (kompleksitetskrav) samt skiftes hver 25. dag. Dette skal konfigureres på Domain-niveau.
- 22) Navnet på den sidste bruger der har været logget ind på computeren må ikke vises, når en anden bruger vil logge ind.

# 16858 Serveradministration- og sikkerhed, 16852 Netværk I og 16852 Computerteknologi

Opdateret af EL, d. 06.04.21

Varighed: 6 uger (uge 16 til og med uge 21 (til og med 28.05.21))

Version 9

- 23) Hver afdeling skal have hver jeres baggrundsbillede, når en almindelig bruger logger på klienten og billedet må ikke kunne ændres. Baggrundsbillederne shares fra filserveren.
- 24) Der skal oprettes mindst 1 ekstra domain administrator og 1 serveroperator.
- 25) I hver afdeling skal en af de almindelige brugere være en superbruger, der kan nulstille de andre brugeres password samt **kun** oprette men ikke slette nye brugere i deres egen afdeling. Vis det virker ved at downloade og installere RSAT (Remote Server Administrative Tools) på en klient PC.
- 26) Når en almindelig bruger logger på memberserveren eller klienten, skal han ikke have mulighed for at starte kommandoprompten, men administratorer skal have denne mulighed. Find også ud af, hvordan du kan forhindre brug af PowerShell for almindelige brugere. Lav først dette til sidst i casen, da cmd er nyttig til de kommende punkter.
- 27) Der skal også være auditering og logning af forsøg på at logge på computeren med forkert navn/password. Alle loginforsøg skal logges, både succes og fejl. Ved 5 forkerte forsøg, skal brugerens konto låses i 25 min i hele domænet. Vis det virker!!!
- 28) "Security Event" og "Application Event" logfilerne skal placeres i mappen "c:\logfiler" på alle computere- og serveres lokale harddisk. Opret mappen "logfiler" med en GPO eller et script. **For Ekspert/Avanceret niveau:** Du skal herefter oprette en "subscription server" på WSUS serveren, der indsamler "Security Event" logfilen fra de øvrige servere (DC1 & 2 og Filserver), inklusiv den selv. Søg inspiration i "Centralizing Windows Logs.pdf" på Teams eller Google efter "Centralizing windows event logs" for flere oplysninger.
- 29) Administratoren skal selvfølgelig kunne tage backup af Active Directory (SystemStateBackup) i tilfælde af nedbrud, og du skal derfor både lave **backup** og **recovery** af hele eller dele af AD på din "nye" DC server. Hvordan kommer du i "safe" mode for at Recover?  
Tilføj enten en ekstra disk på DC serveren eller brug et share på Filserveren til backup af "SystemState".
- 30) Det er ikke altid praktisk at lave gendannelse af AD midt i arbejdstiden, da serveren skal være offline. I Server 2012 og 2016 er der derfor kommet noget smartere, **Active Directory Recycle Bin** eller på dansk **AD Papirkurv**. Find denne funktionalitet og aktiver den. **Vis at det fungerer.**
- 31) Fil/print serveren som blev frigivet fra Skibhus skal være WSUS server, hvor diverse update fra Microsoft kan hentes ned og testes inden de sendes ud til servere og klienter. Dette gøres ved af installere en rolle på serveren samt lave en GPO på DC serveren.
- 32) Fejlfinding ½-1 dag: Jeg kommer nærmere ind på detaljerne, når alle grupperne er klar.
- 33) **For Ekspert niveau:** Implementer en deployment server og deployments tools – det er rigtigt smart!!! <https://docs.microsoft.com/en-us/windows/deployment/windows-deployment-scenarios-and-tools>  
<https://www.youtube.com/watch?v=O1lo8GqcMpk>
- 34) **Ekstra Ekstra (God og nem opgave 😊):** Filserveren skal have et separat iSCSI-drev til deres backup på en **iSCSI-server**. (brug FreeNAS → Guest OS Version (på ESXi) = "FreeBSD 12 or later versions (64-bit)")  
Tilknyt "volume" fra NAS som et fortløbende drev under diskmanager. Hvis filserver i forvejen har C og D, så skal NAS volumet sættes til E.

# 16858 Serveradministration- og sikkerhed, 16852 Netværk I og 16852 Computerteknologi

Opdateret af EL, d. 06.04.21

Varighed: 6 uger (uge 16 til og med uge 21 (til og med 28.05.21))

Version 9

Diverse links til opsætning af FreeNAS:

FreeNAS på ESXi:

<https://www.ixsystems.com/documentation/freenas/11.2-U7/freenas.html>

iSCSI på Windows server:

<https://www.virtualizationhowto.com/2017/07/add-iscsi-shared-storage-in-windows-server-2016/>

<https://www.youtube.com/watch?v=t3B1biwVVmg>

[https://www.youtube.com/watch?v=-3FEA\\_CEWBo](https://www.youtube.com/watch?v=-3FEA_CEWBo)

## Tidsplan for den 6. uge

35) **Senest tirsdag d. 25. maj 2021 kl. 15.15 skal følgende være færdigt:**

- **Mindst en halv dags fejlfinding afviklet** – er færdiggjort ugen før
- **Case evaluering, fase 2** (læreren spørger de enkelte gruppe medlemmer ind til de forskellige teknologier, som er brugt i casen)

36) **Senest tirsdag d. 25. maj 2021 inden midnat skal følgende være færdigt**

- **System dokumentationen** (én pr. gruppe) som afleveres elektronisk på Learn i PDF format

37) **Senest onsdag d. 26. maj 2021 inden midnat skal følgende være færdigt:**

- **For Rutineret** "Modules 10 – 13: L2 Security and WLANs Exam" i "Module Group Exams" med minimum bestået 50 %.
- **For Avanceret** "Modules 10 – 13: L2 Security and WLANs 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 %.

38) Onsdag d. 26. maj 2021 bruges til at forberede gruppe præsentationen for klassen til om torsdagen. Jeg læser systemdokumentationer om formiddagen i lokale 9.

39) Torsdag d. 27. maj 2021 skal grupperne fremlægge projektet for klassen på PowerPoint. Brug ca. 15 min. og del fremlægningen ligeligt imellem jer.

40) Fredag d. 28. maj 2021 ryddes der op, netværksudstyr og server nulstilles og afmonteres fra Rackskabene. Derefter fri 😊

### TEORI (estimeret 2-5 dage):

#### NETVÆRK I (CCNA2v7)

##### Rutineret:

Eleven skal tage "Modules 10 – 13: L2 Security and WLANs Exam" i "Module Group Exams" med minimum bestået 50 %.

##### Avanceret:

Eleven skal mindst tage "Modules 10 – 13: L2 Security and WLANs 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 I. Bemærk: Den praktiske evaluering vægter en smule mere end den teoretiske.

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

- 1) Topologi, IP-Plan, Brugermatrix
- 2) Opbygningen af den virtuelle host (ESXi), f.eks. Raid, Datastore,
  - a. Visning af de virtuelle servere
  - b. Visning af de fysiske klienter
- 3) De 2 DC servere
  - a. Visning af navngivning og statisk IP (IPv4 og v6)
  - b. Visning af AD strukturen
  - c. Visning af DNS
  - d. Visning af DHCP
  - e. Visning af Trust opsætningen og funktionalitet
  - f. Visning af diverse GPO opsætninger, såsom drev mapping, password krav, printer tildeling mm.
- 4) Fil- og Print server
  - a. Visning af navngivning og statisk IP samt ekstra drev d.
  - b. Visning af Printer administrationen (Print management, GPO)
  - c. Visning af Shared mapper
  - d. Visning af Secured mapper
- 5) WSUS
  - a. Visning af navngivning og statisk IP samt ekstra drev d.
  - b. Visning af WSUS server opsætning
  - c. Visning af GPO
  - d. Vis at update kan styres centralt
- 6) Router:
  - a. Statiske IP adresser (IPv4 og v6)
  - b. Standard login sikkerhed med bla. SSH
  - c. Sub-interfaces
  - d. HSRP
  - e. Statisk routing
  - f. Brug af show kommandoer
- 7) Switche:
  - a. Remote opsætning (SSH, IP, default gateway)
  - b. VLANs (Access/Trunk)
  - c. Port security
  - d. EtherChannel
  - e. STP
  - f. Brug af show kommandoer
- 8) Access point:
  - a. Opsætning af AP'er
    - i. Deaktivering af services
    - ii. Ændring af statisk IP
    - iii. Forklaring af WI-FI sikkerhed, er WPA vs WPA2 vs WPA3 (AES/TKIP), SSID, båndbredde G/N/AC, kryptering og trådløs MAC-filter
    - iv. Connect en end-device til WI-FI (f.eks. en Smartphone)

## Læringsmål:

Ved afslutningen af casen skal du være bekendt med følgende:

- Planlægge et mindre firmanetværk, som inkluderer:
  - en netværkstopologi
  - en IP Plan
  - en bruger matrix
  - en tidsplan
  - en dagslog / fejllog
- Installering og konfiguration af et virtuelt miljø på en HyperVisor platform, herunder:
  - Konfiguration af et hardware Raid
  - Forståelse af netværksdelen, såsom vSwitch, Port Groups og fysiske Lan interfaces
  - Forståelse og brug af Datastore, såsom upload af ISO images
  - Oprettelse, installation og administration af en Virtuel Machine
- Installering, implementering og administration af et Active Directory, herunder:
  - Administration og oprettelse af objekter i Active Directory
  - Administration og oprettelse af Group Policy
  - Forståelse og administration af DNS
  - Installation og administration af DHCP Scopes
  - Oprettelse af trust mellem 2 Forest/domains
- Installering af Memberservers, herunder:
  - Indmelding i et MS domain
  - Installation af serverroller
  - Håndtering af Sharing og Security rettigheder i et filsystem
- Opsætning og administration af en netværks Router, herunder
  - Forståelse og konfiguration af SubInterfaces
  - Forståelse og konfiguration af HSRP
  - Forståelse og konfiguration af statisk routing
  - Implementering af login sikkerhed
- Opsætning og administration af en netværks Switch, herunder
  - Forståelse og konfiguration af VLANs
  - Forståelse og konfiguration af Access vs Trunk porte
  - Forståelse og konfiguration af EtherChannel
  - Forståelse og implementering af STP
  - Implementering af port sikkerhed
  - Implementering af login sikkerhed
- Opsætning og konfiguration af WLAN og sikkerhed
- Kende til, beregne og implementere et IPv4 subnet
- Kende til, beregne og implementere et IPv6 subnet