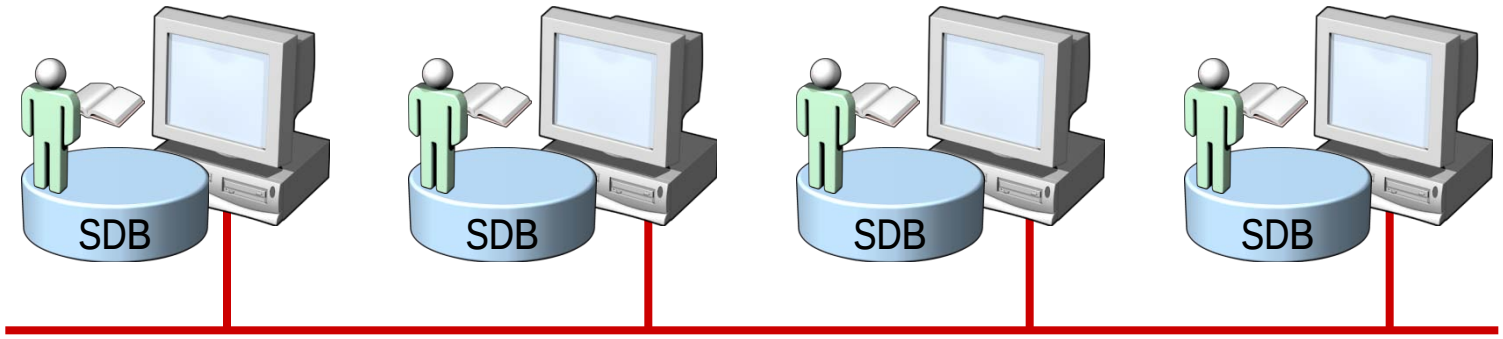
Síťování ve Windows



Mgr. Šimon Suchomel

Workgroup

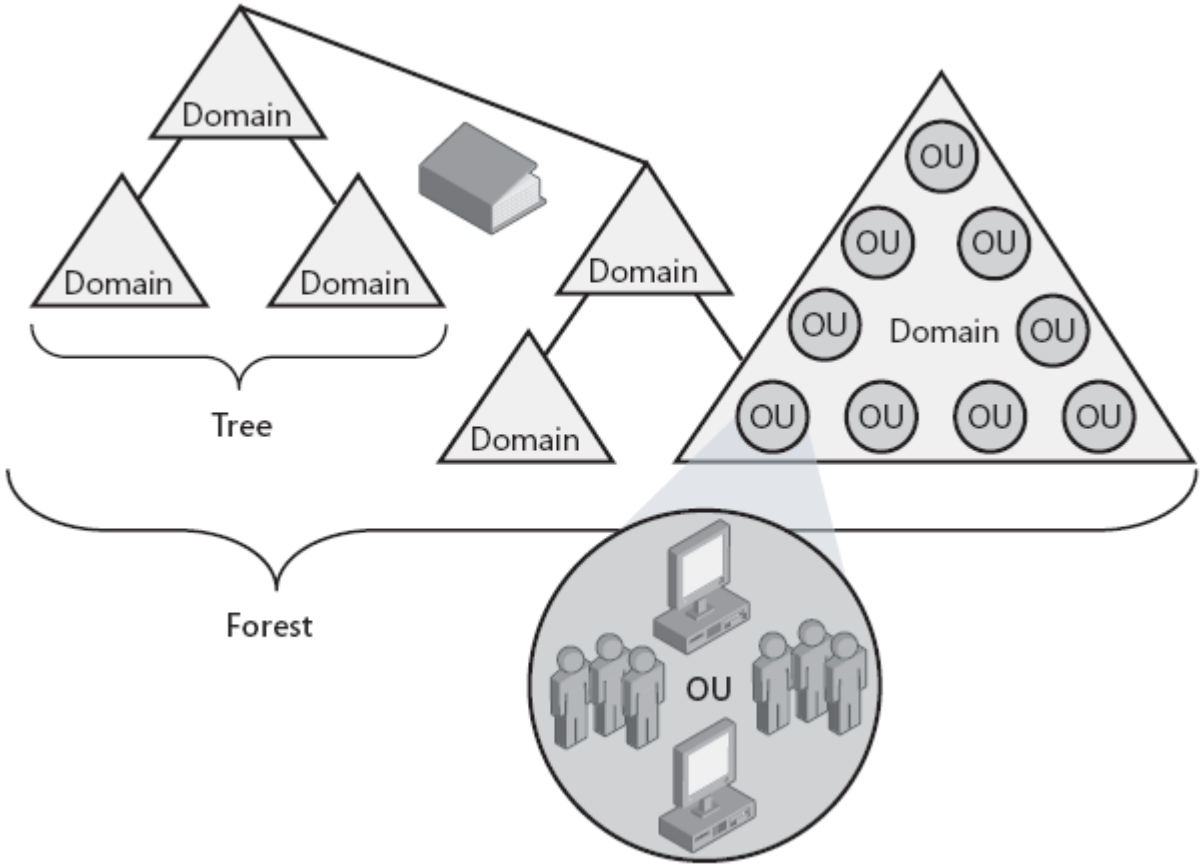
- Workgroup
  - Logické uskupení počítačů v síti, všichni jsou si rovni (peer-to-peer)
  - Všichni počítače si udržují pouze svůj ACL
  - Změna nutná všude
  - Decentralizovaná správa!
  - Nepotřebuje server
  - Jednoduché na provedení
  - Pro síť <10 počítačů



Doména Active Directory

- Centralizovaná správa
- Objekty bezpečně uloženy v jedné logické struktuře
- Optimalizuje síťový provoz
- Rozšiřitelnost
- Uživatel se přihlásí jedním účtem a má přístup ke všem prostředkům, na které má oprávnění v celé struktuře
- Oddělení logické struktury (domény, OU, objekty) od fyzické struktury sítě samotné

Logická struktura Active Directory

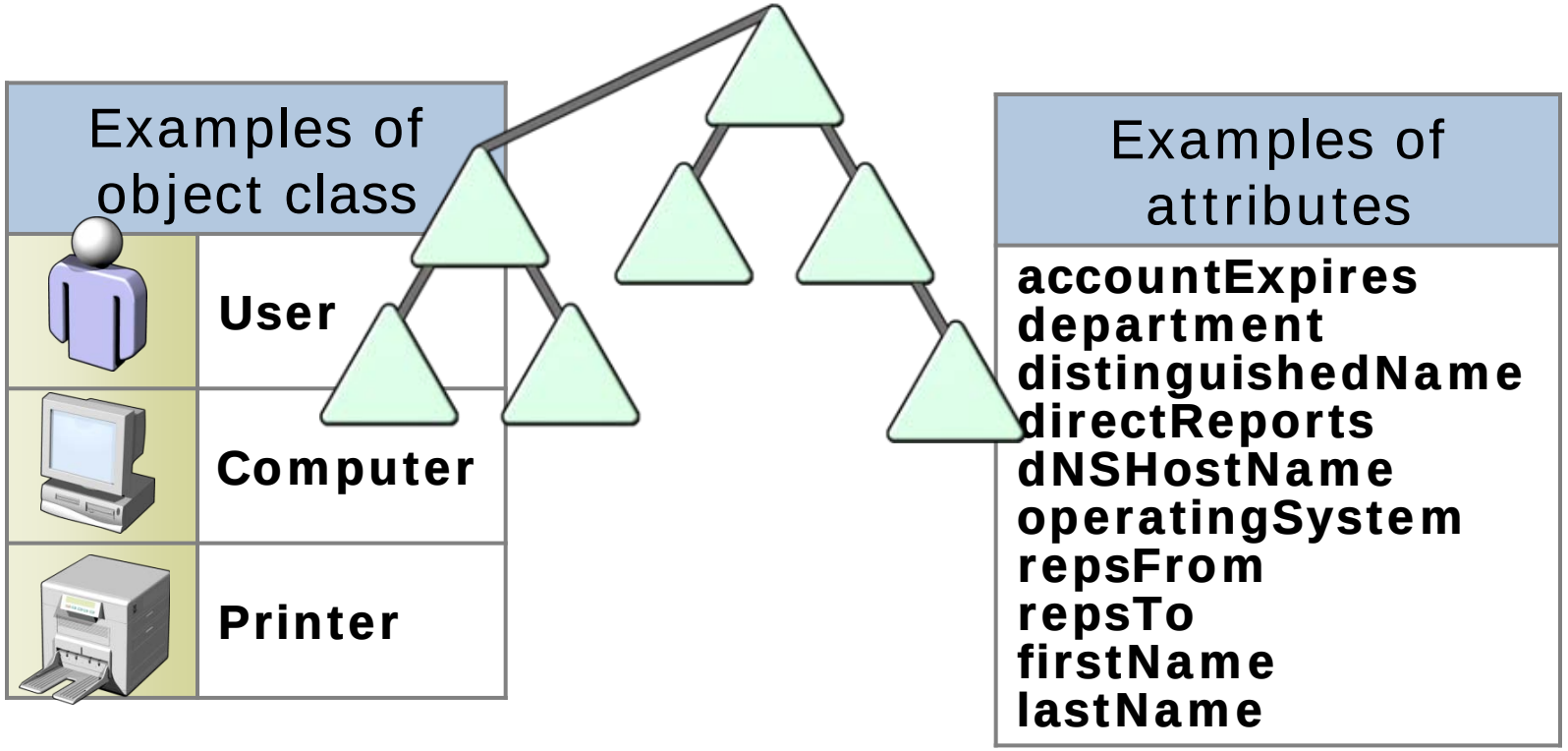


Logická struktura AD

- Objekt = jasně definovaná množina atributů představující síťový zdroj
- OU = „kontejner“ pro organizaci objektů
  - Tvoří hierarchii
  - Lze na ně aplikovat GPO
  - Lze delegovat oprávnění
- Doména
  - Hlavní logická jednotka AD
  - Množina objektů pod jednou správou
  - Pomáhá řídit bezpečnost pro sdílené prostředky
  - Objekty existují v jedné doméně a doména má informace pouze o objektech v ní obsažených
  - Autonomní v bezpečnosti
- Strom = souvislý prostor domén
- Les = více stromů, autonomní celkově, společné Schema

Active Direcrory Schema

- Active Directory = databáze
  - Standard X.500
- Popis objektů a jejich vlastností (atributů)



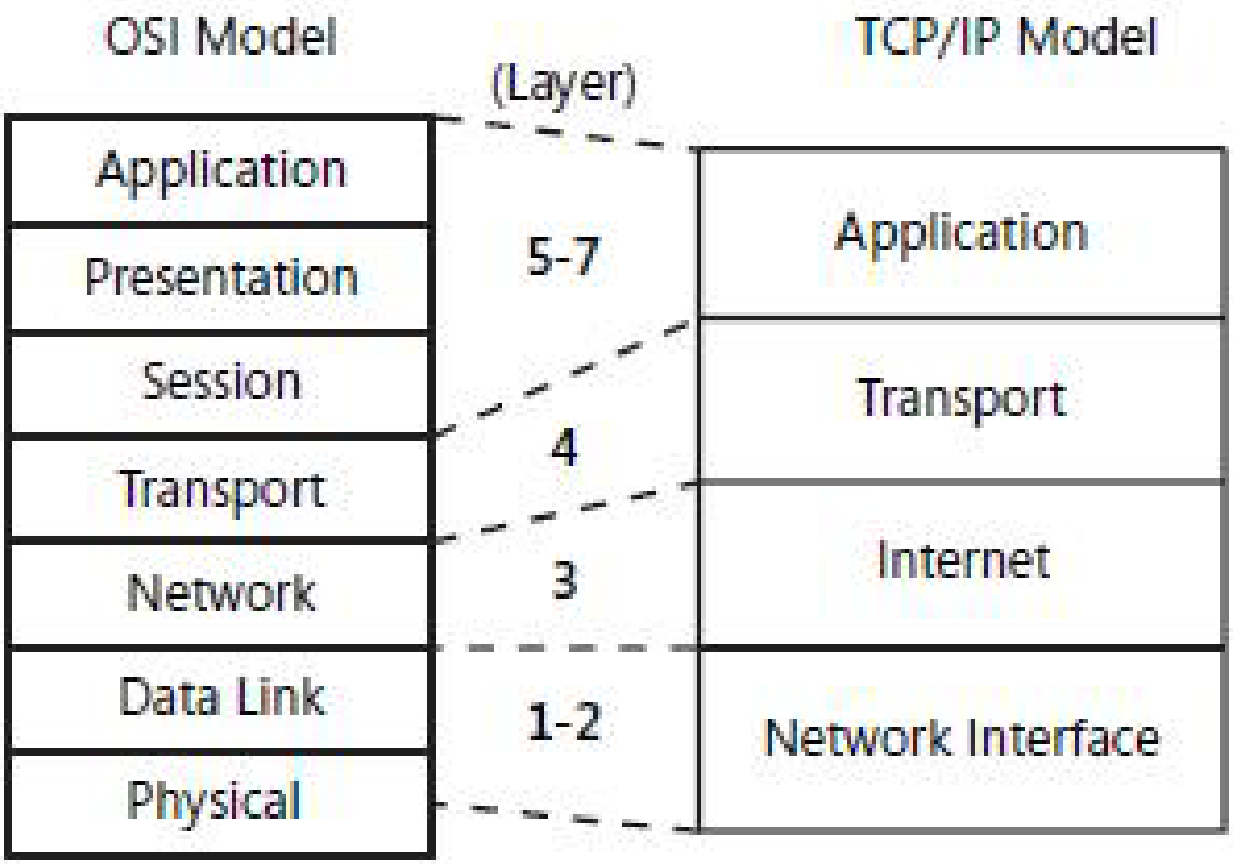
Fyzická struktura AD

- Řadiče domény (DC)
  - Počítač s Windows Server
  - Obsahuje databázi AD
  - DC mnoho, AD jedna
  - Multimaster model replikace
- Site
  - Jedna či více fyzických podsítí
  - V rámci jedné site dobré síťové spojení
  - Většinou zahrnují oblast LAN

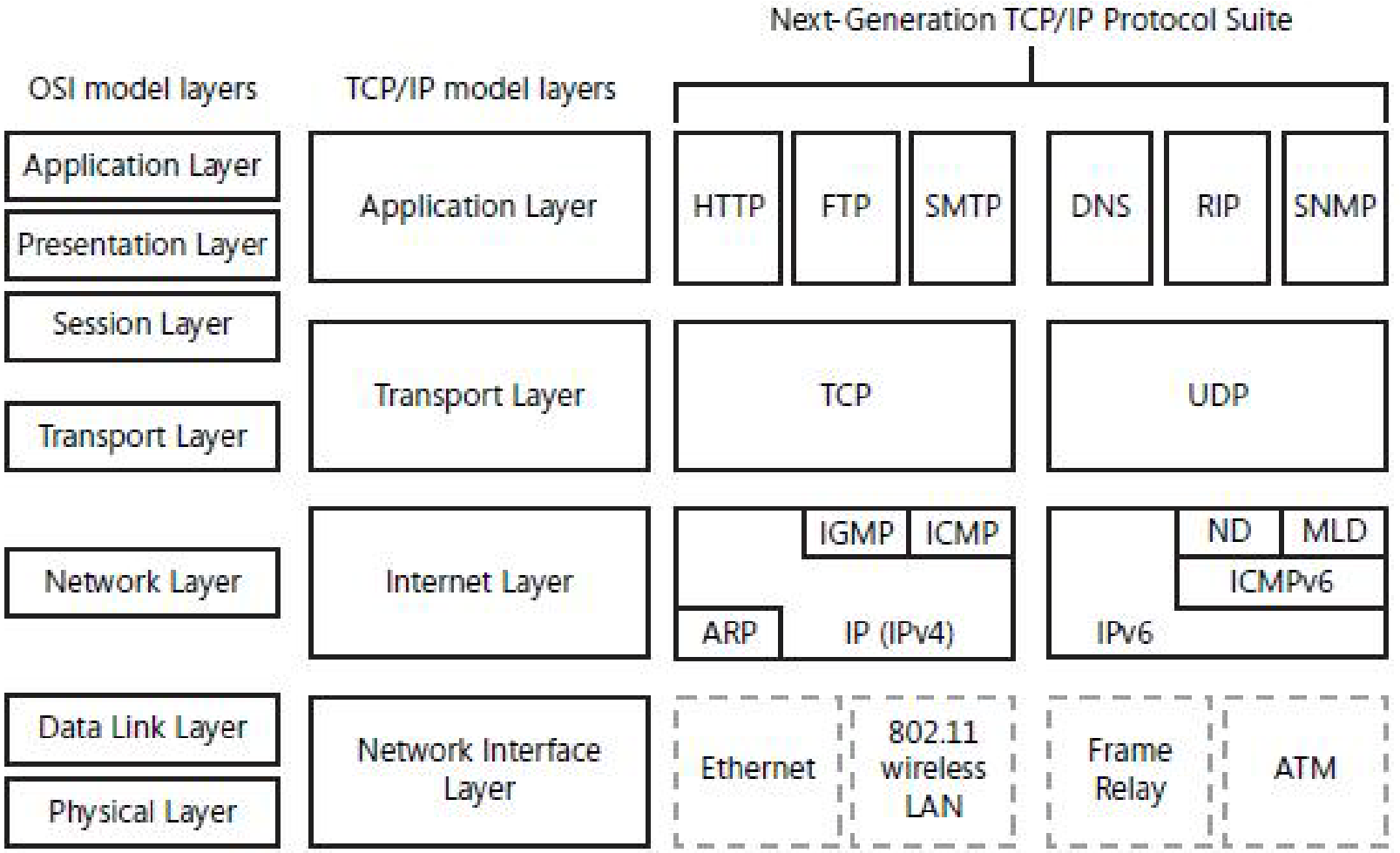
TCP/IP protokol ve Windows

- Windows používá pro přihlášení, souborové a tiskové služby, replikaci …
- Směrovatelný síťový protokol, využívá většina OS
- Windows 2000 Tahoe(NoFR)
- Technologie pro propojení různých systémů (standardní nástroje)
- Microsoft Windows Sockets (Winsock) rozhraní

4 vrstvý síťový model



4 vrstvý síťový model



Network Location Types

- Public
  - Network Discovery je zakázané, firewall blokuje všechna nevyžádaná příchozí spojení
- Private
  - Určeno pro domácí použití, kde chci sdílet prostředky, ale nemám k dispozici Active Directory DC
- Domain
  - Když se autentizuje k DC, Network Discovery a firewall zakázané, počítá se s využitím Group Policy

Jak Windows hledá síťové zdroje

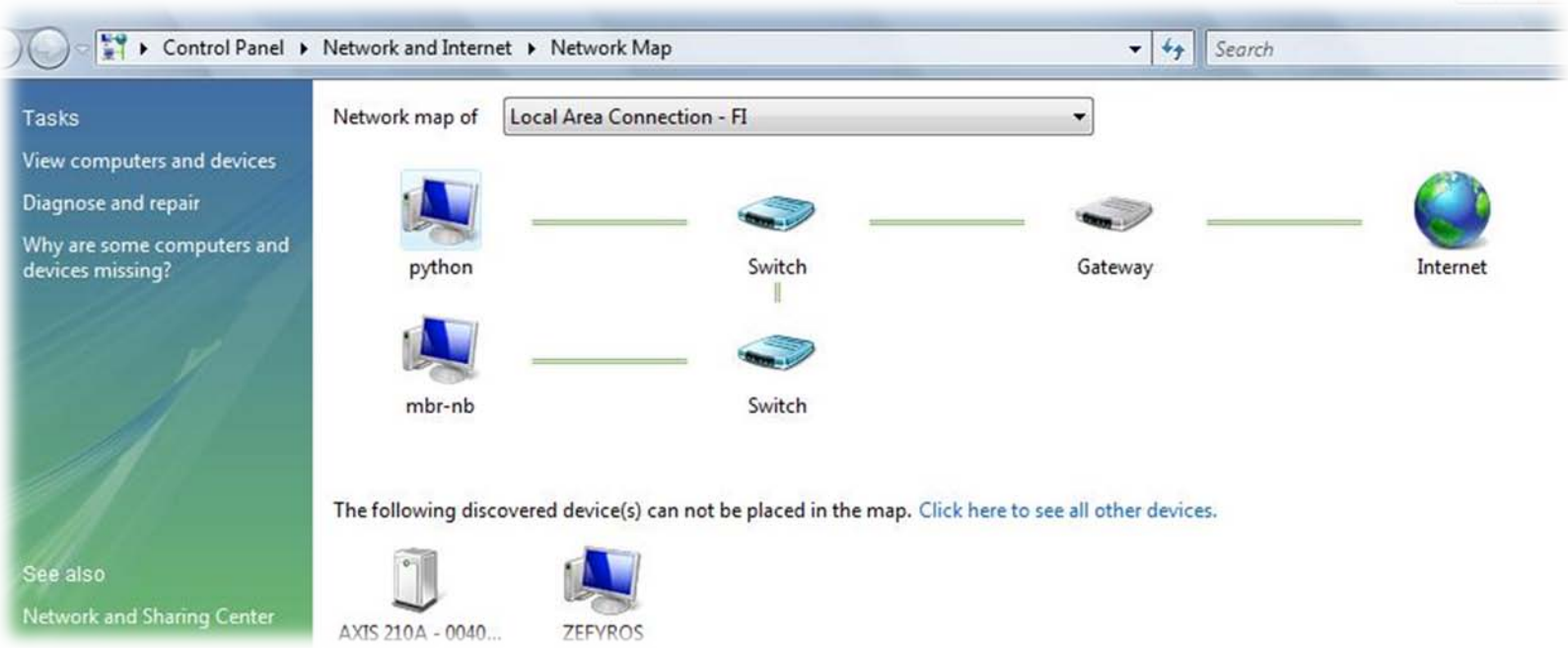
- Network Explorer místo My Network Places
- Network Discovery místo NetBIOS broadcastu – pro malé sítě a domácí použití (př. Media Center ve Vista najde Media Center na Xbox 360)
- Function Discovery Provider Host, Web Services Dynamic Discovery(WS-Discovery), Universal Plug and Play(UPnP)/Simple Service Discovery Protocol(SSDP) – vyjímky na FW
- Multicast protokol pro najití cílových zařízení (sdílená složka, tiskárna...) cílový počítač odpoví na zprávu - WS-Discovery

Jak publikuje síťové zdroje

- Starší systémy NetBIOS oznámení
- WS-discovery, Win7 používá Function Discovery Resource Publication (FDRP) službu
- Client objevuje prostředky, server oznamuje:
  - HELLO pro každý zdroj při spuštění služby, při registraci nového zdroje (obsahuje jméno, popis, doména či pr. skupina, sdílení s read, administrativní nejsou oznámeny)
  - Řeší požadavky podle jména
  - BYE pro každý zdroj při ukončení

Network Map

- Link Layer Topology Discovery (LLTD) služba
- LLTD ve fyzické vrstvě – nemusí být zařízení přidělená IP
- Konfigurace v Group Policy – Computer Configuration\Administrative Templates\Network\Link Layer Topology



Network Connections

- Network Clients
  - Umožňují připojení počítače s určitou sítí operačního systému
- Network Services
  - Poskytují další vlastnosti síťovým spojením
- Network Protocols
  - PC může komunikovat skrze NC pouze za použití protokolů

Network Connections

- Advanced settings
- Bridging
- Zobrazení adresy a konfigurace

Konfigurace TCP/IP

- Co je IP adresa?
  - 192.168.1.102 = 1100000 10101000 00000001 01100110
  - 2 části: NetworkID, HostID
  - Maska podsítě
    - Definuje, kde začíná HostID

Class	Network ID	Range of First Octet	Number of Available Network Segments	Number of Available Hosts	Subnet Mask
A	w.0.0.0	1–126	126	16,777,214	255.0.0.0
B	w.x.0.0	128–191	16,384	65,534	255.255.0.0
C	w.x.y.0	192–223	2,097,152	254	255.255.255.0
D	N/A	224–239	N/A	N/A	N/A
E	N/A	240–255	N/A	N/A	N/A

Co je IP adresa?

- CIDR (Classless Interdomain Routing)
  - Pro zvýšení efektivity, rozdělení na menší podsítě, vytvoření vlastní masky podstítě

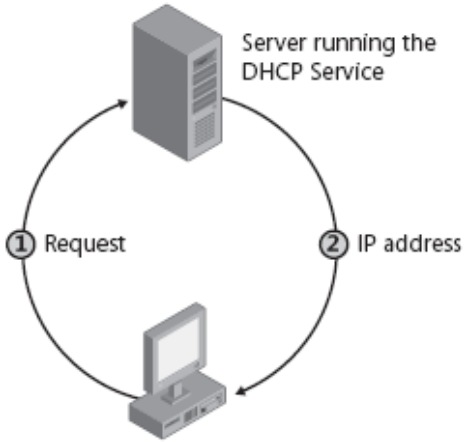
Binary Value	Decimal Value
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254

Co je IP adresa?

- Reálný svět – směrovače pracují s maskou podsítě
- Private Addressing
  - Každé síťové rozhraní, které je zapojené přímo v Internetu musí být registrované u Internet Assigned Numbers Authority (IANA)
  - Každá třída má privátní adresy
    - Class A: 10.0.0.0 do 10.255.255.255
    - Class B: 172.16.0.0 do 172.31.255.255
    - Class C: 192.168.0.0 do 192.168.255.255

Konfigurace statické IP adresy

- Implicitně nastavené na autokonfiguraci – využívá DHCP server
- Většina počítačů přes DHCP
  - Vybraná nastavení:
    - Ip address
    - Default Gateway
    - DNS server
    - Boot server
  - Po startu vyšle DHCPDiscover broadcast
  - DHCP pošle DHCPOffer broadcast (IP, configurace)
  - Klient pošle DHCPRequest vybranému DHCP serveru
  - DHCP pošle DHCPPACK oznámení, že IP adresa byla přidělena na nějakou dobu
- Za půl doby chce obnovit (4 dny)



Automatic Private IP Addressing

- APIPA – konf. jednoduché LAN sítě
- Jediná podsíť, bez připojení do jiné
- 169.254.x.y
- Defaultně povoleno
- Pro domácí použití
- Nastaví se pouze IP a maska!
- Proces APIPA
  - Pokus o najití DHCP, zvolí náhodnou IP, broadcast na tuto IP, nastavení IP
  - ∃ lease TTL > 0, pokus o obnovení, pokus o kontaktování výchozí brány

Manuální konfigurace

- Network and sharing center – Manage network connections (ve Windows 7 change adapter settings) – Properties (ncpa.cpl)
- GPO: User Configuration\Administative Templates\Network\Network Connections
- Netsh interface ipv4 set address „Local Area Connection“ dhcp
- Netsh interface ipv4 set dnsserver „Local Area Connection“ dhcp
- Netsh interface ipv4 set address „Local Area Connection“ source=static address=192.168.1.10 mask=255.255.255.0 gateway=192.168.1.1
- Netsh interface ipv4 set dnsserver „Local Area Connection“ source=static address=192.168.1.2 register=primary
- Netsh interface ipv6 set address „Local Area Connection“ address=2001:db8:3fa8:102a::2 anycast

Alternativní konfigurace

- Zastíní proces APIPA
- Pro mobilní PC, aby fungovaly doma i v práci bez rekonfigurace
- Alternativa pro jedno místo, kde není DHCP
- Plnohodnotná konfigurace narozdíl od APIPA

Nástroje pro řešení problémů TCP/IP

- Ipconfig – zobrazí nastavení TCP/IP
  - /all, /release, /renew, /flushdns
- Ping – konektivita zevnitř ven
  - Ping Loopback, ip adresu, výchozí bránu, Internet ☺
- Tracert – zkusí projít cestu postupně
- Pathping – jako Tracert
  - zobrazí informace o ztrátě paketů na jednotlivých aktivních prvcích
- Arp – překlad IP <-> MAC adres
- NetStat – statistiky a spojení

Arp poisoning

```
C:\Users\Administrator>arp -a

Interface: 192.168.2.55 --- 0xa
  Internet Address      Physical Address      Type
  192.168.2.1           00-18-8b-a4-09-2e     dynamic
  192.168.2.50          00-19-db-4c-91-28     dynamic
  192.168.2.52          00-18-8b-a4-09-2e     dynamic
  192.168.2.53          00-18-8b-a4-09-2e     dynamic
  192.168.2.64          00-1d-60-9c-b5-35     dynamic
  192.168.2.200         00-04-5a-7d-b5-b0     dynamic
  192.168.2.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.1.24            01-00-5e-00-01-18     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

QoS

- Cena šířky pásma <<, stále problém zahlcení
- Umožní real-time provoz prioritizujíc důležitější aplikace (VoIP)
- Kustomizace šířky pásma pro skupiny uživatelů a počítačů
- Minimalizuje dopad velkých, ale neprioritních přenosů (např. záloha)
- Více o QoS
  - http://technet.microsoft.com/en-us/library/bb742475.aspx

Network Access Protection

- Redukuje riziko zapojení „nakažených“ počítačů do sítě
- Network Policy Validation
  - Stav počítače je zkontrolován
  - V monitorovacím stavu se zaznamená do logu
  - V isolovaném prostředí se zařadí do omezeného přístupu
- Health Requirement Policy Compliance
  - Administrátoři nastaví automatický update, nebo doinstalování SW
- Limited Acces for Non-compliant Computers
  - Počítače mají omezený přístup dokud se nevyléčí

Windows Firewall

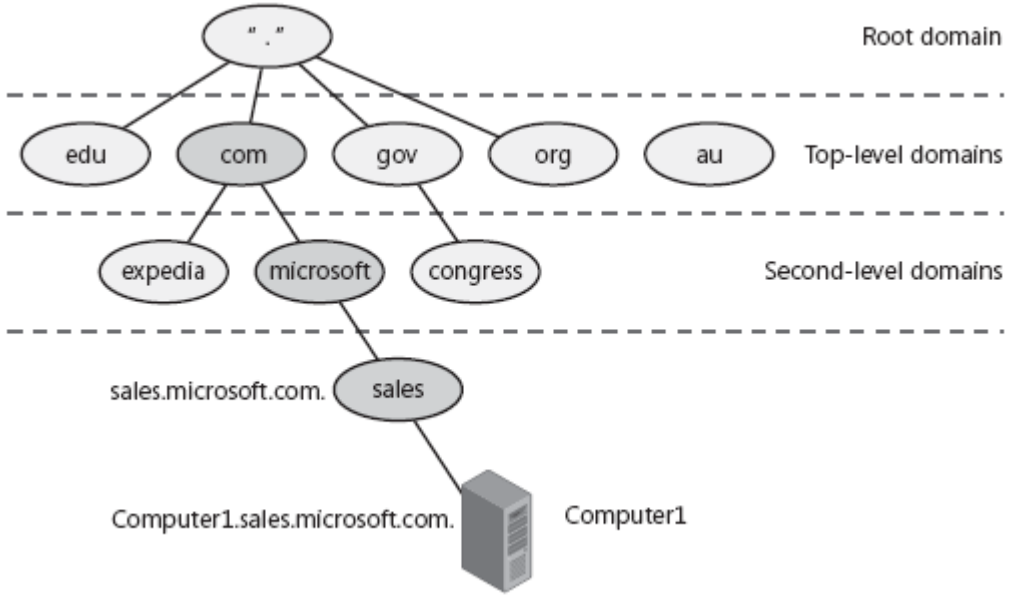
- Filtruje příchozí i odhozí provoz
- Všechny IANA IP protokoly
- Typy pravidel kombinace nebo permutace protokolu, portu (jen TCP a UDP) ICMPv4/6, IP adresy, typ síť. rozhraní, program, služba, Ipsec metadata
- Akce: Allow, Block, Bypass
- GPO snap in
- Remote management, mmc, netsh a API
- Integrace s IPsec, Network Access Protection
- FW profily
- Plná podpora ipv6

FW profily

- Domain
  - Když se počítač ověří vůči DC
- Private
  - Network type je Private
  - PC, které není v doméně po prvním přihlášení dána možnost sítě – Home, Work, Public
  - Home a Work = Private
  - Většinou méně přísné, očekává se domácí, či SOHO síť, používání NAT. Povolena pravidla pro network discovery
- Public
  - Jindy

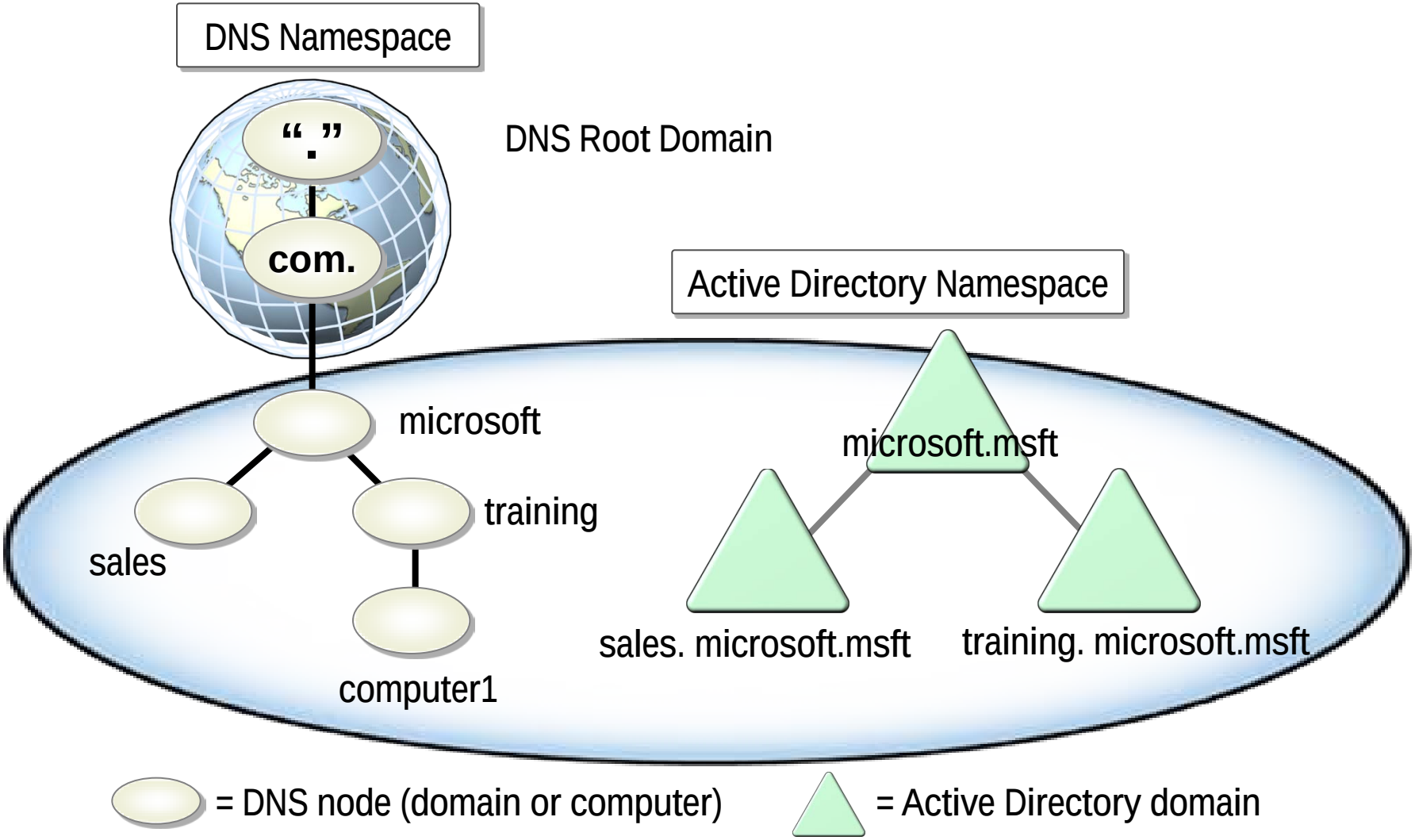
Domain Name System (DNS)

- V sítích Windows server jako hlavní prostředek k nalezení zdrojů v Active Directory
- Domain Namespace
  - Jmenné schéma s hierarchickou strukturou pro databázi DNS
  - Indexováno podle jména
  - Hostname – nejlevější část FQDN



Active Directory a DNS

- Úzce provázané
- Sdílí společný jmenný prostor
- DNS lokalizuje služby využívané Active Directory
- Active Directory distribuuje služby prostřednictvím DNS SRV záznamů
- Klient pak najde službu jednoduchým DNS dotazem

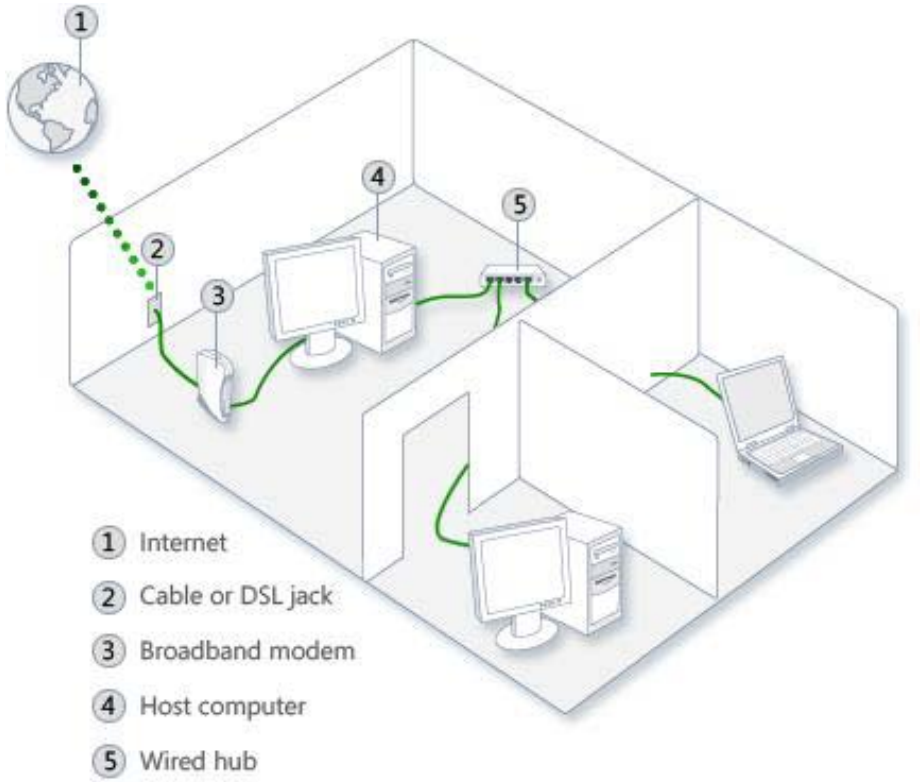

DNS Namespace
“.”
com.
DNS Root Domain
Active Directory Namespace
microsoft
training
sales
computer1
microsoft.msft
sales. microsoft.msft
training. microsoft.msft
= DNS node (domain or computer)
= Active Directory domain

DNS klient

- Funkční TCP/IP, DNS služba dostupná
  - Bez DNS pro překlad jmen a IP adres lze použít tzv. Host File
- Možnost zadat více DNS serverů v pořadí
- Možnost ovlivnit sufixy ne-FQDN dotazů
  - Defaultně se používají sufixy z DNS doménového jména
  - Pokud je dostupný DHCP a nejsou nakonfigurované sufixy přímo, použijí se z DHCP
- Nástroj NetSh – konfigurace sítě

Internet Connection Sharing

- Sdílení připojení mezi více PC – router nebo ICS:
  - Host Computer
    - Share (tab) ve vlastnostech Network Connection
    - Musí mít více síťových rozhraní
    - Slouží jako DNS a DHCP



Další vybraná síťová vylepšení

- DirectAccess
- BranchCache
- VPN Reconnect
- Mobile Broadband device support
- URL Based QoS
- DNS Security Extensions
- Support for Green Computing

DirectAccess – požadavky

- Alespoň jeden DirectAccess server s Windows Server 2008 R2, s 2 síť. rozhraními
- Klient s Windows 7
- DC a DNS s Windows server 2008 SP2 či novější
- PKI
- Ipsec politiky
- IPv6

DirectAccess – postup připojení

- Windows 7 detekuje síť
- Pokus o připojení na intranet web site
- Připojení k serveru pomocí IPv6 a Ipsec (IPv6-over-IPv4 tunel pomocí 6to4 or Teredo)
- V případě FW či proxy, zkusí https (SSL)
- Autentizace certifikáty
- Autorizace k přístupu přes členství ve skupině v AD
- Pokud je NAP – dojde k procesu léčby před připojením DirectAccess
- DirectAccess server začne přeposílat intranetová data

Pozvánka

- PV175 – Správa MS Windows I
  - podzim
  - pracovní stanice
- PV176 – Správa MS Windows II
  - jaro
  - AD