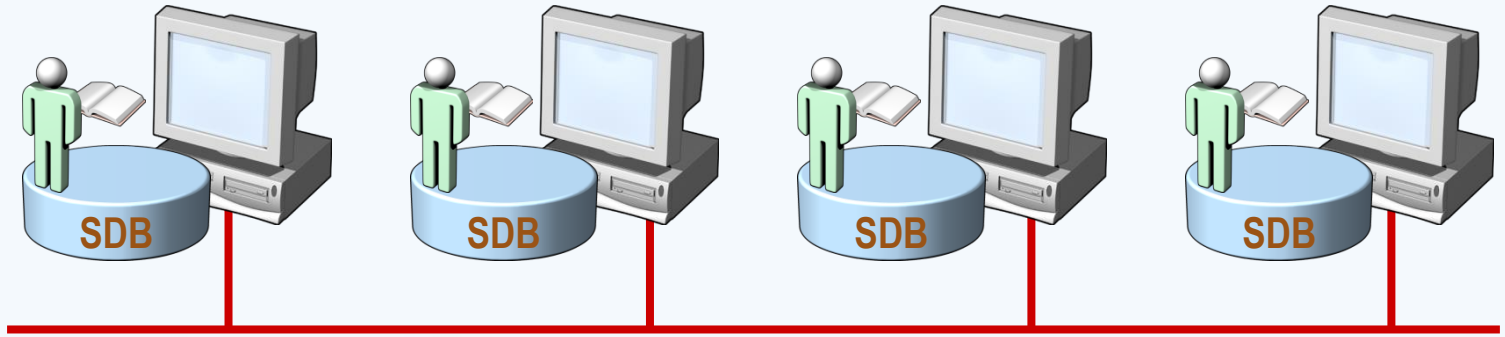
Síťování ve Windows

RNDr. Šimon Suchomel

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

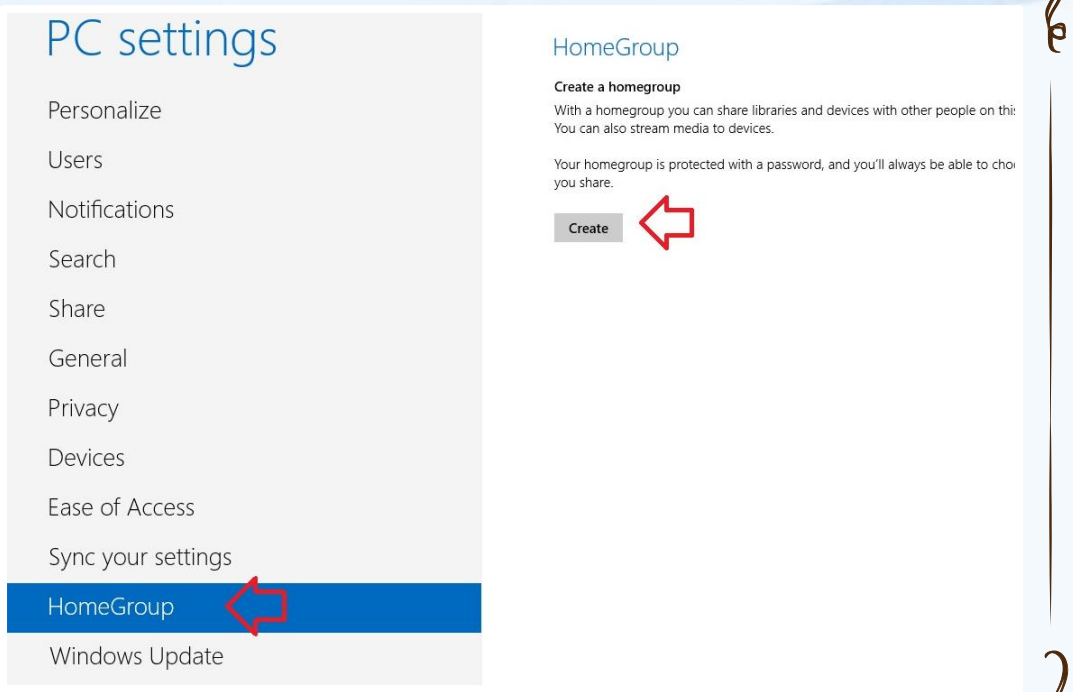


Převzato z MS MOC 2279

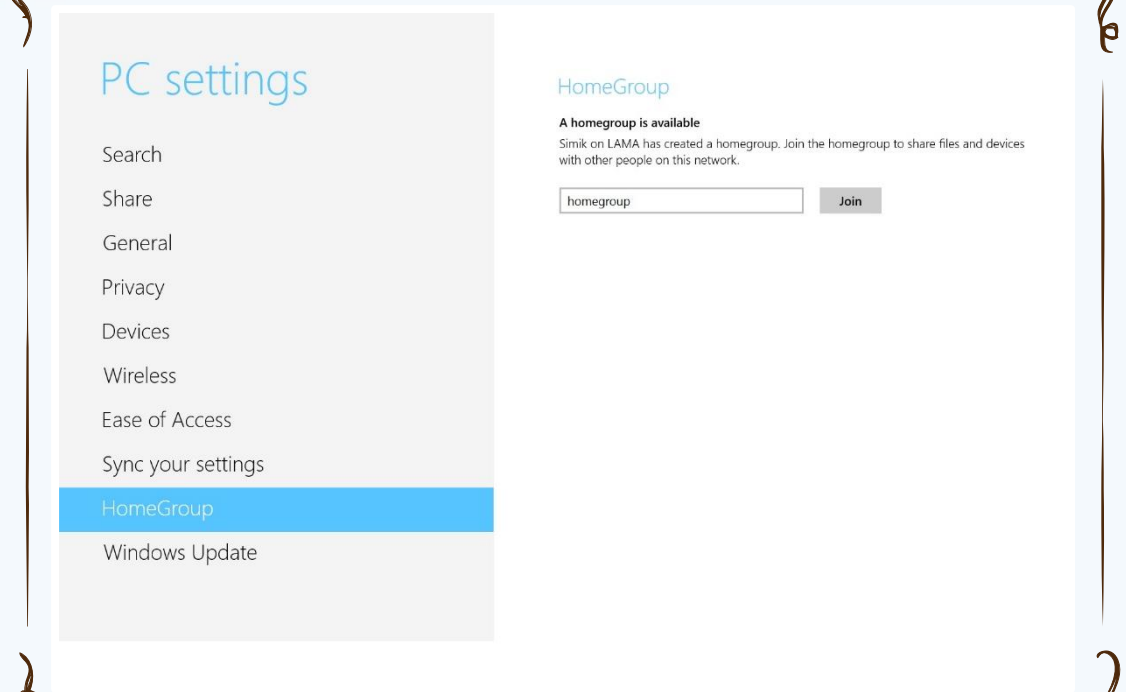
Homegroup

- Spojení 2 nebo více počítačů (obvykle v domácím prostředí), které jsou automaticky nastaveny ke sdílení: souborů (hudby, obrázků, videí, dokumentů), tiskáren a streamování médií
- Všechny počítače musí být ve stejné podsíti
- Chráněno heslem, stačí ho zadat pouze jednou
- Pro správu PC na pracovišti však nepoužitelné (neumožňuje centrální správu, podrobné nastavení oprávnění)

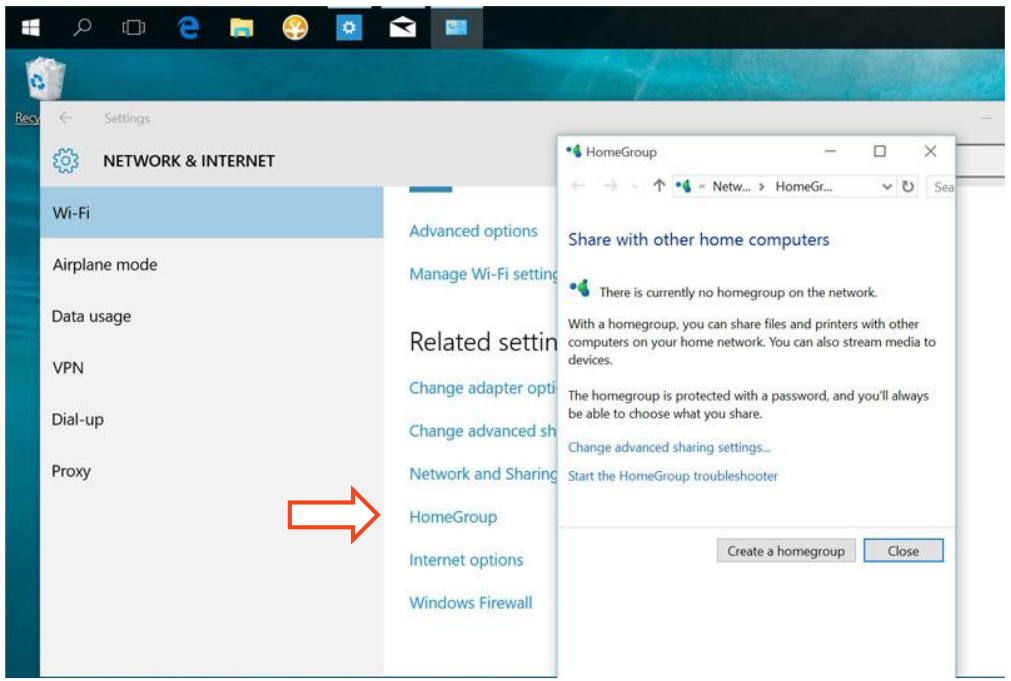
Převzato z windowshelp.microsoft.com



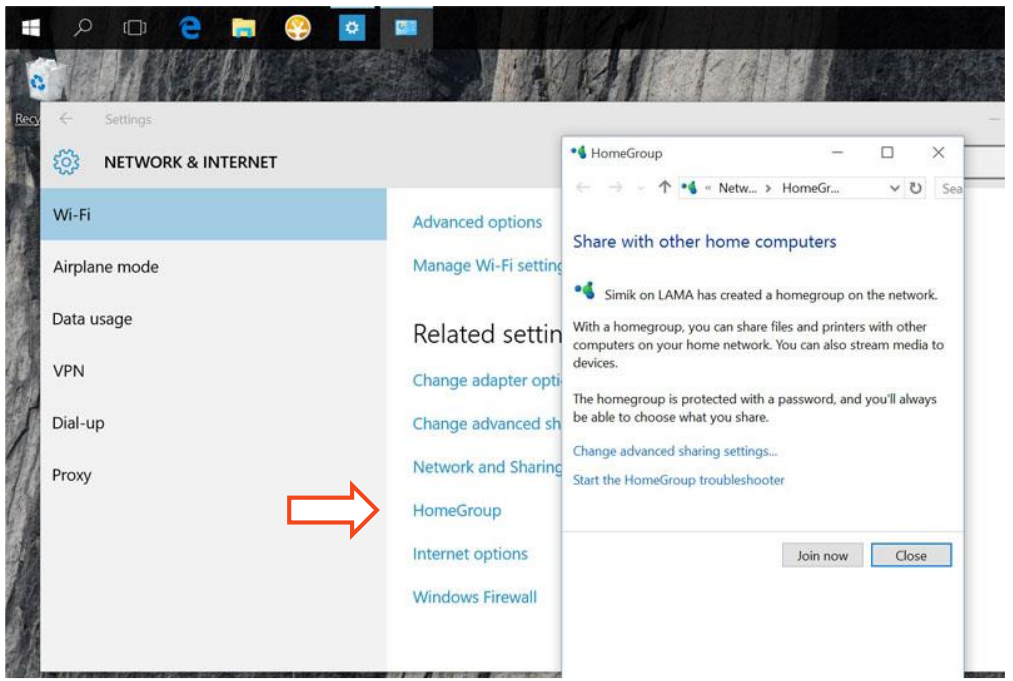
Vytvoření Homegroup



Připojení do Homegroup

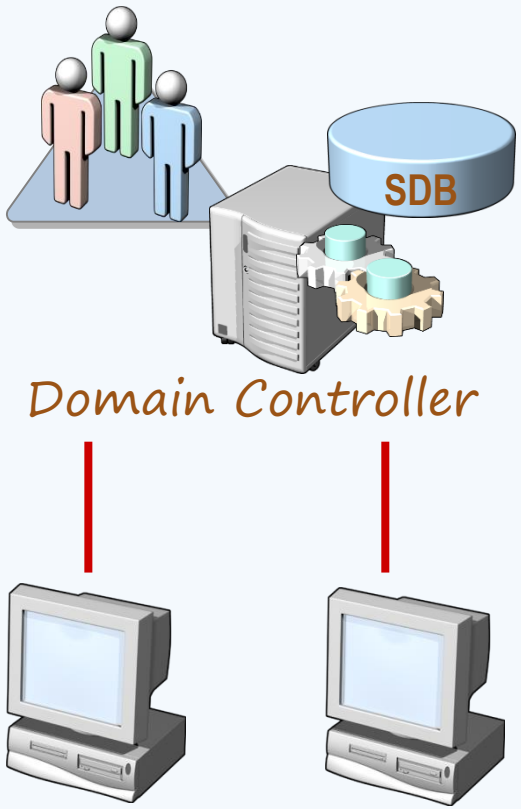


Vytvoření Homegroup



Připojení do Homegroup

Doména Active Directory

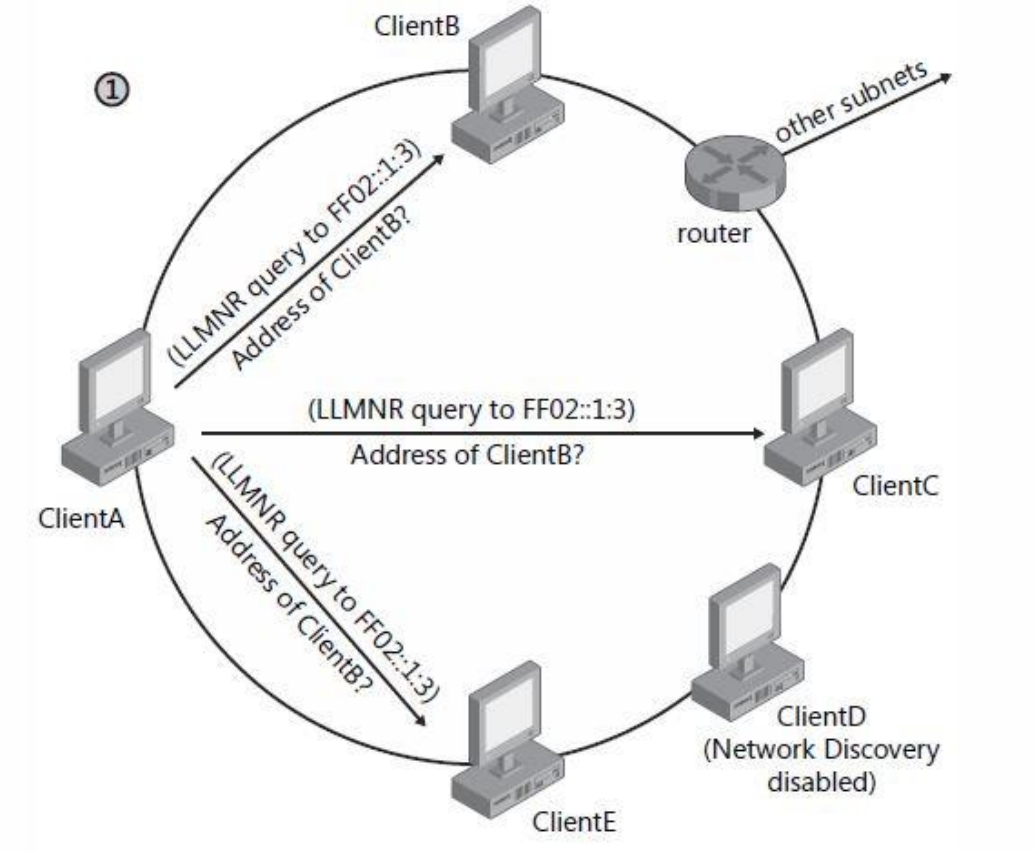


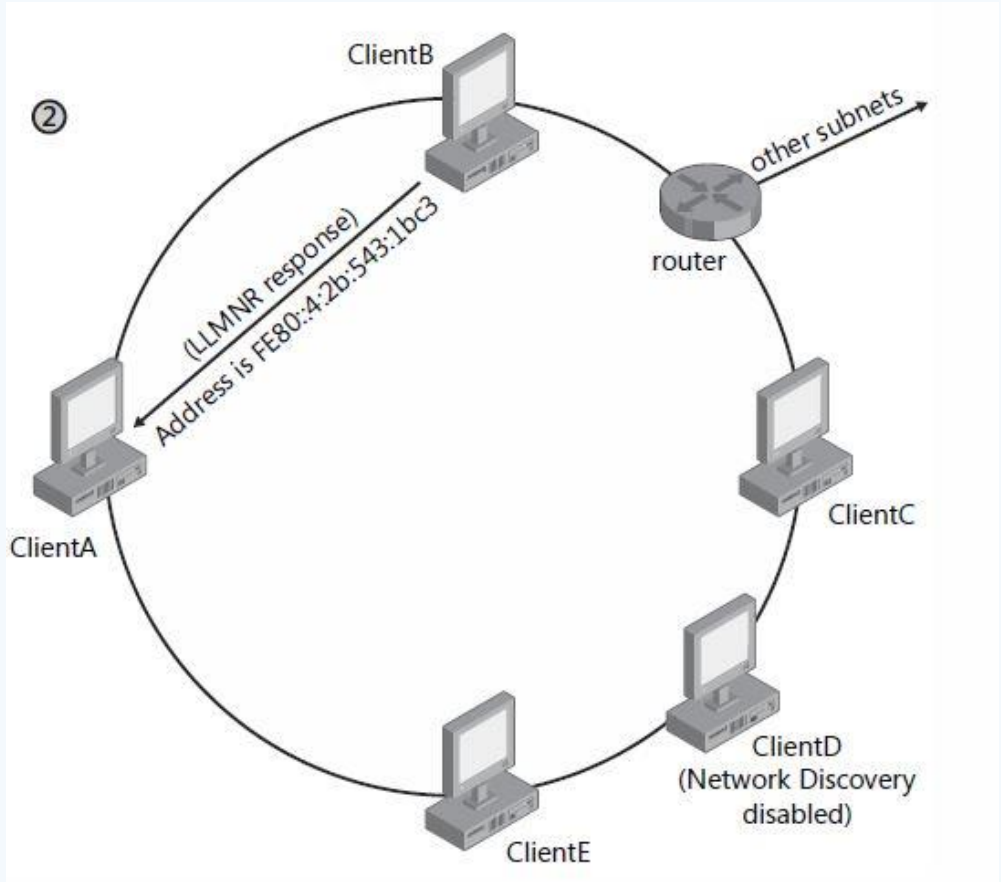
- Centralizovaná správa
- Objekty bezpečně uloženy v jedné logické struktuře
- Optimalizuje síťový provoz
- Rozšiřitelnost
- Uživatel se přihlásí jedním účtem a má přístup ke všem prostředkům, na které má oprávnění v celé struktuře
- Oddělení logické struktury (domény, OU, objekty) od fyzické struktury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

Jak Windows hledá síťové zdroje

- Network Discovery – pro malé sítě a domácí použití (př. Media Center ve W7 najde Media Center na Xbox 360)
- Překlad jmen pomocí Link Local Multicast Name Resolution (LLMNR)
- The Link Layer Topology Discovery (LLTD) Mapper
  - Multicast protokol pro najití cílových zařízení (sdílená složka, tiskárna...) cílový počítač odpoví na zprávu – WS-Discovery

LLMNR





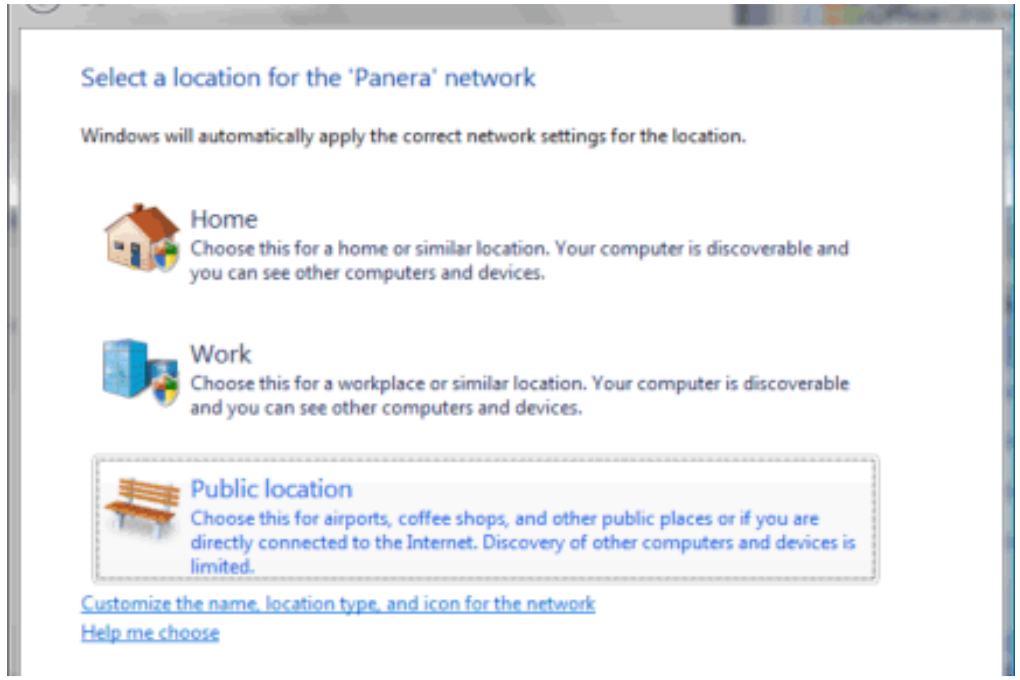
Převzato Training Kit (MCTS Exam70-642)

Jak Windows publikuje síťové zdroje

- LLTD Responder
- WS-discovery, Win7 používá Function Discovery Resource Publication (FDRP) službu
- Klient 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 Location Types

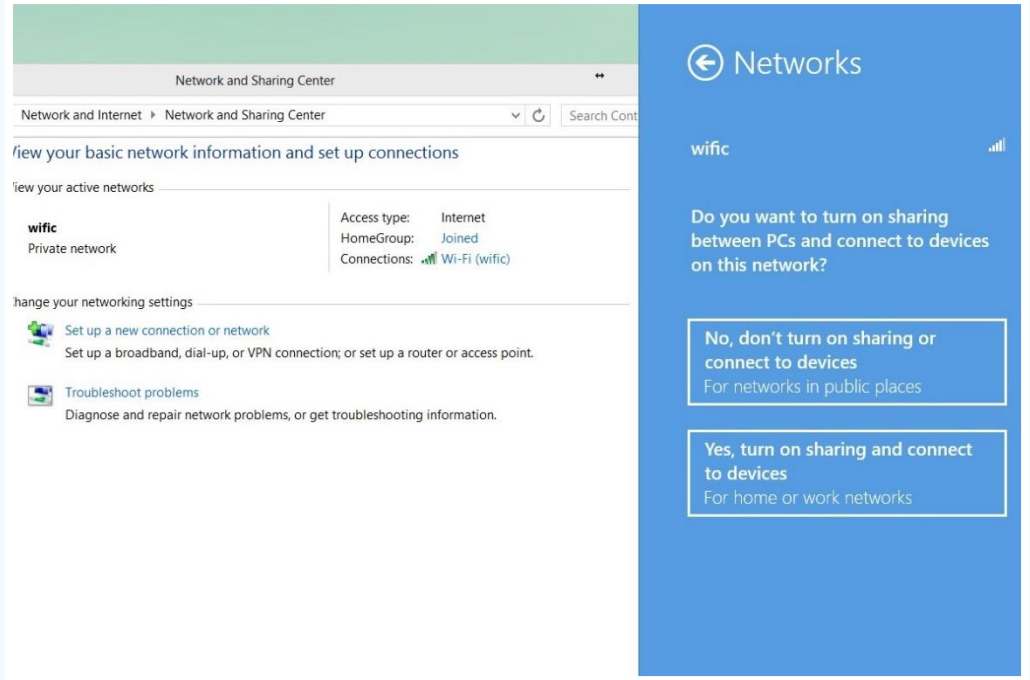
- Public
  - Network Discovery je zakázané, firewall blokuje všechna nevyžádaná příchozí spojení
- Private
  - Určeno pro domácí použití, kde chci sdílet prostředky, ale nemám k dispozici Active Directory DC
- Domain
  - Když se autentizuje k DC, Network Discovery a firewall zakázané, počítá se s využitím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



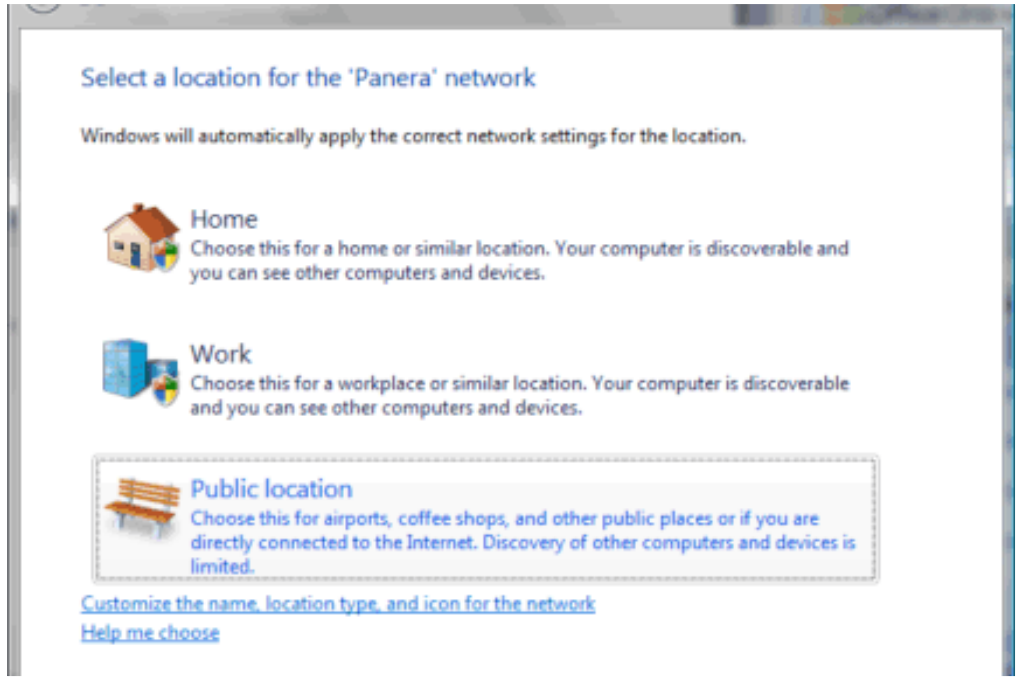
Windows 7 výběr umístění sítě

Home | Work = Private

Public location = Public



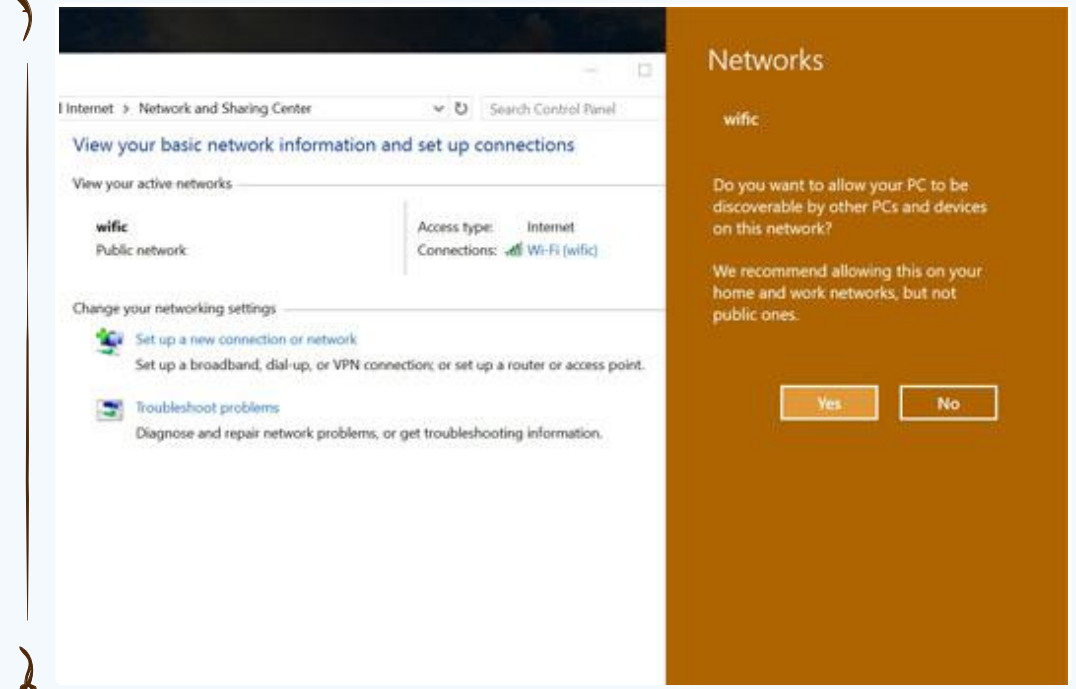
Windows 8 výběr umístění sítě



Windows 7 výběr umístění sítě

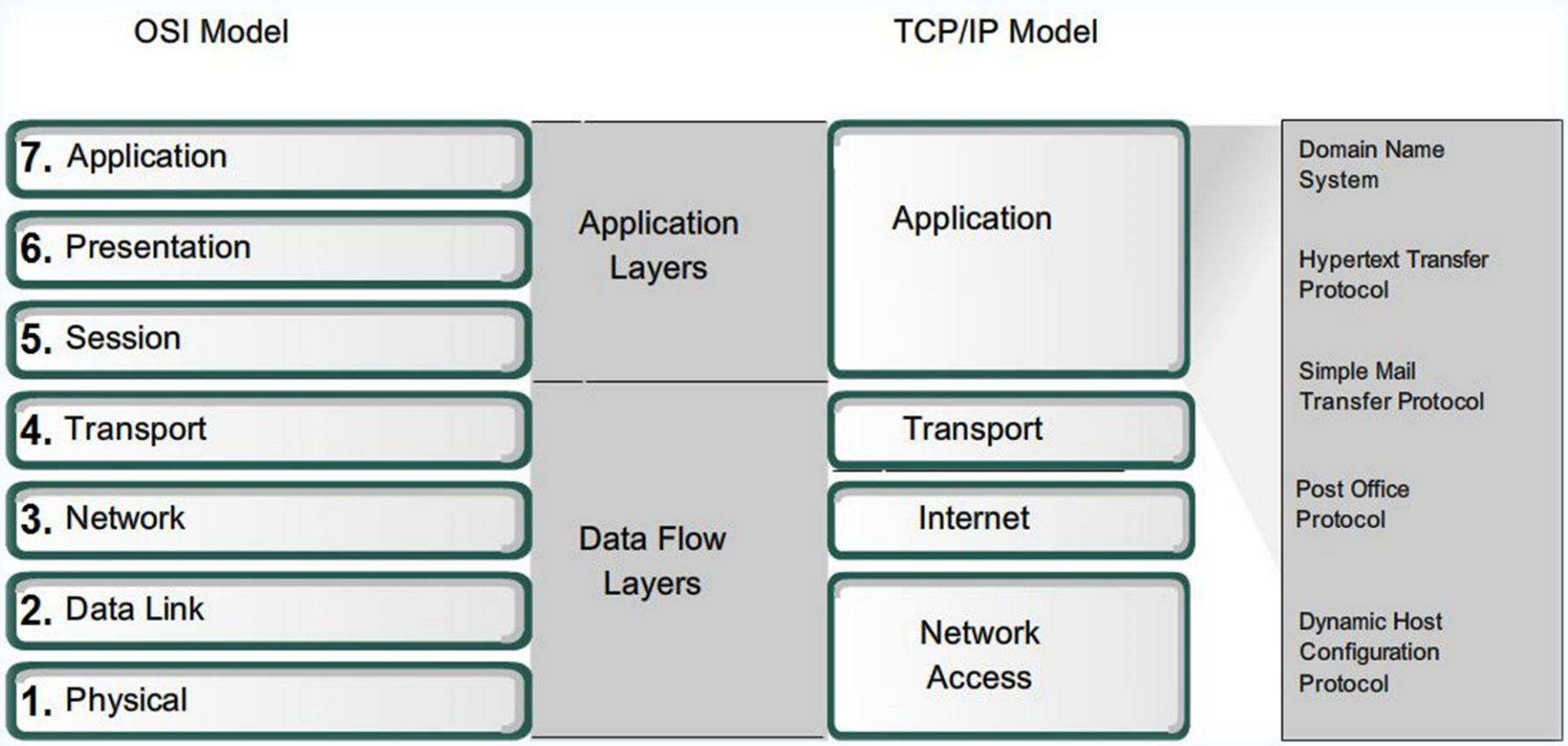
Home | Work = Private

Public location = Public



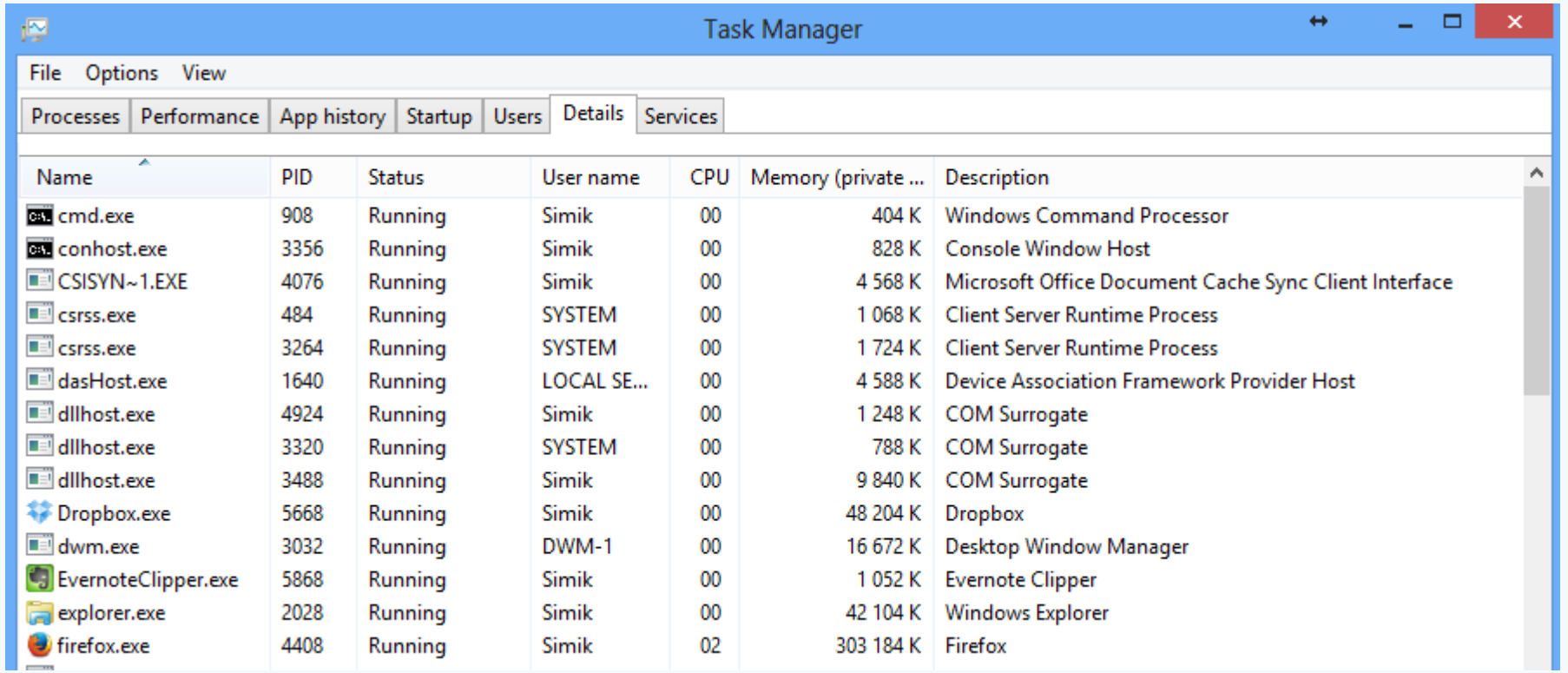
Windows 10 výběr umístění sítě

4 vrstvý síťový model



Převzato z CISCO Networking Academy, CCNA

Aplikační vrstva



SMB protokol

- Klient-server protokol pro sdílený přístup k prostředkům na síti
- SMB v2 od Vista a Server 2008, v3 od Windows 8 a Server 2012
- UNC síťové adresy \\jmeno_serveru\jmeno_zdroje
- Advanced sharing settings
  - File and Printer sharing – aktivuje možnost sdílení
- Při přejmenování nebo přesunutí složky se informace o sdílení ztrácí
- Administrativní sdílení – neviditelné na síti, $

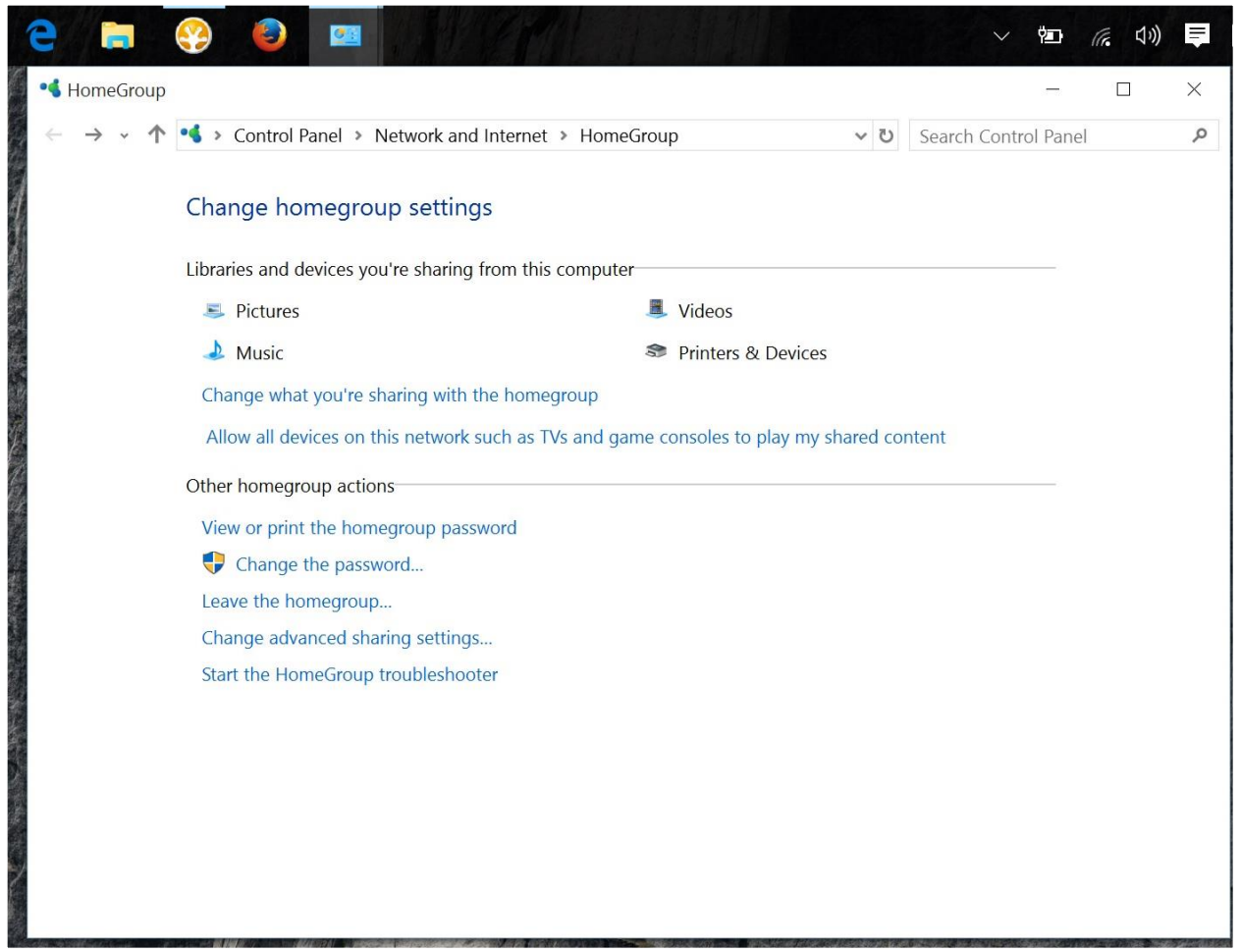
Oprávnění sdílených složek

- Vztahují se pouze na uživatele přistupující přes síť
- Kombinuje se s NTFS oprávněním, použije se to **nejvíc restriktivní**
- Sdílení lze aktivovat pouze nad složkou, ne nad souborem
  - Výjimka je sdílení uvnitř uživatelského profilu (Access-Based Enumeration)

Oprávnění	Popis
Read	Uživatelé mohou zobrazit obsah souboru, atributy a spustit programy
Change	Read + Uživatelé mohou vytvářet a přepisovat soubory, změnit atributy, zobrazovat vlastníka a oprávnění
Full Control	Read + Change + měnit oprávnění, převzít vlastnictví

DLNA

- Digital Living Network Alliance
- Pro jednoduché sdílení multimédií v domácí síti
- Počítače, mobilní zařízení, AV zařízení, herní zařízení
- DLNA server pro sdílení – DMS (Digital Media Server)
  - PC (aplikace 3. stran např. Servio), NAS, mobil …
- DLNA klient – DMP (Digital Media Player)
  - AV receiver, TV, mobil, herní konzole, PC …
  - Klient musí umět obsah přehrát



DLNA ve Windows Homegroup

Allow all devices on this network as TVs and game consoles to play my shared content

Windows Firewall

- Windows Firewall with Advanced Security
- Může filtrovat příchozí i odchozí provoz
- Typy pravidel kombinace protokolu, portu, IP adresy, typ síť. rozhraní, programu, služby, Ipsec metadat …
- FW profily podle typu sítě

Profil	Popis
Domain	Když se počítač ověří vůči DC
Private	Většinou méně přísné, očekává se domácí, či SOHO síť, používání NAT. Povolena pravidla pro network discovery
Public	Jindy

TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledgement

Převzato z CISCO Networking Academy, CCNA

Transportní vrstva

- Výběr transportního protokolu závisí na použité aplikaci
- Adresa v transportní vrstvě představuje číslo portu

Internet vrstva

- IP protokol verze 4 a verze 6
- Co je IPv4 adresa?
  - 192.168.1.102 = 11000000 10101000 00000001 01100110
  - 2 části: NetworkID, HostID
- Maska podsítě
  - Definuje, kde začíná HostID
  - 255.255.255.0 = 11111111 11111111 11111111 00000000

Maska sítě

- CIDR (Classless Interdomain Routing)
- Maska určuje do jaké sítě adresa patří
- 147.251.43.97/28 odpovídá masce 255.255.255.240

Binární hodnota	Dekadická hodnota
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

Speciální adresy

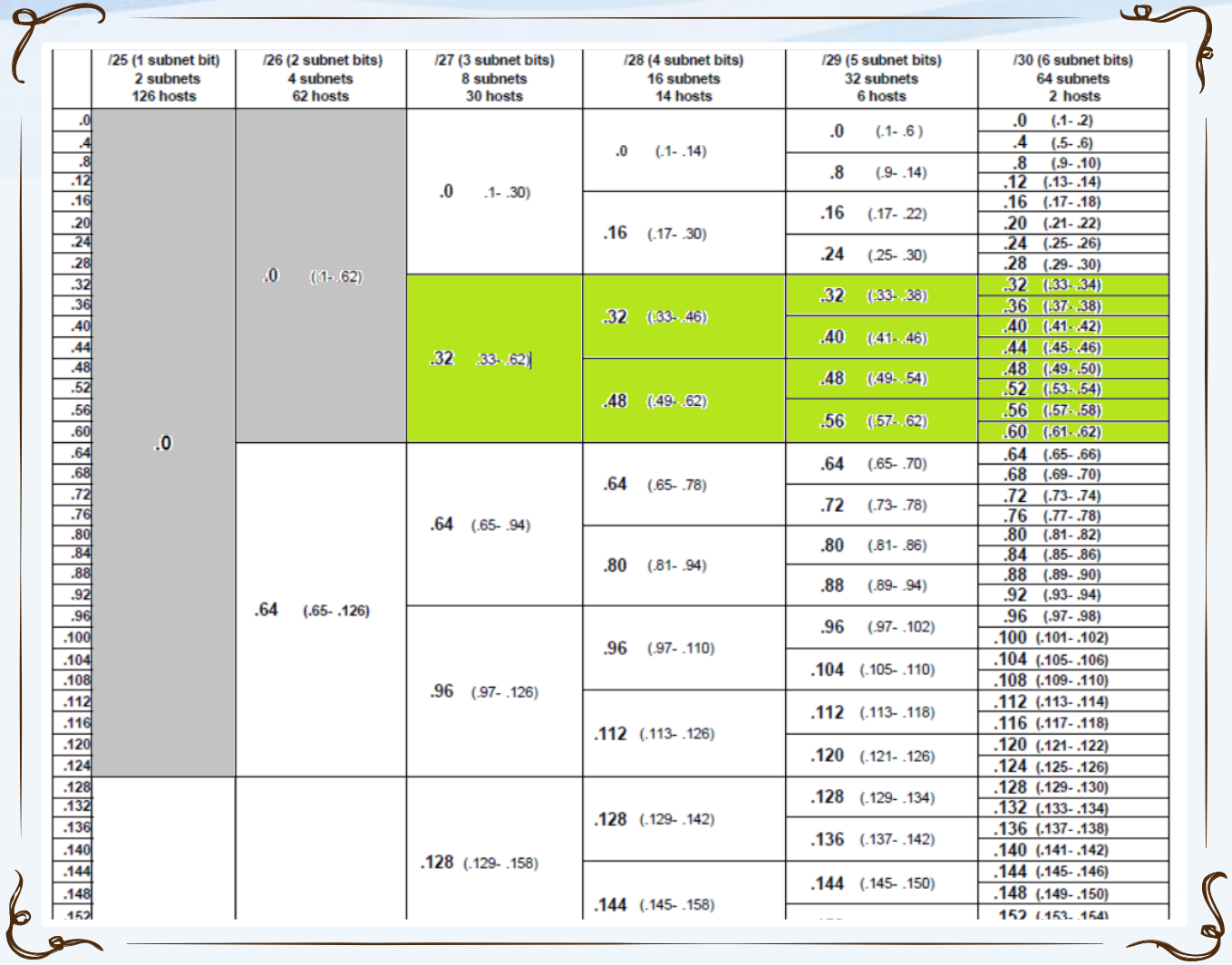
- Privátní adresy
  - 10.0.0.0 – 10.255.255.255 (10.0.0.0/8)
  - 172.16.0.0 – 172.31.255.255 (172.16.0.0/12)
  - 192.168.0.0 – 192.168.255.255 (192.168.0.0/16)
- Výchozí cesta
  - 0.0.0.0 – 0.255.255.255 (0.0.0.0/8)
- Loopback
  - 127.0.0.0 – 127.255.255.255 (127.0.0.0/8)
- Lokální adresy (Link-Local, APIPA)
  - 169.254.0.0 – 169.254.255.255 (169.254.0.0/16)
- Test-Net adresy 192.0.2.0 /24, Multicast 224.0.0.0/4

IPv4 adresace

- Nejnižší adresa v každé síti je adresa sítě
- Nejvyšší pak adresa broadcast
- Počet počítačů v síti = 2^n – 2, kde n je počet bitů v HostID

IPv4 adresace

- IP adresa zařízení 147.251.48.37
- Maska sítě 255.255.255.224
- CIDR notace 147.251.48.37/27
- IP adresa binárně 10010011.11111011.00110000.00100101
- Maska binárně 11111111.11111111.11111111.11100000
- Adresa sítě 147.251.48.32/27
- Broadcast adresa 147.251.48.63/27
- Počet možných zařízení v síti 2^5 - 2 = 30



	/25 (1 subnet bit) 2 subnets 126 hosts	/26 (2 subnet bits) 4 subnets 62 hosts	/27 (3 subnet bits) 8 subnets 30 hosts	/28 (4 subnet bits) 16 subnets 14 hosts	/29 (5 subnet bits) 32 subnets 6 hosts	/30 (6 subnet bits) 64 subnets 2 hosts
.0	.0	.0 (.1- .62)	.0 (.1- .30)	.0 (.1- .14)	.0 (.1- .6)	.0 (.1- .2)
.4						.4 (.5- .6)
.8					.8 (.9- .14)	.8 (.9- .10)
.12						.12 (.13- .14)
.16				.16 (.17- .30)	.16 (.17- .22)	.16 (.17- .18)
.20						.20 (.21- .22)
.24					.24 (.25- .30)	.24 (.25- .26)
.28						.28 (.29- .30)
.32			.32 (.33- .62)	.32 (.33- .46)	.32 (.33- .38)	.32 (.33- .34)
.36						.36 (.37- .38)
.40					.40 (.41- .46)	.40 (.41- .42)
.44						.44 (.45- .46)
.48				.48 (.49- .62)	.48 (.49- .54)	.48 (.49- .50)
.52						.52 (.53- .54)
.56					.56 (.57- .62)	.56 (.57- .58)
.60						.60 (.61- .62)
.64		.64 (.65- .126)	.64 (.65- .94)	.64 (.65- .78)	.64 (.65- .70)	.64 (.65- .66)
.68						.68 (.69- .70)
.72					.72 (.73- .78)	.72 (.73- .74)
.76						.76 (.77- .78)
.80				.80 (.81- .94)	.80 (.81- .86)	.80 (.81- .82)
.84						.84 (.85- .86)
.88					.88 (.89- .94)	.88 (.89- .90)
.92						.92 (.93- .94)
.96			.96 (.97- .126)	.96 (.97- .110)	.96 (.97- .102)	.96 (.97- .98)
.100						.100 (.101- .102)
.104					.104 (.105- .110)	.104 (.105- .106)
.108						.108 (.109- .110)
.112				.112 (.113- .126)	.112 (.113- .118)	.112 (.113- .114)
.116						.116 (.117- .118)
.120					.120 (.121- .126)	.120 (.121- .122)
.124						.124 (.125- .126)
.128			.128 (.129- .158)	.128 (.129- .142)	.128 (.129- .134)	.128 (.129- .130)
.132						.132 (.133- .134)
.136					.136 (.137- .142)	.136 (.137- .138)
.140						.140 (.141- .142)
.144				.144 (.145- .158)	.144 (.145- .150)	.144 (.145- .146)
.148						.148 (.149- .150)
.152						.152 (.153- .154)

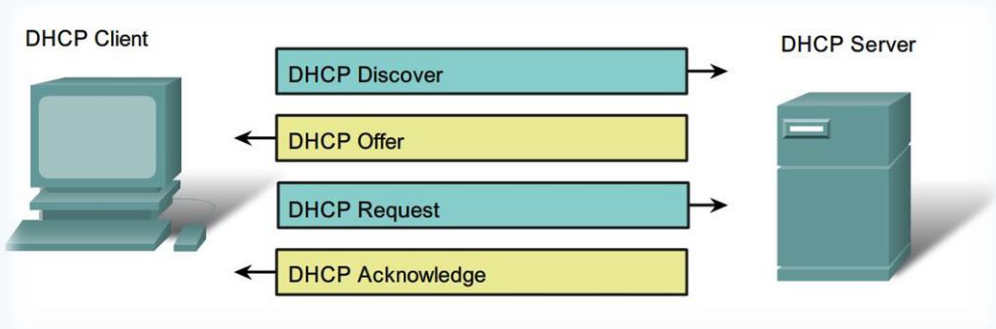
VLSM chart

- Zobrazení posledního oktetu tabulkou
- Zelený je přidělený rozsah IP adresního prostoru

Převzato z windows.microsoft.com

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 (IP, configurace)
  - Klient pošle DHCPRequest vybranému DHCP serveru
  - DHCP pošle DHCPPACK oznámení, že IP adresa byla přidělena na nějakou dobu
- Za uplynutí poloviny doby platnosti, se klient snaží nastavení obnovit



Převzato z CISCO Networking Academy, CCNA

Automatic Private IP Addressing

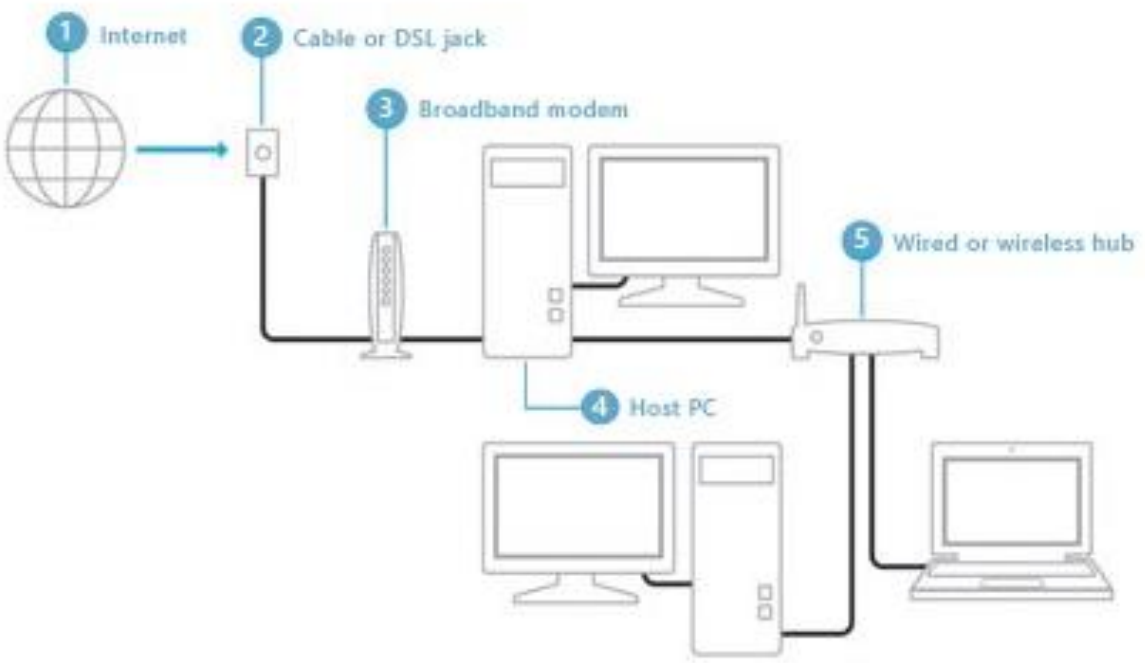
- APIPA – konf. jednoduché LAN sítě
- Jediná podsíť, bez připojení do jiné
- 169.254.x.y
- Defaultně povoleno
- Pro domácí použití
- Nastaví se pouze IP a maska!
- Proces APIPA
  - Pokus o najití DHCP, zvolí náhodnou IP, test této IP, nastavení IP
  - ∃ lease TTL > 0, pokus o obnovení, pokus o kontaktování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

Manuální konfigurace

- *Network and sharing center -> Change adapter settings (ncpa.cpl)*
- 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 fungovala doma i v práci bez rekonfigurace
- Alternativa pro jedno místo, kde není DHCP
- Plnohodnotná konfigurace na rozdíl od APIPA



Internet Connection Sharing (ICS)

Sdílení připojení mezi více PC

- Host Computer
  - Share (tab) ve vlastnostech Network Connection
  - Musí mít více síťových rozhraní
  - Slouží jako DHCP + NAT

Převzato z windows.microsoft.com

ICS

- Pro sdílení připojení přes WiFi adaptér vytvořit ad-hoc WiFi síť
  - Win 7: Network and Sharing Center -> Set up a new connection or network -> Set up a wireless ad hoc network
  - Win 8: netsh wlan set hostednetwork mode=allow ssid=jmeno key=heslo

    netsh wlan start hostednetwork
- Adaptér musí podporovat Hosted Network, lze zkontrolovat přes netsh wlan show drivers

Network Connections

- Network Clients
  - Umožňují připojení počítače s určitou sítí operačního systému (př. Připojení ke sdílené složce v síti Microsoft)
- Network Services
  - Poskytují další vlastnosti síťovým spojením (př. vysdílení složky)
- Network Protocols
  - PC může komunikovat skrze NC pouze za použití protokolů

Network Access vrstva

- Šíření signálů
- MAC adresa – adresace na úrovni L2 vrstvy Ethernetu
- ARP = Protokol pro překlad MAC <-> IPv4
- MAC adresa

Nástroje pro řešení problémů TCP/IP

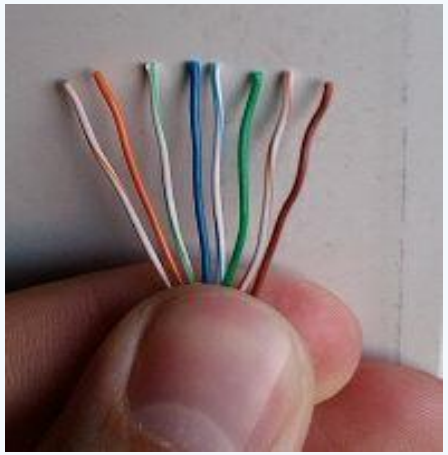
- ipconfig – zobrazí nastavení TCP/IP
  - /all, /release, /renew, /flushdns
- Ping – konektivita zevnitř ven
  - Ping Loopback, ip adresu, výchozí bránu, Internet ☺
- Tracert – zkusí projít cestu postupně
- Pathping – jako Tracert
  - zobrazí informace o ztrátě paketů na jednotlivých aktivních prvcích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

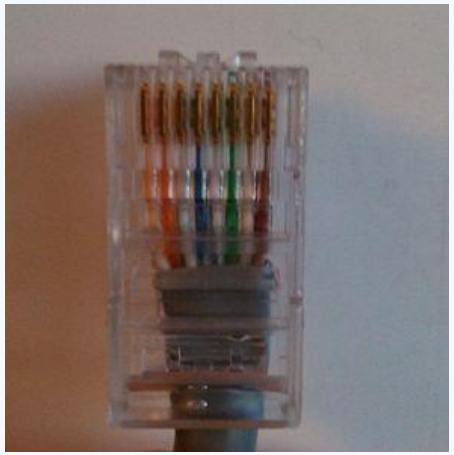
ARP poisoning

```
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

C:\Users\Administrator>
```

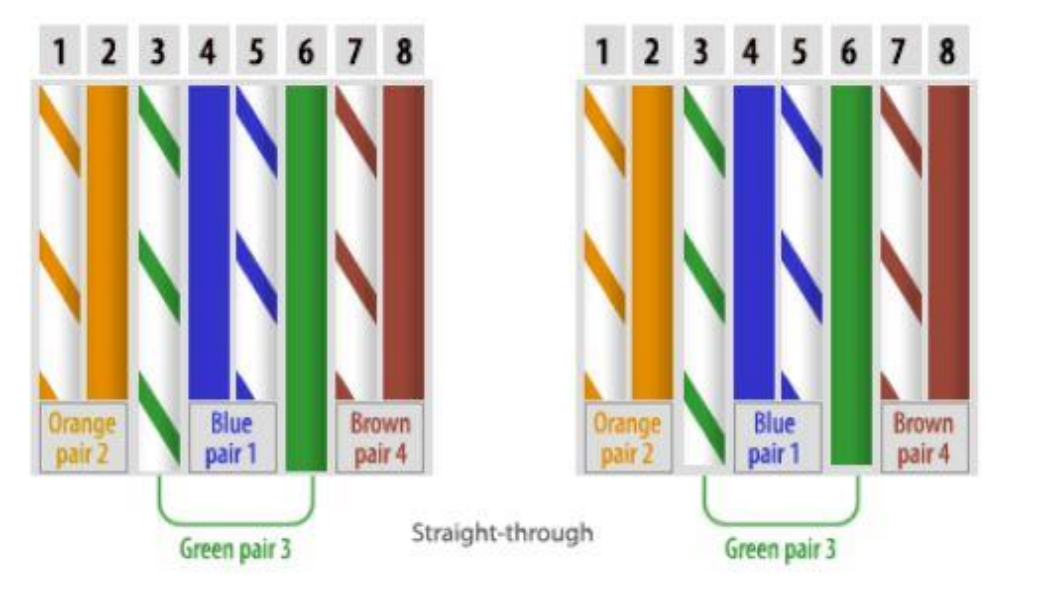
Strukturovaná kabeláž

- Ethernetový kabel UTP Cat5e – pro 1 Gbps, v současné době nejrozšířenější
- Konektor RJ45
- Krimpovací kleště pro konektor RJ45



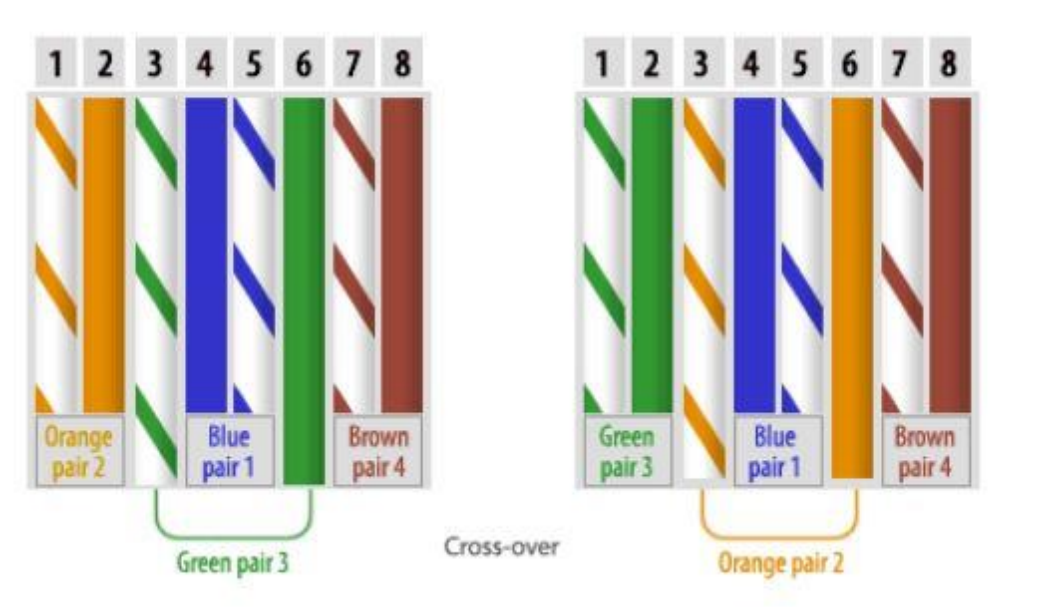


Přímý kabel (T568B)



- PC – Switch
- Switch – Router

Kroucený kabel (T568B – T568A)

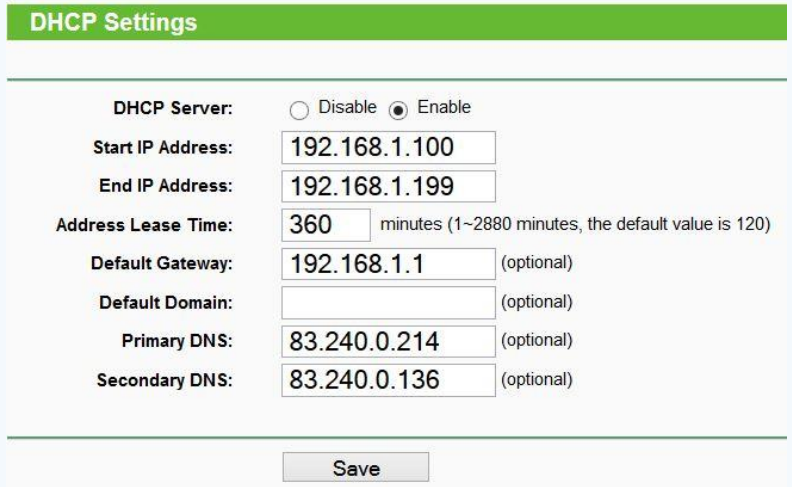


- PC – PC
- PC – Router (Ethernet port)
- Switch – Switch
- Router – Router (Ethernet)

- Pzn. tzv. router pro domácí použití není router, ale multifunkční domácí zařízení (switchoroutroaccesspoint ☺)

Vytvoření jednoduché domácí sítě

- Kolik mám zařízení?
- WiFi / kabely
- Privátní síťový rozsah
- NAT
- DHCP
- Zařízení pro stálý provoz na síti?
- Vhodné vedení kabelů



Kritéria pro výběr switche

- Cena
- Kabel / Bezdrátové
- Rychlost
- Porty
- Rozšiřitelnost
- Možnosti správy
- Funkce

Domácí router

Porty

Pozvánka

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