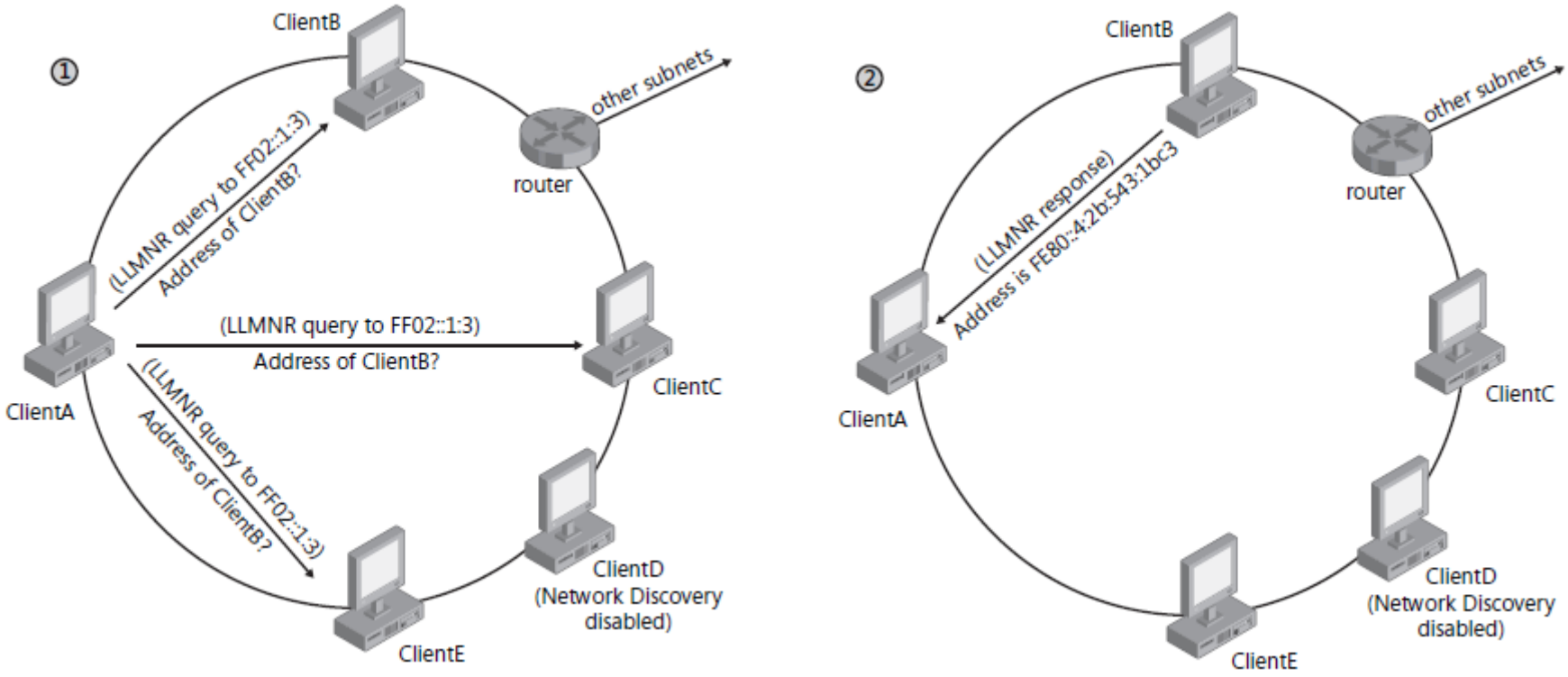
Překlad jmen, instalace AD

Šimon Suchomel

Překladové služby

- DNS
- LLMNR (Link Local Multicast Name Resolution)
- NetBIOS

LLMNR



Převzato z MCTS Self Paced Training Kit Exam 70-642.Configuring Windows Server 2008 Network

hostname

- Každý počítač má hostname
- na rozdíl od NetBIOSu použitelný v Internetu - hierarchický obor názvů
- Je částí FQDN, Fully Qualified Domain Name
  - atlantis.fi.muni.cz
- jediný hostitel může být v síti znám pod více hostitelskými jmény
- Pozn. UNC konvence
  - \\atlantis

Statický překlad jmen

- NetBIOS - soubor LMHOSTS pro WINS

  147.251.53.156 nereis01 #PRE

- Host name -soubor HOSTS pro DNS

  147.251.48.66 atys

  147.251.48.17 artemis instalace

%SYSTEMROOT%\system32\drivers\etc\

DNS

- Hierarchický systém doménových jmen
- Protokol používá porty TCP/53 i UDP/53
- Kromě překladu jmen zajišťuje informace o distribuci služeb v síti (SRV záznamy)

DNS nejčastější typy záznamů

- host – address (A) - běžný záznam, překlad jména na IP adresu počítače
- alias – canonical name (CNAME) - další jméno (alias) pro existující záznam v doméně
- mail exchanger (MX) - adresa poštovního serveru
- service location (SRV) - adresa některé služby, jako ldap, kerberos, ftp, a další
- name server (NS) - seznam serverů, které zajišťují DNS služby pro doménu, záznam se nachází v nadřazené doméně a v aktuální doméně
- pointer (PTR) - užívá se pro reverzní překlad IP -> host
- start of authority (SOA) - odkazuje na server, kde jsou primární údaje (primární NS)

DNS zóny

- primární zóna: obsahuje informace o zóně v textovém souboru s možností zápisu; je vždy jen jedna
- sekundární zóna: obsahuje informace o zóně v textovém souboru, ale pouze pro čtení
- zóna integrovaná do Active Directory: jedná se o primární zónu, která nemá záznamy v textovém souboru, ale ukládá je přímo do databáze AD
- stub zóna: tato zóna se použije, pokud potřebujeme spojit jmenné prostory více zón; obsahuje pouze SOA, NS a A záznamy jmenných serverů ostatních zón; je určena pouze pro čtení; může být integrovaná do AD

Instalace AD

- Windows Server
- Administrátorský přístup

- Vymyšlené DNS a NetBios jméno domény
  - Možná instalace nového DNS serveru
- Konfigurace síťového rozhraní

Instalace AD - komponenty

- Les, strom, doména
  - Organizační jednotky, sites
- Doménový řadič
- Funkční úrovně
  - Domény: Win 2000 native, Win. Server 2003, Win. server 2008
  - Lesa: Win. Server 2003, Win. Server 2008, *(R2)
- Databáze AD

NTDS

- Ntds.dit
  - databázový soubor Active Directory
  - obsahuje všechny objekty AD na doménovém řadiči
- Edb*.log
  - logovací soubor databázových transakcí
- Edb.chk
  - soubor s checkpointy transakcí
  - ukazuje, které transakce z logu, byly zapsány do Active Directory

SYSVOL

- obsahuje systémový svazek, který bude sdílen a replikován mezi všemi doménovými řadiči
- obsahuje veškeré skupinové politiky domény

Úkoly

- Přihlásíme se, změníme si hesla, přejmenujeme PC
- Zkontrolujeme nastavení:
  - Lokální statická IPv4 adresa (př. 10.10.10.1/24)
  - Konektivita mezi stroji (výjimka na FW)

- Splňujeme prerekvizity instalace AD?

Úkoly

- Přidáme roli AD DS
- Kontrolní otázka: Co je zapotřebí mít pro vytvoření DC?
  1. Platné DNS jméno
  2. Platné NetBios jméno
  3. DHCP server pro přidělení adresy DC
  4. DNS server
- Je nainstalován řadič domény?

Úkoly

- Dcpromo.exe

- Kontrolní otázka: Jak nainstaluji nový strom v existujícím lese a co je k tomu potřeba?

Kontrolní otázky

- Jaká je hlavní funkce Dcpromo?

- Po přidělení nové IP adresy určitému počítači jste zjistili, že určitý DNS server špatně překládá jméno tohoto počítače ze své lokální cache. Jak tento problém vyřešíte?
  a) Na DNS serveru spustíte dnscmd /clearcache
  b) Restartujete službu DNS klient na klientském počítači
  c) Na klientském počítači spustíte ipconfig /flushdns
  d) Restartujete všechny DNS klientské počítače

- Řadičem domény může být:
  a) Počítač s operačním systémem Windows 7 s nainstalovanou databází AD
  b) Počítač s Windows Server 2008 R2 povýšený jako řadič domény
  c) Notebook umístěný v ložnici s povolným Internet Connection Sharing
  d) Jakékoliv zařízení umožňující řídit DNS doménu bez primárního DNS serveru včetně DHCP konfigurace

Úkoly

- Přihlášení na DC
- Uvědomit si, že neexistují lokální účty
- Dostupnost domény z jiných počítačů
- Zapojení počítačů do domény

- Netstat {př. Netstat –sp tcp}
- DNS snap in
- Prohlídka záznamu
- SRV záznam
- _služba._protokol.jméno TTL třída SRV priorita váha port cíl

Úkoly

- DNS překlady
- Nslookup
- Ipconfig /displaydns /flushdns
- Přidání A záznamu a PTR záznamu
- Ověření konfigurace forwarders vs. Root hints
  - DNS recursion
- Smazání DNS cache na serveru
  - Dnscmd.exe /clearcache
- Restart služby netlogon