ascom

IP Training Programme

HOUSE OF TECHNOLOGY

- en del af mercantec

Module 1: IP Generic

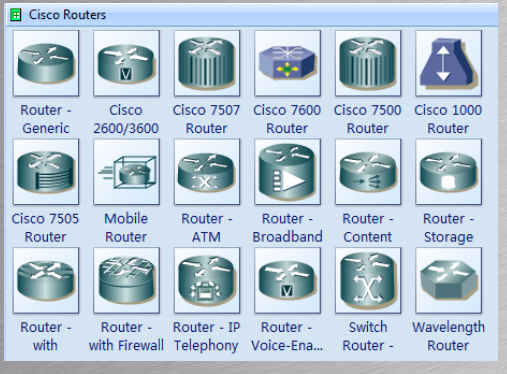
Session 4: Applications and protocols

ascom

HOUSE OF TECHNOLOGY

- en del af mercantec

ROUTING PROTOCOLS



Route table creation

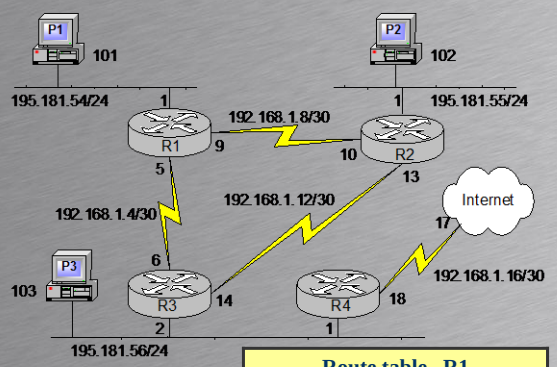
- The route table in routers can be created and maintained in two ways
  1: Static route table entry
  - Entries are entered manually

  2: Dynamic route table entry
  - Entries are sent between routers automatically
  - Require the use of a Routing protocol – such as
    - RIP, OSPF, IS-IS or BGP

RIP

- RIP will transmit its Routing table to its neighbor routers every 30. seconds.
- The neighbors will learn the transmitting routers logical networks.
- The neighbors will transmit their routing tables so the local router learns their logical networks.

Convergence!
Everybody knows everybody



Route table R1

NETWORK	SEND TO	HOP
195.181.54/24	195.181.54.1	1
192.168.1.4/30	192.168.1.5	1
192.168.1.8/30	192.168.1.9	1
195.181.55/24	192.168.1.10	2
192.168.1.12/30	192.168.1.10	2
195.181.56/24	192.168.1.6	2
192.168.1.16/30	192.168.1.6	3
0.0.0.0	192.168.1.6	4

Route table R2

NETWORK	SEND TO	HOP
195.181.55/24	195.181.55.1	1
192.168.1.8/30	192.168.1.10	1
192.168.1.12/30	192.168.1.13	1
195.181.54/24	192.168.1.9	2
192.168.1.4/30	192.168.1.9	2
195.181.56/30	192.168.1.14	2
192.168.1.16/30	192.168.1.14	3
0.0.0.0	192.168.1.14	4

Route table R3

NETWORK	SEND TO	HOP
195.181.56/24	195.181.56.2	1
192.168.1.4/30	192.168.1.6	1
192.168.1.12/30	192.168.1.14	1
195.181.54/24	192.168.1.5	2
192.168.1.8/30	192.168.1.5	2
195.181.55/24	192.168.1.13	2
192.168.1.16/30	195.181.56.1	2
0.0.0.0	195.181.56.1	3

Route table R4

NETWORK	SEND TO	HOP
195.181.56/30	195.181.56.1	1
192.168.1.16/30	192.168.1.18	1
192.168.1.4/30	195.181.56.2	2
192.168.1.12/30	195.181.56.2	2
195.181.54/24	195.181.56.2	3
195.181.55/24	195.181.56.2	3
192.168.1.8/30	195.181.56.2	3
0.0.0.0	192.168.1.17	2

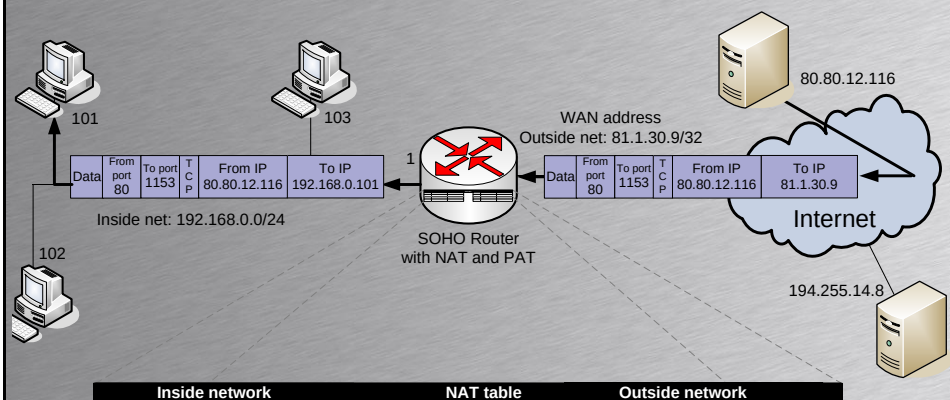
NAT translation
private IP addresses

- NAT: Network Address Translation
  - -one to one IP address translation
- Translates IP addresses from inside to outside network
- Private IP adresses allocated to be used behind NAT
  - -10.0.0.0/8
    - 10.0.0.0 to 10.255.255.255
  - -172.16.0.0/12
    - 172.16.0.0 to 172.31.255.255
  - -192.168.0.0/16
    - 192.168.0.0 to 192.168.255.255
- NAT hides the inside network (LAN) from the outside

NAT and PAT

- TCP and UDP uses port numbers.
- NAT/PAT software keeps track on connections using:
  - Protocol (eg. TCP)
  - Inside from IP (eg. 192.168.0.101)
  - Inside from port (eg. Port 1152)
  - Outside to IP (eg. 80.80.12.116)
  - Outside to port (eg. port 80)
- The five parameters describe a unique connection

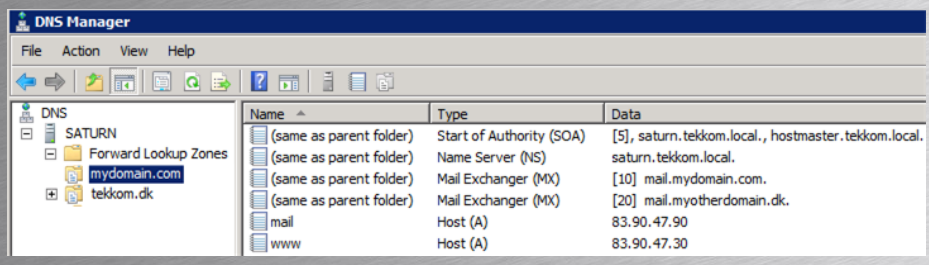
Always unique ports



Inside network			NAT table	Outside network		
Protocol	From	To		Protocol	From	To
TCP	192.168.0.101:1152	80.80.12.116:80	↔	TCP	81.1.30.9:1152	80.80.12.116:80
TCP	192.168.0.102:1152	80.80.12.116:80	↔	TCP	81.1.30.9:2345	80.80.12.116:80
TCP	192.168.0.101:1153	80.80.12.116:80	↔	TCP	81.1.30.9:1153	80.80.12.116:80

Windows DNS Server

- Windows server version 2003, 2008 and 2012 has intutive DNS server management tools.



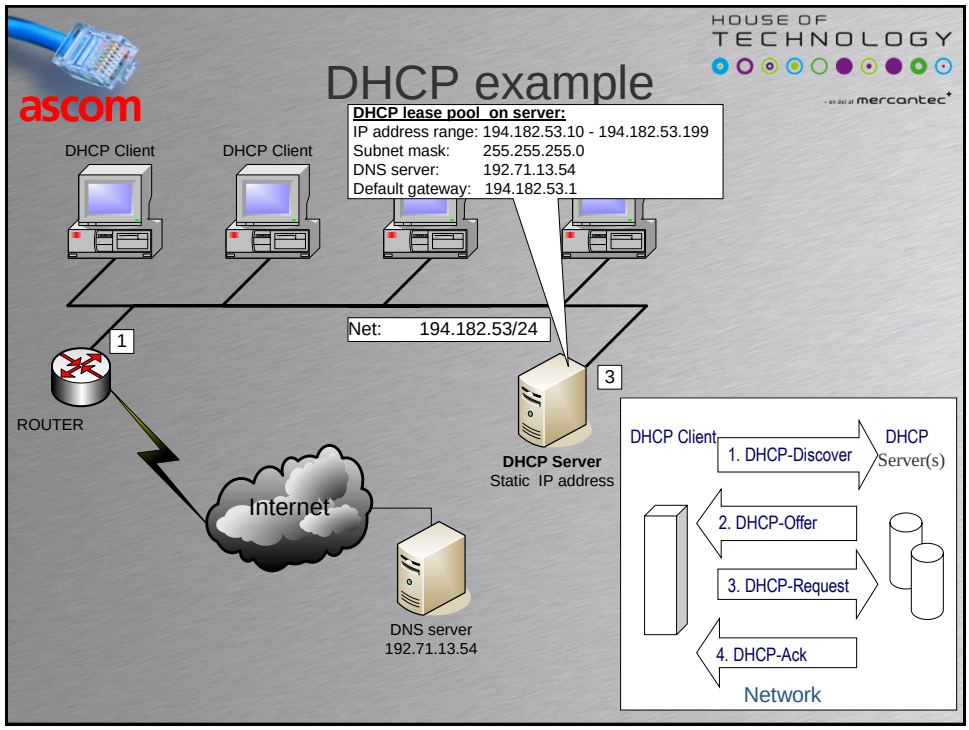
- mail.mydomain.com A record points to 83.90.47.90
- www.mydomain.com A record points to 83.90.47.30
- mail.mydomain.com MX record (preference=10)
- mail.myotherdomain.dk MX record (preference=20)

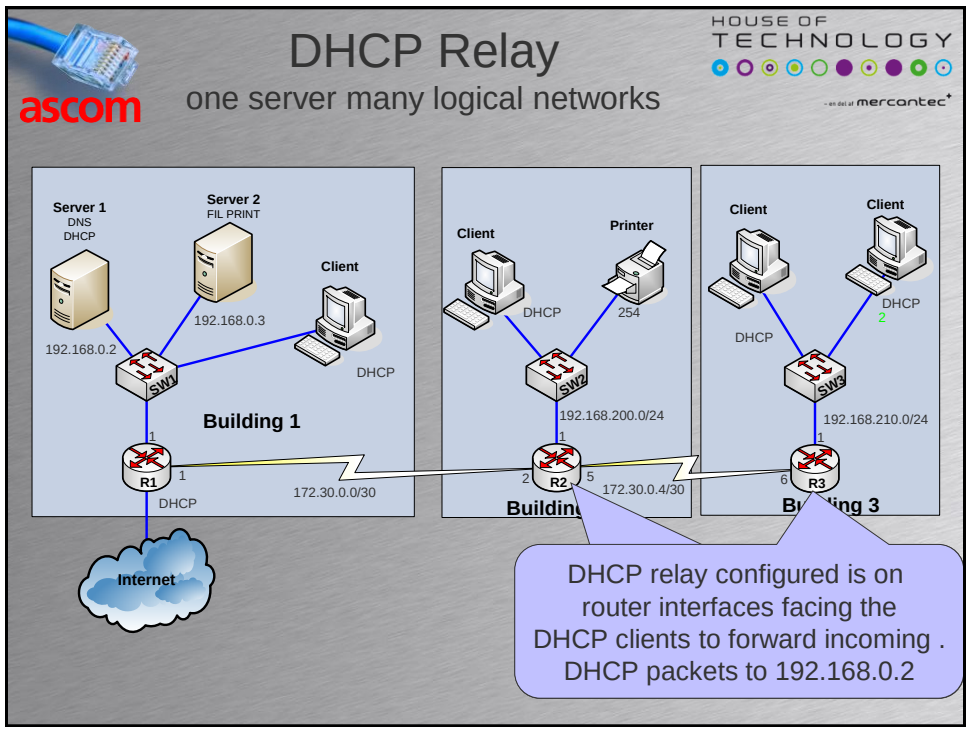
DNS zone records

- **MX** – Mail eXchange
  - Shows Mail servers for the domain.
- The ascom.se domain has two mail servers
  - Mail.ascom.se and mail.ascom.nl
  - The mailserver with lowest preference has highest priority and will be used first. If unreachable the next lowest preference is tried.
- The IP address of the mail server(s) is found using a A-record lookup

Command Prompt

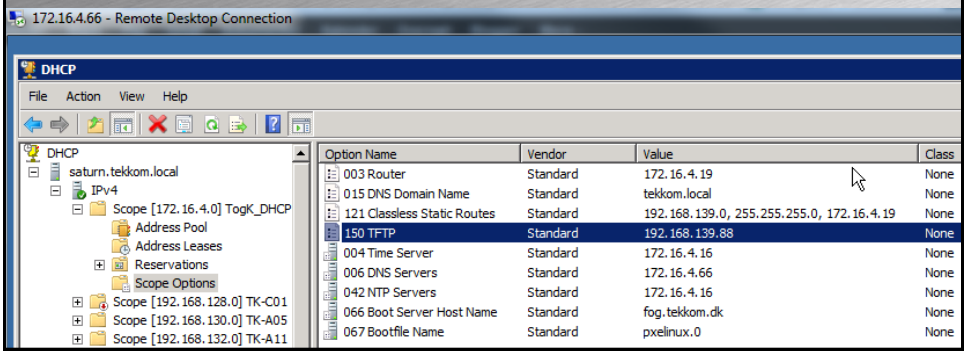
```
C:\>nslookup -type=MX ascom.se
Server:  resolver1.opendns.com
Address:  208.67.222.222

Non-authoritative answer:
ascom.se        MX preference = 10, mail exchanger = mail.ascom.se
ascom.se        MX preference = 20, mail exchanger = mail.ascom.nl
```


ascom
HOUSE OF TECHNOLOGY
mercantec
DHCP example
DHCP lease pool on server:
IP address range: 194.182.53.10 - 194.182.53.199
Subnet mask: 255.255.255.0
DNS server: 192.71.13.54
Default gateway: 194.182.53.1
DHCP Client
DHCP Client
Net: 194.182.53/24
1
ROUTER
3
DHCP Server
Static IP address
Internet
DNS server
192.71.13.54
DHCP Client
1. DHCP-Discover
DHCP Server(s)
2. DHCP-Offer
3. DHCP-Request
4. DHCP-Ack
Network


ascom
HOUSE OF TECHNOLOGY
mercantec
DHCP Relay
one server many logical networks
Server 1
DNS
DHCP
Server 2
FIL PRINT
Client
192.168.0.3
192.168.0.2
SW1
DHCP
Building 1
R1
1
DHCP
172.30.0.0/30
Internet
Client
Printer
DHCP
254
SW2
192.168.200.0/24
R2
2
5
172.30.0.4/30
Client
Client
DHCP
2
DHCP
SW3
192.168.210.0/24
R3
6
DHCP relay configured is on router interfaces facing the DHCP clients to forward incoming . DHCP packets to 192.168.0.2

DHCP options

- Windows DHCP server options configuration example
- TFTP servers are often used to store IP phones configuration files.



Subnetting

- Classfull IP addresses

Network part	Host part

- For example: 172.16.4.5/16
  - Network part 172.16
  - Host part: 4.5
- Classless IP addresses

Network part	Subnet part	Host part

- For example 172.16.4.5/24
  - Network part: 172.16.4
  - Host part: 5

Classless IP addresses

- Subnettet class B network as /24
  - One class B net subnettet to 256 subnets

Network	Subnet mask	Max hosts
172.16.0.0	255.255.255.0	254
172.16.1.0	255.255.255.0	254
172.16.2.0	255.255.255.0	254
...	...	...
172.16.253.0	255.255.255.0	254
172.16.254.0	255.255.255.0	254
172.16.255.0	255.255.255.0	254

Exponentiation

- Mathematical operation
- Called “potens” in Swedish, Norwegian and Danish.
- 2^5 = 2 ^ 5 = 2 * 2 * 2 * 2 * 2 = 32
- 7^2 = 7 ^ 2 = 7 * 7 = 49
- 2^{64} = 2 ^ 64 = 18.446.744.073.709.551.616
- Often used when dealing with numeric systems.

Numeric systems II

8367_{10}

```
7*10^0 = 7*1    =    7
6*10^1 = 6*10   =   60
3*10^2 = 3*100  =  300
8*10^3 = 8*1000 = 8000
Decimal sum     = 8367
```

1101_{2}

```
1*2^0  = 1*1    =    1
0*2^1  = 0*2    =    0
1*2^2  = 1*4    =    4
1*2^3  = 1*8    =    8
Decimal sum     =   13
```

The binary byte

11111111_{2}

```
1*2^0  = 1*1    =   1
1*2^1  = 1*2    =   2
1*2^2  = 1*4    =   4
1*2^3  = 1*8    =   8
1*2^4  = 1*16   =  16
1*2^5  = 1*32   =  32
1*2^6  = 1*64   =  64
1*2^7  = 1*128  = 128
Decimal sum     = 255
```

The binary byte

11111000_2

```
0*2^0  = 1*1    =   0
0*2^1  = 1*2    =   0
0*2^2  = 1*4    =   0
1*2^3  = 1*8    =   8
1*2^4  = 1*16   =  16
1*2^5  = 1*32   =  32
1*2^6  = 1*64   =  64
1*2^7  = 1*128  = 128
Decimal sum     = 248
```

Classless IP addresses

- A binary “1” in the subnet mask means the bit belongs to the logical network or subnet
- A binary “0” in the subnet mask means the bit belongs to the host part of the IP address

Prefix	Subnet mask - decimal	Subnet mask - binary
/24	255.255.255.0	11111111.11111111.11111111.00000000
/25	255.255.255.128	11111111.11111111.11111111.10000000
/26	255.255.255.192	11111111.11111111.11111111.11000000
/27	255.255.255.224	11111111.11111111.11111111.11100000
/28	255.255.255.240	11111111.11111111.11111111.11110000
/29	255.255.255.248	11111111.11111111.11111111.11111000
/30	255.255.255.252	11111111.11111111.11111111.11111100

Classless IP addresses

- To adapt the size of a logical network to customer networks the classes were abandoned.
  - Subnets is logical networks

prefix	Subnet mask	Subnets	Max hosts
/24	255.255.255.0	1	254
/25	255.255.255.128	2	126
/26	255.255.255.192	4	62
/27	255.255.255.224	8	30
/28	255.255.255.240	16	14
/29	255.255.255.248	32	6
/30	255.255.255.252	64	2

Network and broadcast

- Two IP addresses of each logical network is reserved for special purposes. They are illegal as host IP addresses
  - All host bits “0” is the logical network name
  - All host bits “1” is the local broadcast IP address
- For example the 192.168.100.0/24 network
  - 192.168.100.0 is the network name
  - 192.168.100.255 is the broadcast address
  - Usable IP address ranges from
    - 192.168.100.1 to 192.168.100.254
    - A total of 254 usable addresses

A /24 network

		Net part	Host part
195 . 181 . 54 . 0	=	11000011 . 10110101 . 00110110	00000000
195 . 181 . 54 . 1	=	11000011 . 10110101 . 00110110	00000001
195 . 181 . 54 . 2	=	11000011 . 10110101 . 00110110	00000010
			:
		. 00110110	00111110
		. 00110110	00111111
		. 00110110	01000000
		. 00110110	01000001
:		:	:
195 . 181 . 54 . 126	=	11000011 . 10110101 . 00110110	01111110
195 . 181 . 54 . 127	=	11000011 . 10110101 . 00110110	01111111
		. 00110110	10000000
		. 00110110	10000001
			:
		. 00110110	10111110
		. 00110110	10111111
		. 00110110	11000000
195 . 181 . 54 . 193	=	110000 . 10110101 . 00110110	11000001
:		:	:
195 . 181 . 54 . 254	=	11000011 . 10110101 . 00110110	11111110
195 . 181 . 54 . 255	=	11000011 . 10110101 . 00110110	11111111

195.181.54.0/24

All host bits zero. This is a Illegal IP address and is used as the network name

All host bits one. This is a Illegal IP address and is used as the broadcast address of the network

Two /25 networks

		Net part - subnet part blue	Host part
195 . 181 . 54 . 0	=	11000011 . 10110101 . 00110110	00000000
195 . 181		110	00000001
195 . 181		110	00000010
			:
195 . 181		110	00111110
195 . 181		110	00111111
195 . 181		110	01000000
195 . 181 . 54 . 65	=	11000011 . 1011 . 00110110	01000001
:		:	:
195 . 181 . 54 . 126	=	11000011 . 10110101 . 0011 . 10	01111110
195 . 181 . 54 . 127	=	11000011 . 10110101 . 00110110	01111111
195 . 181 . 54 . 128	=	11000011 . 10110101 . 00110110	10000000
195 . 181 . 54 . 129	=	11000011 . 1011 . 00110110	10000001
			:
		0110110	10111110
		0110110	10111111
		0110110	11000000
		00110110	11000001
:		:	:
195 . 181 . 54 . 254	=	11000011 . 10110101 . 00110110	11111110
195 . 181 . 54 . 255	=	11000011 . 10110101 . 00110110	11111111

195.181.54.0/25

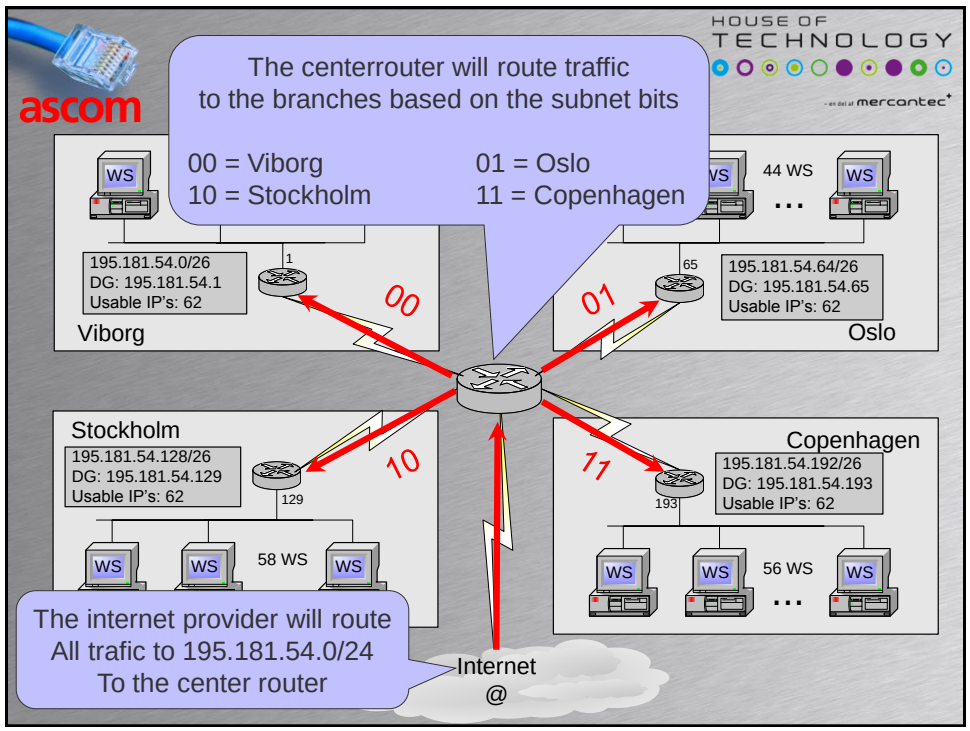
195.181.54.128/25

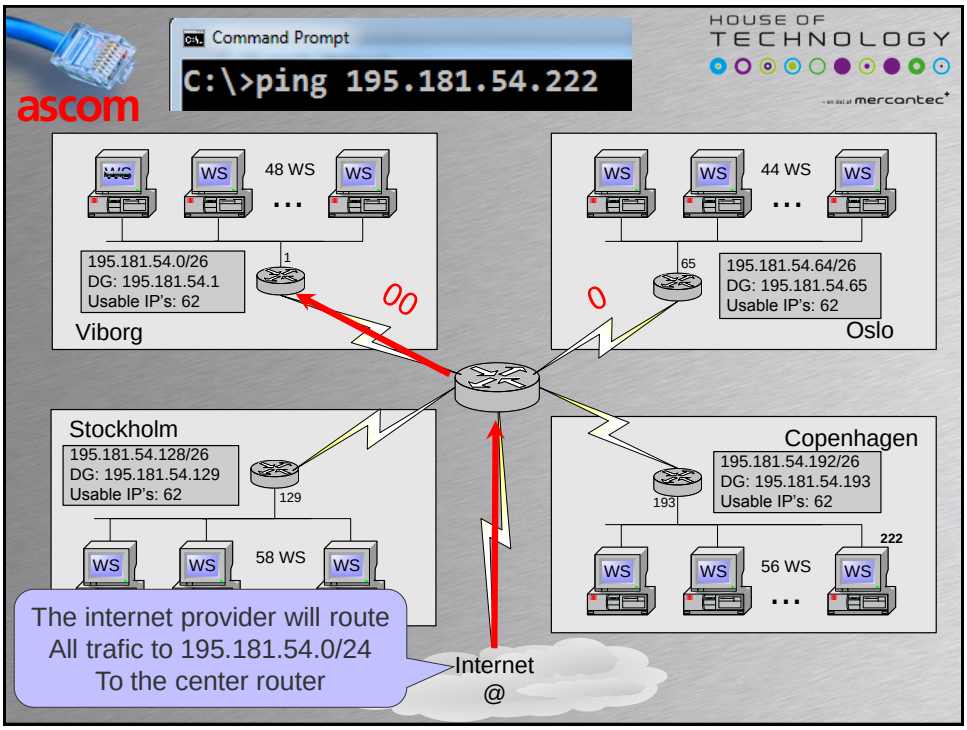
All seven host bits one. This is a Illegal IP address and is used as the broadcast address of the Network 195.181.54.0/25

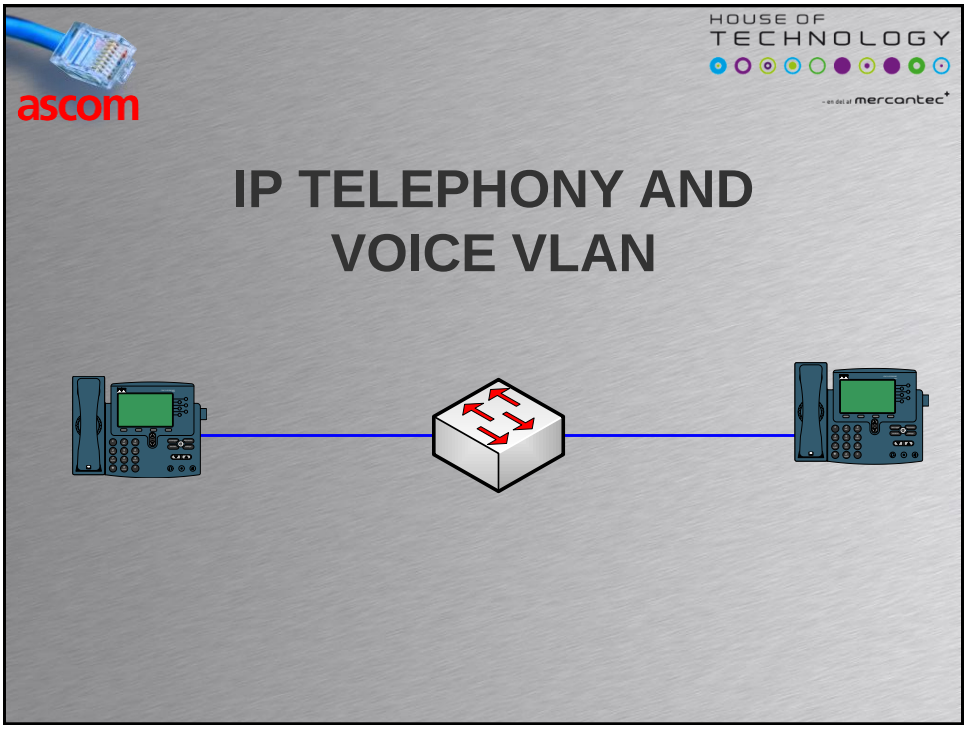
All seven host bits zero. This is a Illegal IP address and is used as the network name 195.181.54.128/25

Four /26 networks

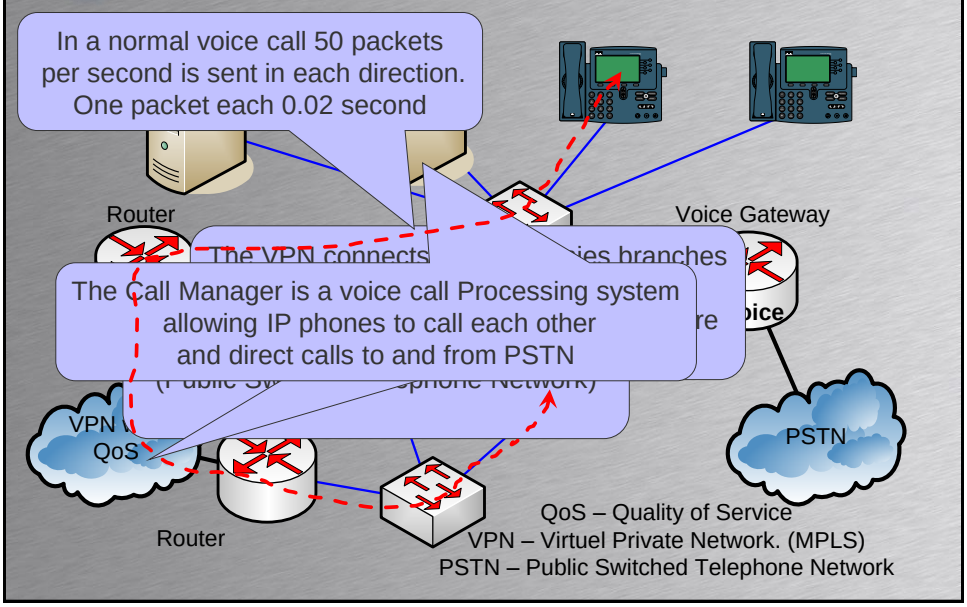
		Net part - subnet part blue	Host part	
195 . 181 . 54 . 0	=	11000011 . 10110101 . 00110110 .	00000000	195.181.54.0/26
195 . 181 . 54 . 1	=	11000011 . 10110101 . 00110110 .	00000001	
195 . 181 . 54 . 2	=	11000011 . 10110101 . 00110110 .	00000010	
:		:	:	
195 . 181 . 54 . 62	=	11000011 . 10110101 . 00110110 .	00111110	
195 . 181 . 54 . 63	=	11000011 . 10110101 . 00110110 .	00111111	
195 . 181 . 54 . 64	=	11000011 . 10110101 . 00110110 .	01000000	195.181.54.64/26
195 . 181 . 54 . 65	=	11000011 . 10110101 . 00110110 .	01000001	
:		:	:	
195 . 181 . 54 . 126	=	11000011 . 10110101 . 00110110 .	01111110	
195 . 181 . 54 . 127	=	11000011 . 10110101 . 00110110 .	01111111	
195 . 181 . 54 . 128	=	11000011 . 10110101 . 00110110 .	10000000	195.181.54.128/26
195 . 181 . 54 . 129	=	11000011 . 10110101 . 00110110 .	10000001	
:		:	:	
195 . 181 . 54 . 190	=	11000011 . 10110101 . 00110110 .	10111110	
195 . 181 . 54 . 191	=	11000011 . 10110101 . 00110110 .	10111111	
195 . 181 . 54 . 192	=	11000011 . 10110101 . 00110110 .	11000000	195.181.54.192/26
195 . 181 . 54 . 193	=	11000011 . 10110101 . 00110110 .	11000001	
:		:	:	
195 . 181 . 54 . 254	=	11000011 . 10110101 . 00110110 .	11111110	
195 . 181 . 54 . 255	=	11000011 . 10110101 . 00110110 .	11111111	




ascom
Command Prompt
C:\>ping 195.181.54.222
HOUSE OF TECHNOLOGY
mercantec
WS
48 WS
195.181.54.0/26
DG: 195.181.54.1
Usable IP's: 62
1
Viborg
44 WS
65
195.181.54.64/26
DG: 195.181.54.65
Usable IP's: 62
Oslo
Stockholm
195.181.54.128/26
DG: 195.181.54.129
Usable IP's: 62
129
58 WS
Copenhagen
195.181.54.192/26
DG: 195.181.54.193
Usable IP's: 62
193
222
56 WS
The internet provider will route
All trafic to 195.181.54.0/24
To the center router
Internet
@


ascom
HOUSE OF TECHNOLOGY
mercantec
IP TELEPHONY AND
VOICE VLAN

IP Telephony



IP Telephony

- IP telephony is an instant service
  - Voice packet stream between phones
    - Normaly 50 packets per second
- To ensure good voice quality, voice packets should be transferred between phones
  - With low delay (< 150mS)
  - With little jitter (< 30mS)
    - Jitter is variable delay between packets in
  - With little packet loss (< 1%)

IP Telephony

- VoIP best practice is separating voice and data traffic in the network
  - Enhancing security not mixing VoIP and data
  - Troubleshooting simplified
  - Easier to deploy Quality of Service
- Two ways of separating data and voice
  - Two physical networks
  - One physical network with separate VLAN's for voice and data

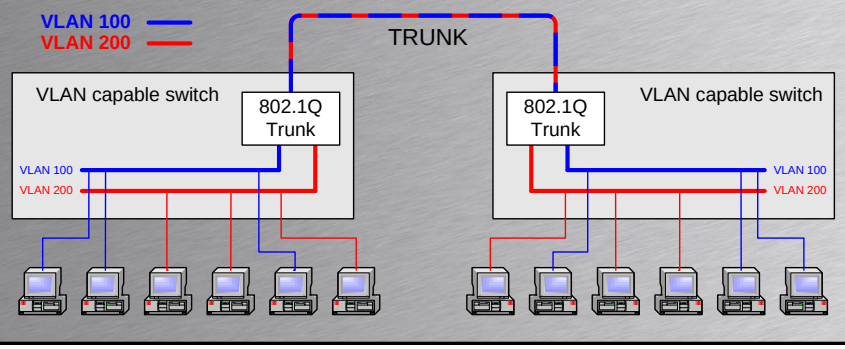
IP Telephony

- Two physical networks
  - Expensive
    - 2 x Devices, 2 x cabling and 2 x VPN's
  - Easy to ensure good voice quality
- One physical network
  - Two logical networks – one for voice one for data
    - Using a data-VLAN and a voice-VLAN
  - Cheaper
  - More difficult to ensure voice quality
    - Need end-to-end quality of service configured

VLAN Review

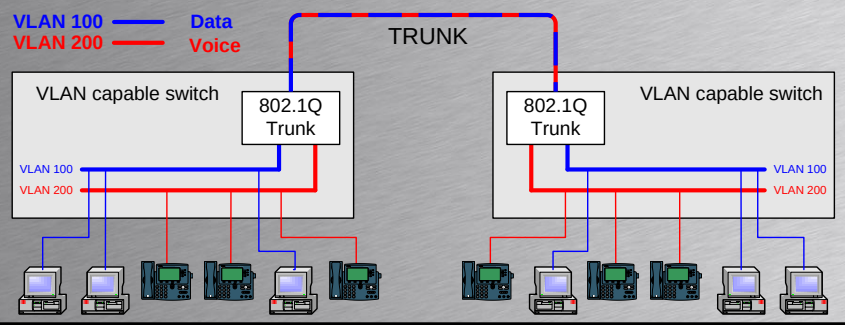
Virtual Local Area Network

- Switch ports belong to a VLAN
- Devices on same VLAN can communicate
- Switch ports configured as trunks can exchange VLAN traffic between switches



Voice VLAN option 1

- Traffic separated physically between switch and users desk
  - One cable and one switch port for users PC
  - One cable and one switch port for users IP Phone
  - Expensive in cabling and switches

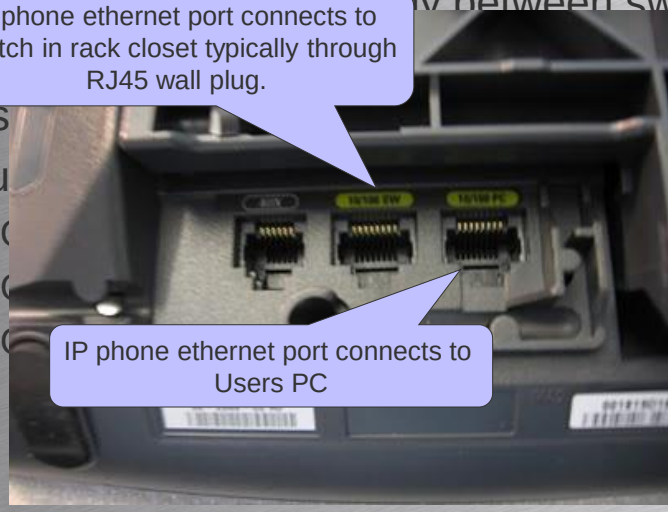


Voice VLAN option 2

ascom

HOUSE OF TECHNOLOGY

- ...lly between switch and
- Us... ...bility
- Bu... ...one
  - ...
  - ...one it self
  - ...he PC

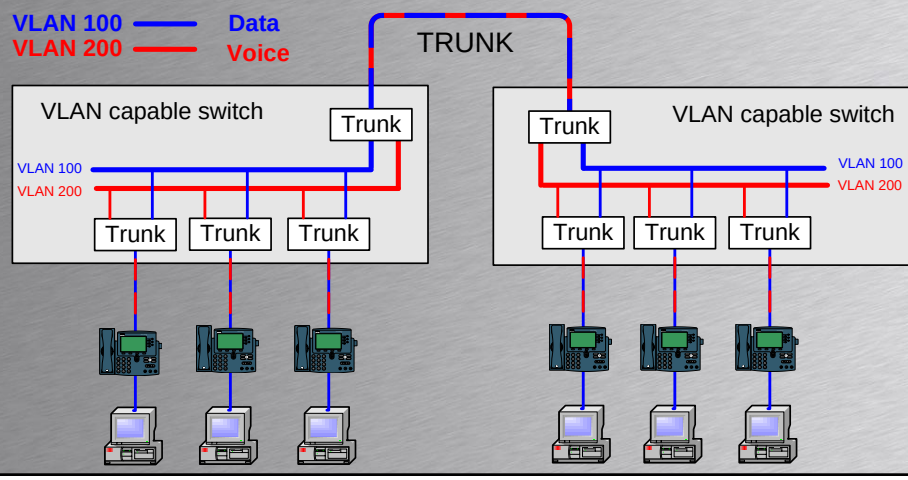


Voice VLAN option 2

ascom

HOUSE OF TECHNOLOGY

- Data traffic carried in VLAN 100
- Voice traffic carried in VLAN 200



PoE

Power over Ethernet

- Most IP phones are powered by 48 Vdc
- Many IP phones can get power from
  - External power supply connected to mains
  - From switches capable of delivering power
    - PoE or Power over Ethernet
    - Picture below is a partial printout from a PoE capable switch

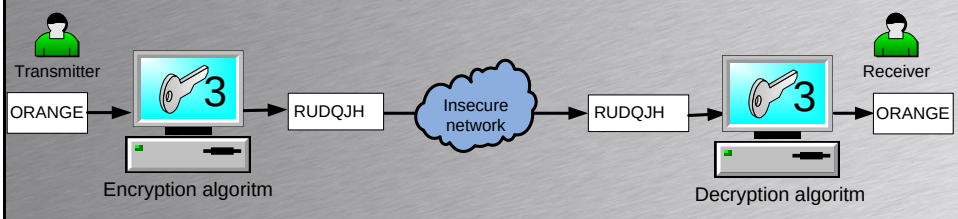
mars.tekkom.dk - PuTTY

```
Campus1#show power inline
Available:280.0(w)  Used:44.1(w)  Remaining:235.9(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa0/1     auto   on         6.3     IP Pnone 7940       2     15.4
Fa0/2     auto   on         6.3     IP Pnone 7940       2     15.4
Fa0/3     auto   off        0.0                         -     15.4
```

NETWORK SECURITY

BEST PRACTICE

Encryption/Decryption



- Encryption algorithm: Caesar cipher (Very insecure)
- Encryption key : 3 (Shift cipher 3 letters)
- Plain alfabet : ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
- Cipher alfabet : DEFGHIJKLMNOPQRSTUVWXYZ0123456789ABC
- Plain text : ORANGE
- Cipher text : RUDQJH

Breaking a cipher text

- To break an encrypted message the code breaker must know:
  - Encryption algorithm
  - Encryption key
- The most common encryption algorithm are public – we all use them
  - Paying over the internet …
  - Using “secure” WEB-pages (https://)
- The code breaker knows the encryption algorithm but not the secret key

Brute force code breaking

- Test all possible keys
- Compare clear text with database with common words
- Codebreaker find key in four attempts!

```
Key  0: RUDQJH      Key 12: FI1E75      Key 24: 36P2VT
Key  1: QTCPIG      Key 13: EH0D64      Key 25: 25O1US
Key  2: PSBOHF      Key 14: DGZC53      Key 26: 14N0TR
Key  3: ORANGE      Key 15: CFYB42      Key 27: 03MZSQ
Key  4: NQ9MFD      Key 16: BEXA31      Key 28: Z2LYRP
Key  5: MP8LEC      Key 17: ADW920      Key 29: Y1KXQO
Key  6: LO7KDB      Key 18: 9CV81Z      Key 30: X0JWPN
Key  7: KN6JCA      Key 19: 8BU70Y      Key 31: WZIVOM
Key  8: JM5IB9      Key 20: 7AT6ZX      Key 32: VYHUNL
Key  9: IL4HA8      Key 21: 69S5YW      Key 33: UXGTMK
Key 10: HK3G97      Key 22: 58R4XV      Key 34: TWFSLJ
Key 11: GJ2F86      Key 23: 47Q3WU      Key 35: SVERKI
```

Strong keys necessary

Encryption standards

Standard	Key size	Status	Time required to break*
Caesar	36 (less than 6 bit)	Very insecure	0,000.000.000.72 second
DES	56 bit	Insecure	400 days
Triple DES	56, 112 or 168 bit	(In)secure	112 bit key: 800 days
AES	128, 192 or 256 bit	Secure	128 bit key: 5 x 10^21 year

* Time required to check all possible keys at 50.000.000.000 keys per second. (reference http://arxiv.org/ftp/arxiv/papers/1003/1003.4085.pdf)

- DES = Data Encryption Standard
- AES = Advanced Encryption Standard
- Theoretical number of keys:
  - 56 bit = 2^56 = 72057594037927936
  - 256 BIT = 2^256 = 115792089237316195423570985008687907853269984665640564039457584007913129639936

Network security

- Network designers protect the network infrastructure and servers by
  - Establishing trust boundaries
  - Firewalls
- Network designers protect network from
  - Intrusion from unwanted sources
  - Non-authorized equipment
  - User authentication and user rights
  - Physical locked server rooms and wiring closets
  - Eavesdropping by encrypting data
  - …

MAC address flooding

- A switch sorts traffic based on MAC addresses.
- A switch has limited memory

mars.tekkom.dk - PuTTY

```
freja#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   4    0000.85b9.9c4d    DYNAMIC     Fa0/6
   4    0007.e940.0abf    DYNAMIC     Fa0/7
   4    000c.29de.fe14    DYNAMIC     Fa0/16
   4    0014.5e67.614a    DYNAMIC     Fa0/11
   4    0015.17c5.2898    DYNAMIC     Fa0/8
   4    0015.17c5.289a    DYNAMIC     Fa0/10
   4    0018.187c.b400    DYNAMIC     Fa0/13
```

MAC address flooding

- Symptom:
  - An attacker sends thousands of ethernet frames to a switch with random source MAC addresses
  - The switchs limited memory will be consumed and the switch will flood traffic to all ports for ethernet frames with unknown destinations.
  - The attacker can sniff packets and gain access to sensitive data

MAC address flooding

- Counter measures:
  - A port security feature which limits the number of MAC addresses on a per port basis
  - Often programmable per port number
  - Often the port will shut down for a period of time if maximum number exceeded
- Impact
  - When adding equipment in existing customer networks port security may shut down the port unintentionally

Hash function

- A hash is a mathematical function
- Maps variable length data to fixed length data
- Used to protect passwords
- Password not stored on server
- Hash stored on server

Notice small change in password e to i

mars.tekkom.dk - PuTTY

```
[root@oldmars ~]#md5 -s "MySecretPassword"
MD5 ("MySecretPassword") = 7315a012ecad1059a3634f8be1347846
[root@oldmars ~]#md5 -s "MySicretPassword"
MD5 ("MySicretPassword") = b9a762c4fb2b1e29b1bd72d537f3bee6
[root@oldmars ~]#
```

LDAP

Lightweight Directory Access Protocol

LDAP

Lightweight Directory Access Protocol

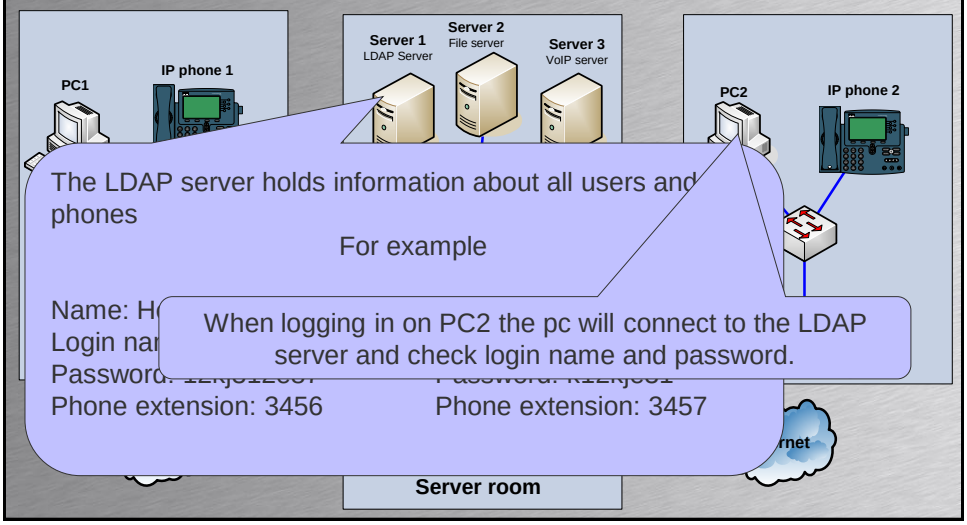
- Like an electronic telephone directory
  - LDAP server – The directory
  - LDAP client – The user
- The LDAP server for example holds
  - Login credentials (username, password)
  - User information (name, office)
  - Extension numbers for IP-Phones
  - Authorization information
- The LDAP server is used for centralized login

LDAP

Lightweight Directory Access Protocol

- Different kind of systems use the same source for information (The directory)
  - IP Phones
  - Servers
  - Client computers
- One directory for all systems
  - Needs redundancy (No single point of failure)
- LDAP is a common protocol used by hosts to access the directory and its entries.
  - LDAP is a TCP/IP based protocol

LDAP example



The LDAP server holds information about all users and phones

For example

Name: H
Login nar
Password:
Phone extension: 3456

Password:
Phone extension: 3457

When logging in on PC2 the pc will connect to the LDAP server and check login name and password.

ACTIVE DIRECTORY

Windows Server®
Active Directory

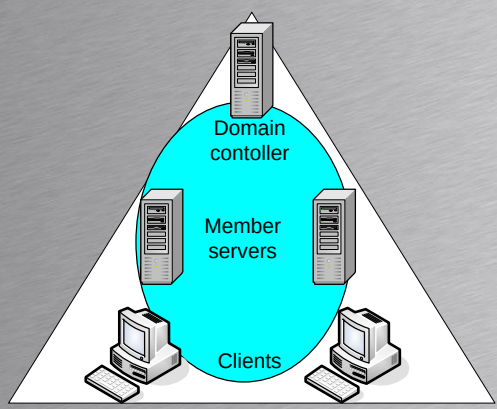
Active Directory

AD or ADS

- AD is a Microsoft developed directory service
- build for Microsoft Windows Domains
  - A domain is collection of resources (servers…)
- Uses LDAP for communication
- Uses DNS for name resolution
  - Hostnames to and from IP addresses
- Uses encryption and secure login

The AD domain

- A domain contain at least one DC
  - DC – Domain Controller
- The DC holds the Active Directory

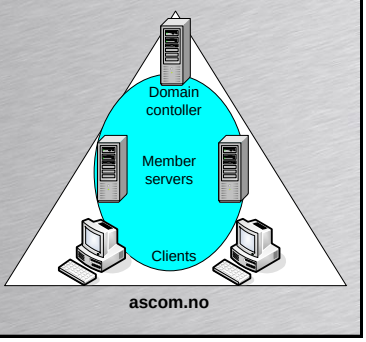


ascom.no

The AD domain

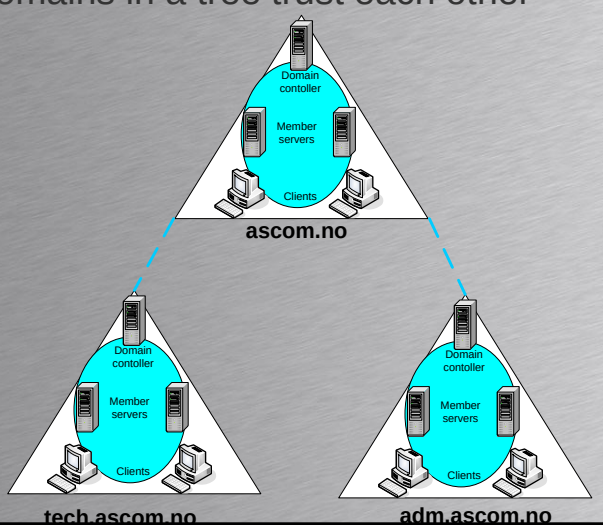
- There must be a DNS server for the domain
  - Automatically installed when installing AD
- Host register their names and IP addresses to the DNS server
  - All hosts in the domain has its own A-record
  - For example:

A record in DNS	IP address
dc.ascom.no	192.168.1.10
server1.ascom.no	192.168.1.21
server2.ascom.no	192.168.1.22
client1.ascom.no	192.168.1.101
client2.ascom.no	192.168.1.102



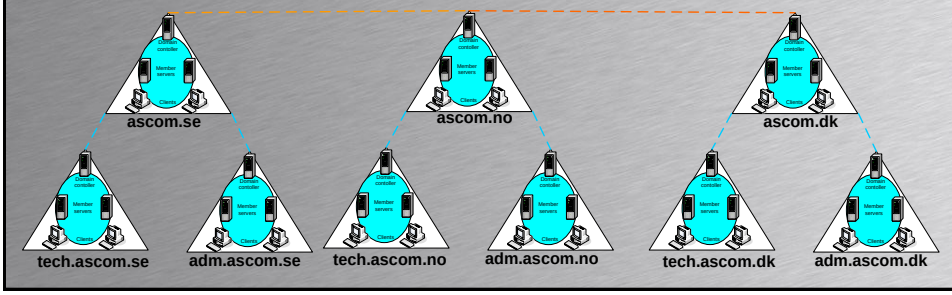
The AD tree

- A tree consist of at least one domain
  - Domains in a tree trust each other



The AD forest

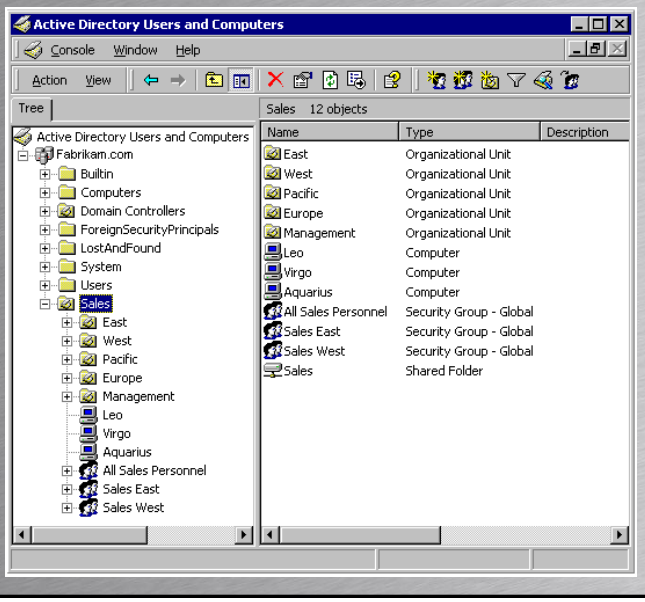
- A forest consist of at least one tree
  - trees in a forest configures to trust each other
- It is possible to build big organizational networks reflecting the actual organization
  - Not organization adapting to technology but technology adapting to organization



Some AD buzzwords

Buzzword	Explanation
Domain member	A host – server or client – belonging to a domain
Domain controller(s)	One ore more servers holding the Active Directory
Domain	Consists of at least one DC and zero or more domain members
Tree	A tree consists of one or more domains grouped in a hierarchy
Forest	A collection of one or more trees
Object	A collection of properties which together is a resource For example a user is an object consisting of many properties -username, login name, password, extension…..
OU	Organizational Unit – A container holding objects for easy administration. For example: If a OU is holding 1000 user objects – You can configure a policy on the OU to a new background image on the desktop. Then all the users PC's will show that image.

AD screenshot



SERVER TECHNOLOGIES

Client/Server

- Basically a client is a program that ask a question using a specific protocol
- Basically a server is a program that can answer a question using the same specific protocol.
- For example
  - A web browser (client) requesting to see a web page using the http protocol. (request)
  - The web server sending the web-page to the client using the http protocol. (response)

Server operating systems

- Different kind of server operating systems exist
- For example
  - Windows 2008 server
  - Windows 2012 server
  - Redhat enterprise server Linux version 6
  - Ubuntu Linux server version 12.1
  - IBM AIX Unix version 7.1
  - Apple Mac OS server
  - IBM i (Previously OS/400)
  - ….

Which server goes where?

- Basically all server OS solves the same tasks – Running server programs
- A specific OS is chosen from
  - Preference (What the administrator likes)
  - Price and performance
  - Some server programs can only run on some server OS's
    - For example Microsoft Exchange Server
    - Business Critical server programs such as big banking server running on a huge IBM mainframe

Thank you for listening

☺