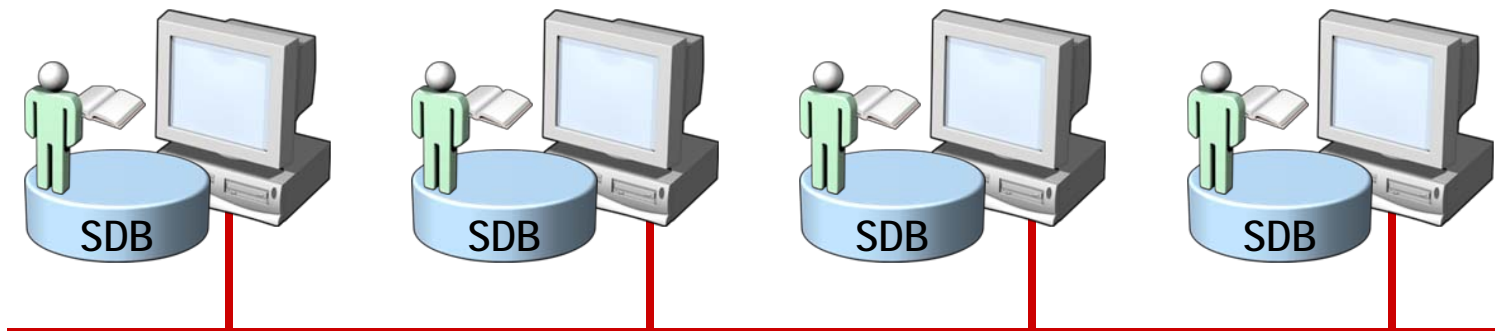


Sítování ve Windows



Workgroup

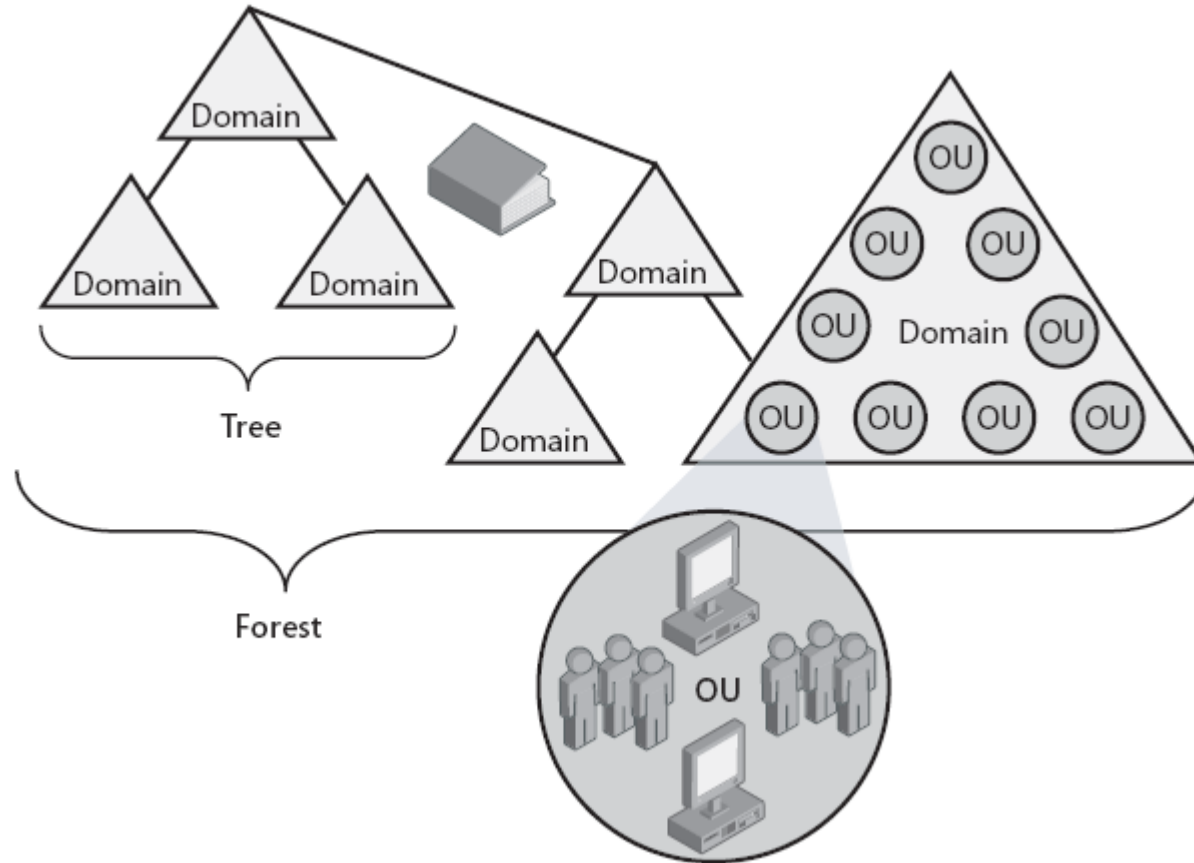
- Workgroup
 - Logické uskupení počítačů v síti, všichni jsou si rovni (peer-to-peer)
 - Všichni počítače si udržují pouze svůj ACL
 - Změna nutná všude
 - Decentralizovaná správa!
 - Nepotřebuje server
 - Jednoduché na provedení
 - Pro síť <10 počítačů



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

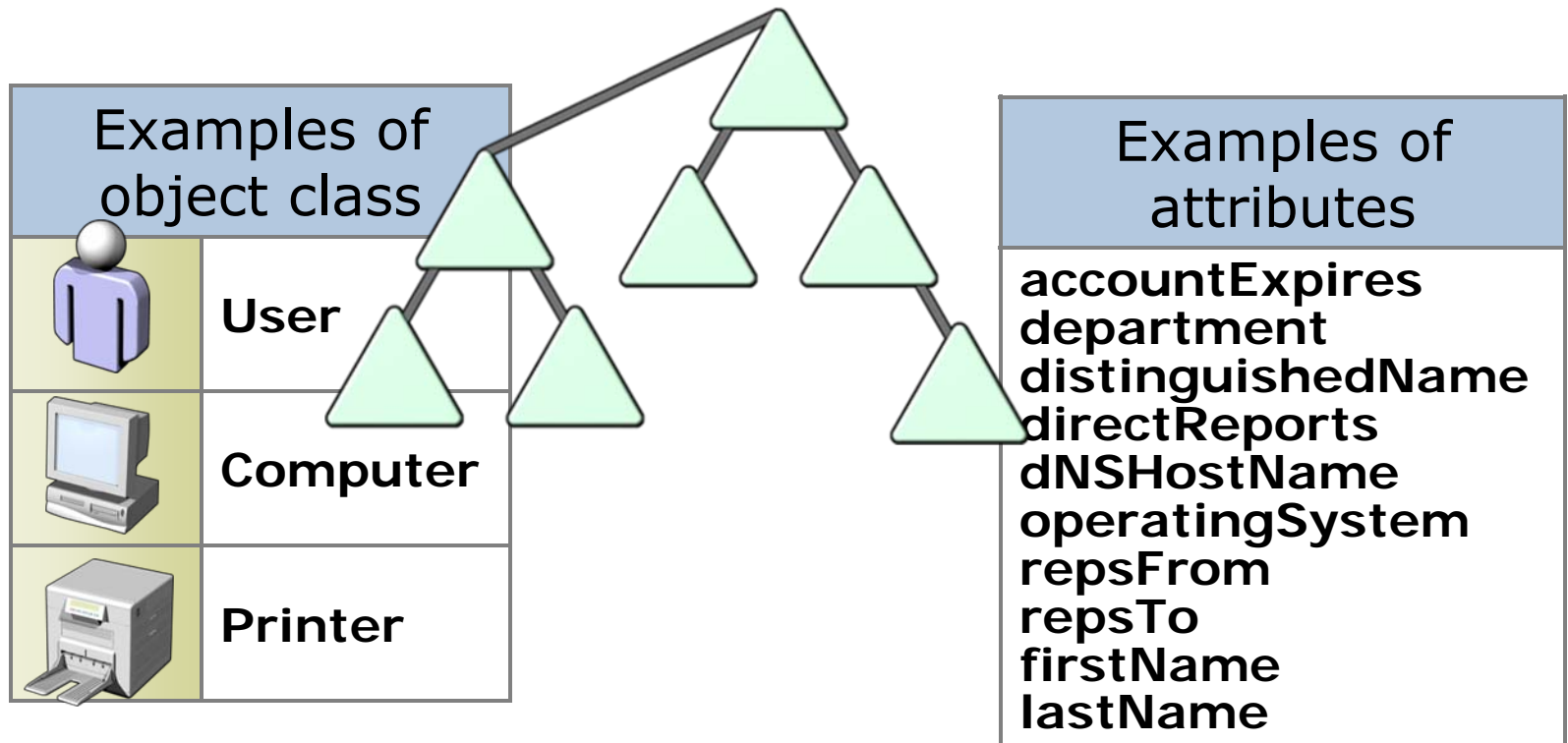


Logická struktura AD

- 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 Directory Schema

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



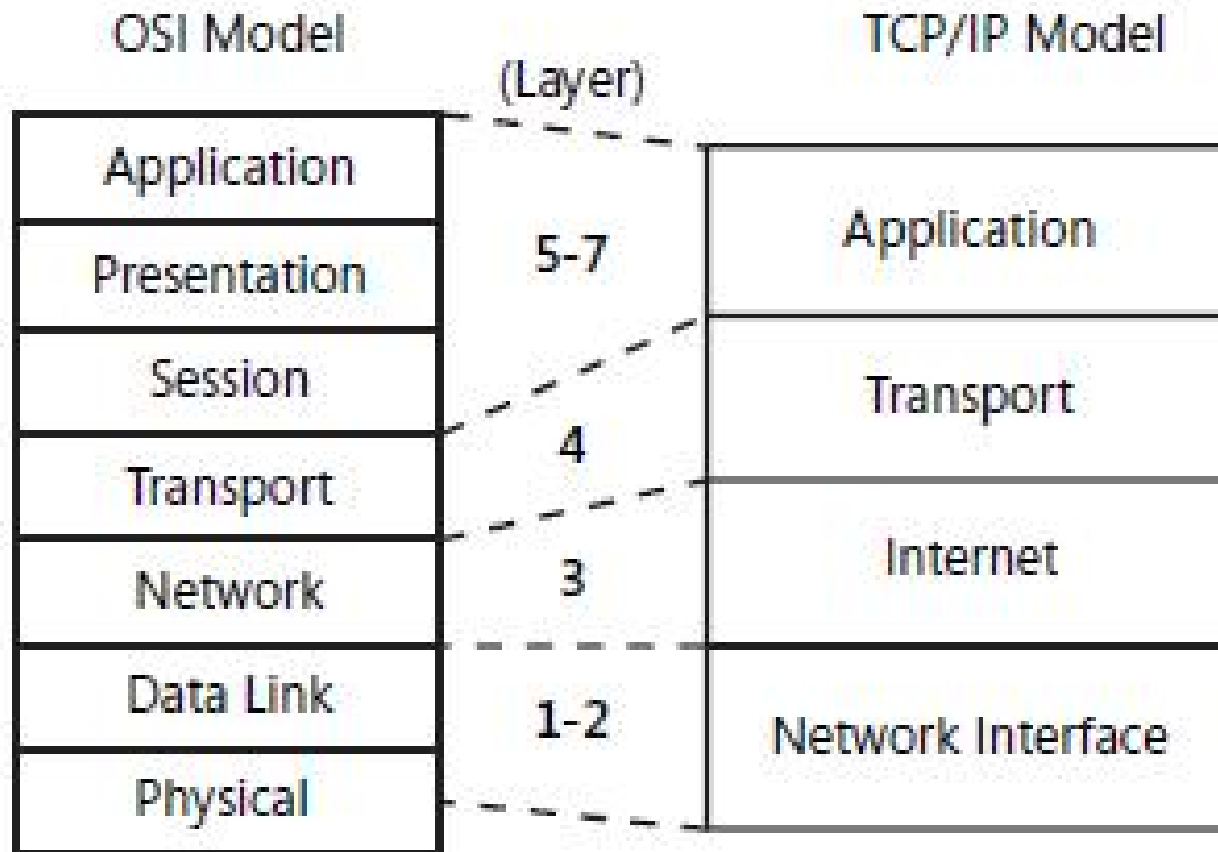
Fyzická struktura AD

- 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

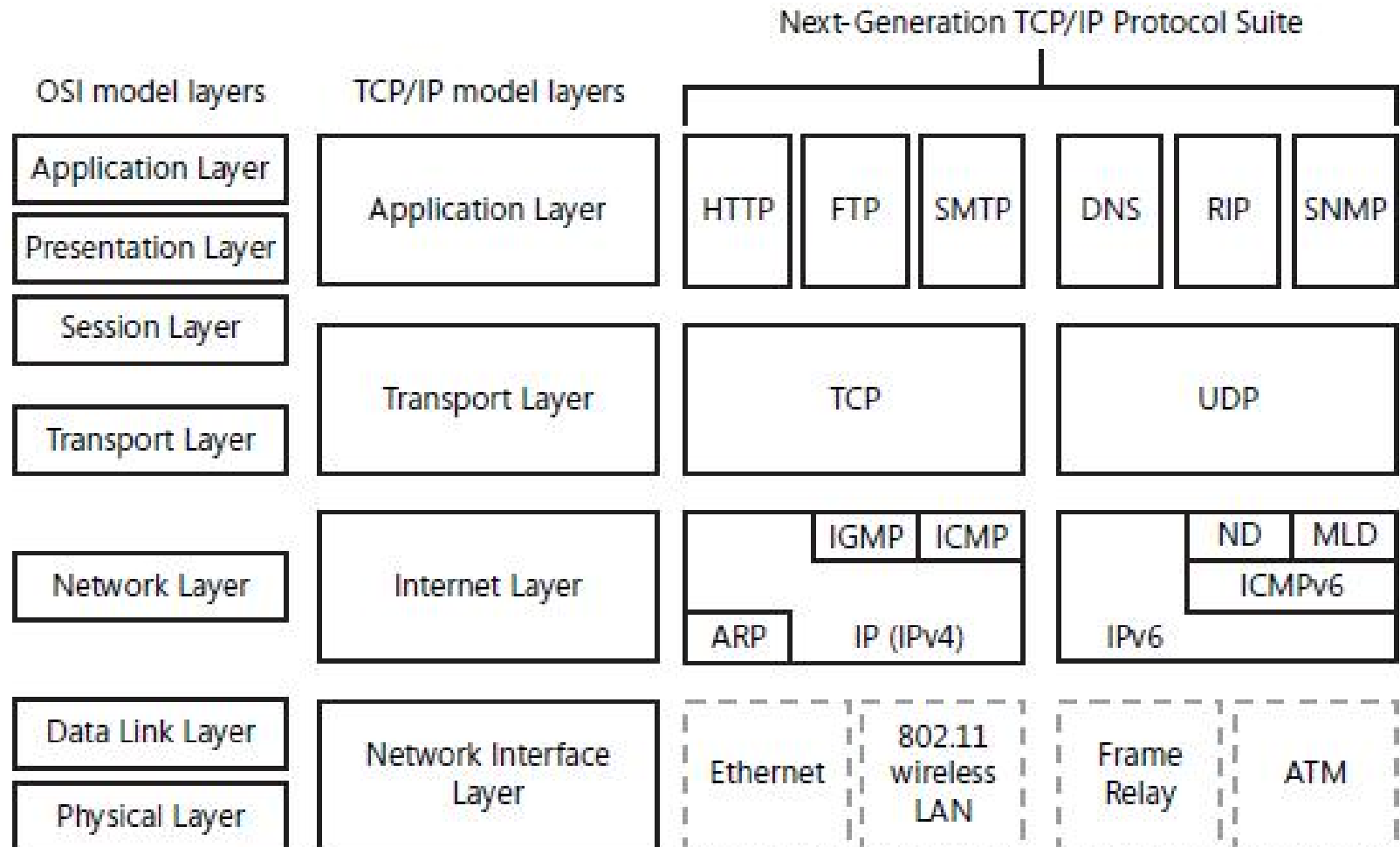
TCP/IP protokol ve Windows

- 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



4 vrstvý síťový model

- Fyzická vrstva – MAC, huby, switche
- Síťová vrstva
 - Směrování, datagramy
 - IP – adresování a směrování paketů
 - ARP – IP <-> MAC požadováno pro síťová broadcastová spojení se sdíleným přístupem (Ethernet)
 - ICMP – stavové a chybové informace
 - IGMP – (I. Group Management P.) zajišťuje multicast, informuje sousední multicastové směrovače o multicastových členech v konkrétní síti

4 vrstvý model

- Transportní vrstva
 - Poskytuje komunikační spoj mezi zařízeními
 - Požadovaná metoda doručení určuje protokol
 - TCP – spojované, spolehlivé, ACK
 - UDP – opak TCP (malé objemy, nebo jiný druh dat)
- Aplikační vrstva
 - Práce s uživatelskými daty
 - Mnoho TCP/IP standardních nástrojů a služeb (FTP, Telnet, DNS, SNMP, POP3 ...)
 - WINS – Windows Internet Name Service překládá NetBIOS jména na IP adresy, hodně používané v NT verzích
 - NAT – mnoho zařízení v privátní síti má přístup do Internetu přes jednu veřejnou IP adresu

Konfigurace TCP/IP

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

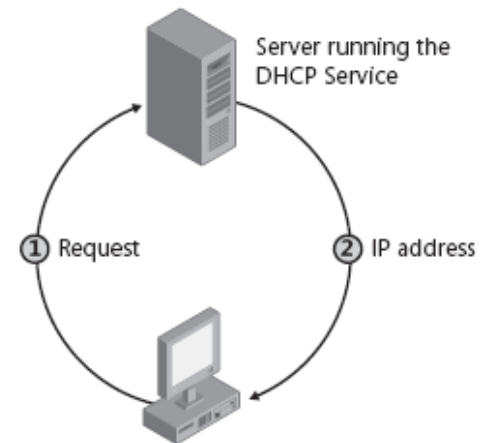
Binary Value	Decimal Value
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254

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 DHCPDiscoverbroadcast
 - DHCP pošle DHCPOffer broadcast (IP, konfigurace)
 - Klient pošle DHCPRequest vybranému DHCP serveru
 - DHCP pošle DHCPACK 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 najítí DHCP, zvolí náhodnou IP, broadcast na tuto IP, nastavení IP
 - \exists lease TTL > 0, pokus o obnovení, pokus o kontaktování výchozí brány

Manuální konfigurace

- Network and sharing center – Manage network connections – Properties
- GPO: User Configuration\Administrative Templates\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

- Ping – konektivita zevnitř ven
 - Ping Loopback, ip adresu, výchozí bránu, Internet 😊
- Ipconfig – zobrazí nastavení TCP/IP
 - /all, /release, /renew, /flushdns
- Net view – vzdálené sdílené prostředky
- Tracert – zkusí projít cestu postupně
- Pathping – zobrazí informace o ztrátě paketů na jednotlivých aktivních prvcích
- NetStat – statistiky a spojení

Jak Vista hledá síťové zdroje

- 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) – výjimky na FW
- Multicast protokol pro najetí cílových zařízení (sdílená složka, tiskárna...) cílový počítač odpoví na zprávu - WS-Discovery

Jak publikuje síťové zdroje

- Starší systémy NetBIOS oznámení
- WS-discovery, Vista 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)
- LLTD ve fyzické vrstvě – nemusí být zařízení přidělená IP
- Konfigurace v Group Policy – Computer Configuration\Administrative Templates\Network\Link Layer Topology

The screenshot displays the Windows Network Map interface. The breadcrumb path is Control Panel > Network and Internet > Network Map. The network map is titled "Network map of Local Area Connection - FI". The diagram shows a topology where two computers, "python" and "mbr-nb", are connected to a central "Switch". This switch is connected to another "Switch", which is connected to a "Gateway", which is finally connected to the "Internet".

Tasks

- View computers and devices
- Diagnose and repair
- Why are some computers and devices missing?

See also

Network and Sharing Center

The following discovered device(s) can not be placed in the map. [Click here to see all other devices.](#)

- AXIS 210A - 0040...
- ZEFYROS

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 izolovaném prostředí se zařadí do omezeného přístupu
- Health Requirement Policy Compliance
 - Administrátoři nastaví automatický update, nebo doinstalování SW, např. přes SMS
- Limited Acces for Non-compliant Computers
 - Počítače mají omezený přístup dokud se nevyléčí

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

Windows Firewall

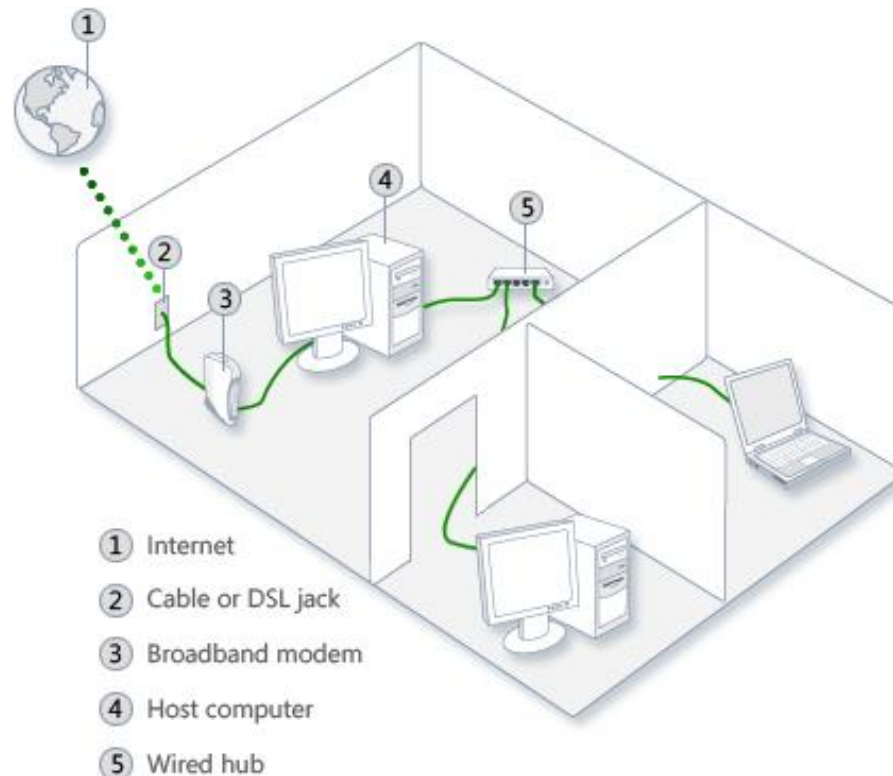
- Filtruje příchozí i odchozí provoz
- Všechny IANA IP protokoly
- Typy pravidel kombinace nebo permutace protokolu, portu (jen TCP a UDP) ICMPv4/6, IP adresy, typ síť. rozhraní, program, služba, Isec metadata
- Akce: Allow, Block, Bypass
- GPO snap in
- Remote management, mmc, netsh a API
- Integrace s Isec, 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

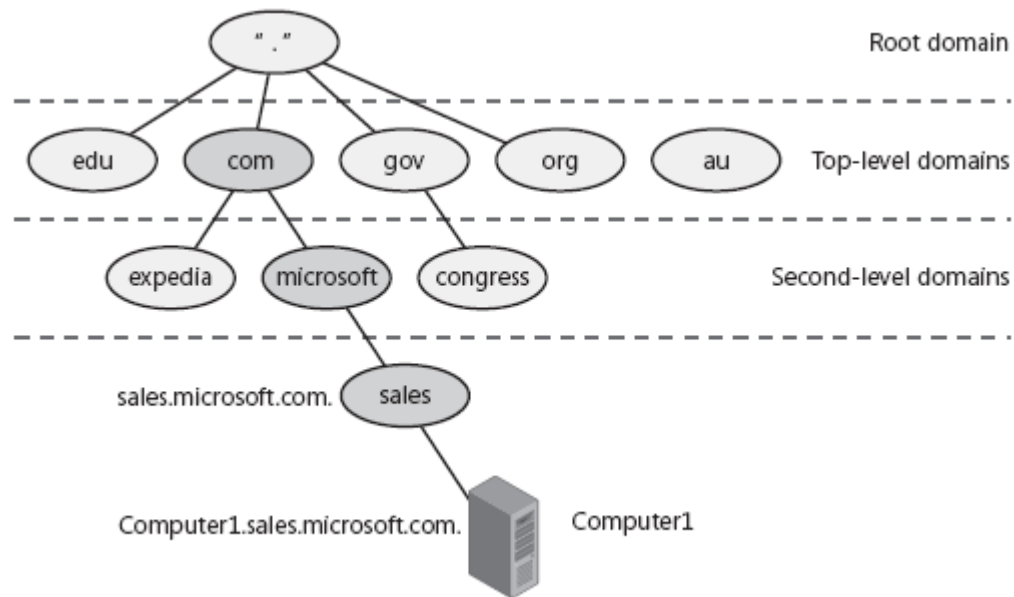
Internet Connection Sharing

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



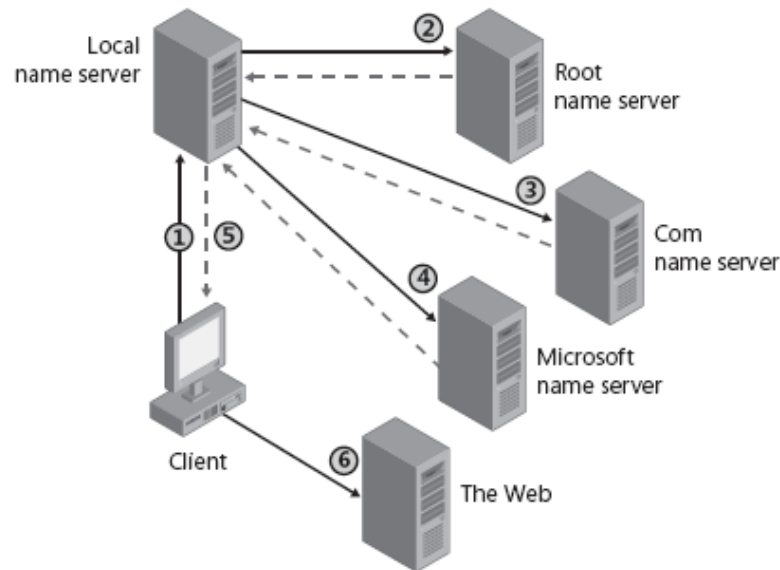
Domain Name System (DNS)

- 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



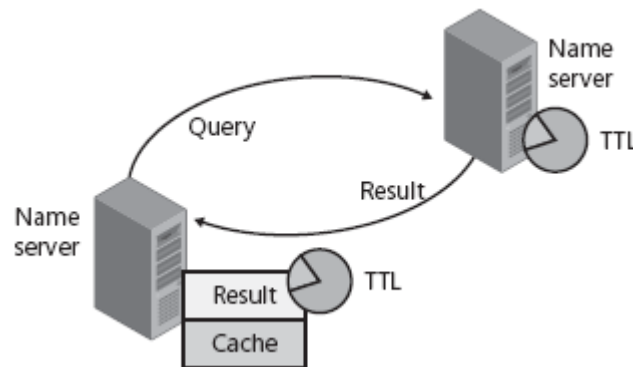
Překlad jmen

- Dopředný dotaz – A záznamy
 - Překlad jmen na IP
 - Name server pouze ve své zóně



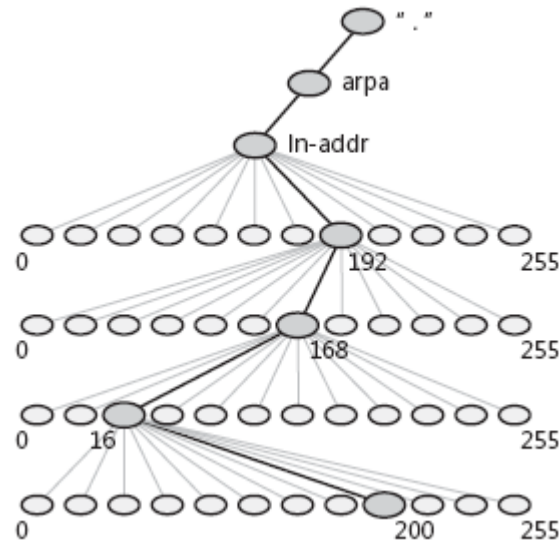
Překlad jmen

- Name server caching
 - Každý name server má dočasnou lokální cach zodpovězených dotazů
 - TTL výhody / nevýhody, hledání optima



Překlad jmen

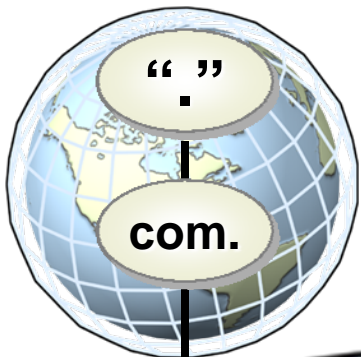
- Zpětný dotaz – PTR záznamy
 - Mapuje IP adresu na jméno
 - Jak nalézt v doménách indexovaných podle jména IP adresu?
 - In-addr.arpa



Active Directory a DNS

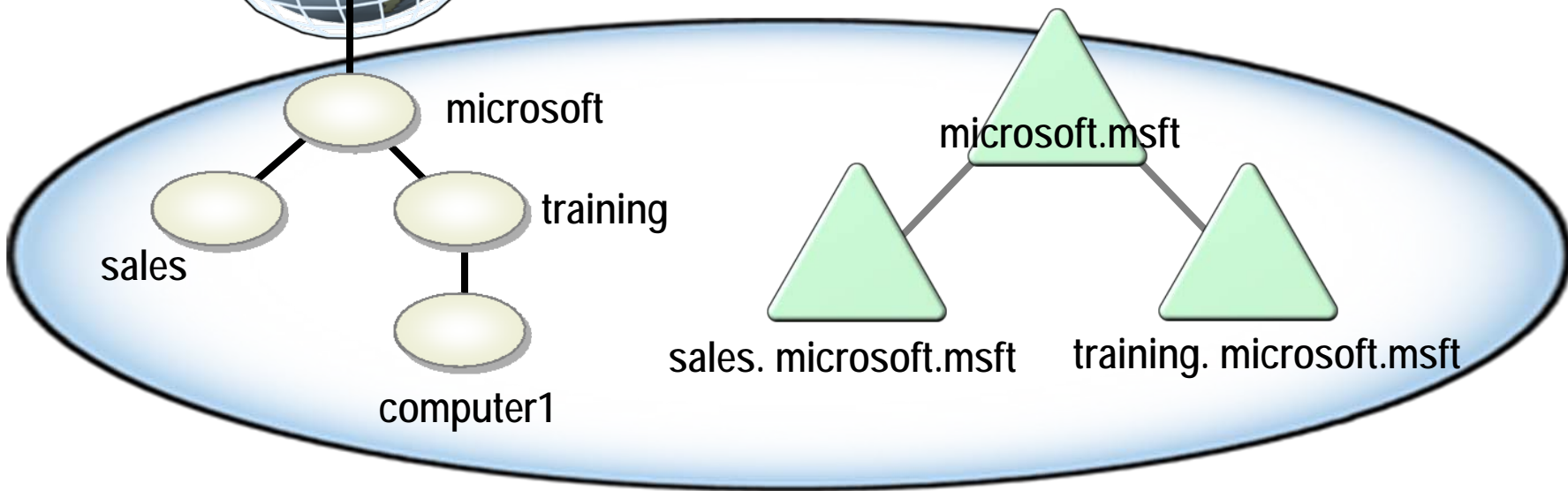
- Úzce provázané
- Sdílí společný jmenný prostor
- DNS lokalizuje služby využívané Active Directory
- Active Directory distribuuje služby prostřednictvím DNS SRV záznamů
- Klient pak najde službu jednoduchým DNS dotazem


DNS Namespace



DNS Root Domain

Active Directory Namespace



 = 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

Core networking improvements

- Vylepšení výkonu, bezpečnosti, ovladatelnosti
- Regulace latence (RTT)
- High bandwidth connection
- TCP Receive Window Scaling
 - Bez TCPRWS max velikost okna 64KB (Windows XP)
 - Okno vyjednáno v rámci ustanovení spojení
 - Vista používá scale factor 8 (max okno tedy 16MB)
- NewReno modifikace pro fast recovery RFC 2582
- Rozšíření pro Selective Acknowledgement (SACK) RFC 2883 (akceptuje duplikátní pakety)
- Explicit Congestion Notification (ECN) to IP RFC 3168
 - Netsh interface tcp set global ecncapability=enabled
- RFC 3517 A Conservative Selective Acknowledgment (SACK)
- RFC 4138 Forward RTO-Recovery
- ...

Další vylepšení

- Vylepšení spolehlivosti
 - Neighbour Unreachability Detection IPv4
 - Changes in Dead Gateway Detection
- Podpora IPv6
 - Defaultně Dual IP layer (IPv4 & IPv6)
 - GUI konfigurace
 - IPsec support
 - IPv6 over Point-to-Point Protocol
 - DHCPv6
- 802.1X Networking Authentication
- Strong Host Model
 - Netsh interface ipv4 set interface "Local Area Connection" WeakHostSend=enabled, receive analogicky
- ...