Správa systému MS Windows II

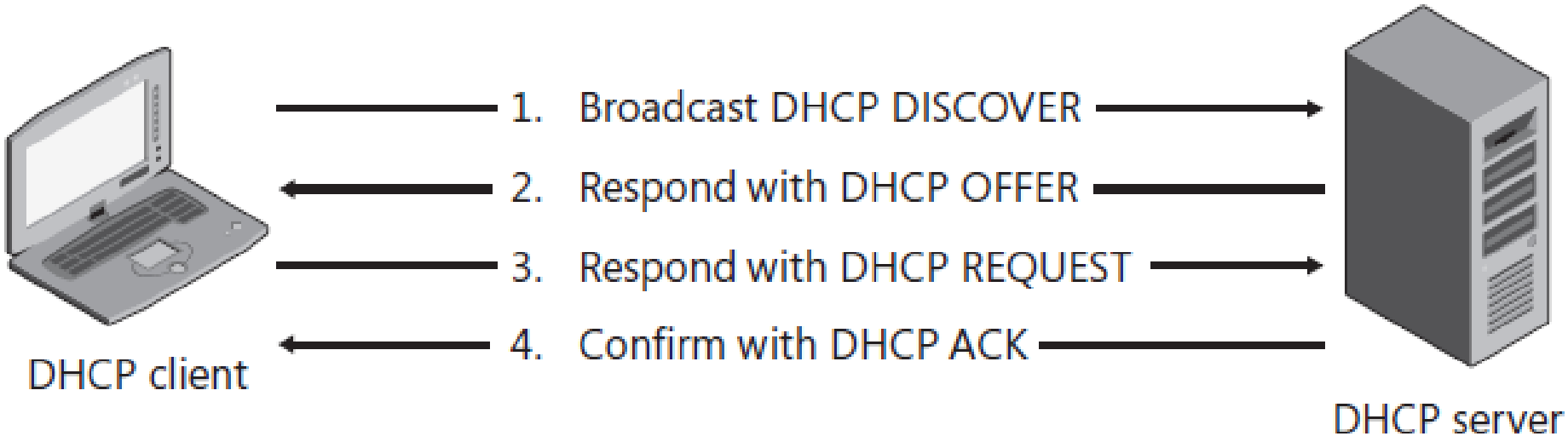
Jaro 2016

- DHCP
- Networking IPv6

DHCP

DHCP

- Dynamic Host Configuration Protocol (DHCP)
  - Automatická konfigurace IP
  - Jednodušší než ruční nastavení pro každý počítač (změny IP adres a dalších parametrů)



DHCP a ARP

- Ukázka reálného provozu s pomocí WireSharku

Source	Destination	Protocol	Length	Info
0.0.0.0	255.255.255.255	DHCP	354	DHCP Request - Transaction ID 0xeaf52cc5
192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0xeaf52cc5
Giga-Byt_c0:53:b2	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.44
ZygateCo_90:a9:ba	Giga-Byt_c0:53:b2	ARP	60	192.168.1.1 is at 00:02:cf:90:a9:ba
Giga-Byt_c0:53:b2	Broadcast	ARP	42	Who has 192.168.1.44? Tell 0.0.0.0
192.168.1.44	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x8a8ac949
192.168.1.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x8a8ac949

- http://www.keyboardbanger.com/dhcp-exposed/

DHCP 3

- DHCP server si udržuje databázi IP, které může přidělovat
  - Jakmile IP přidělí klientovi (Lease) označí ji
  - IP je přidělena na konkrétní časový úsek (Lease duration)
  - V polovině tohoto úseku klient požádá DHCP server prodloužení přidělení
    - Pokud není DHCP online, zkusí znovu v polovině zbývající doby
    - Pokud již uplynulo 87.5% celkové přidělené doby, začne hledat nový DHCP server

DHCP 4

- Klient může IP adresu uvolnit (relase), pokud tak neučiní, DHCP server ji po celou dobu trvání Lease Duration nikomu nepřidělí.
  - Tam kde se klienti často mění je vhodná kratší doba (např. WiFi či různé hot-spoty) jinak může dojít k vyčerpání dostupných adres
- DHCP Scope – rozsah IP adres s parametry sítě (DNS, GW, Lease Duration, Exclusion range…)
- Zpravidla se serverům definují statické IP adresy (pro případ výpadku DHCP)

DHCP 5

- Co způsobí výpadek DHCP v síti? Jsou škody okamžité?
- Až se budete učit na zkoušku – myslete na autorizaci DHCP v Active Directory. Kdy je scope aktivní – malá ikonka. Není nic snazšího než si to otestovat…

Demo

Úkoly 1

- Na VM s nejnižším portem nainstalujte roli DHCP server, binding na adaptér LAN.
  - Tedy nikoliv na adaptér WAN☺
- Na VM s druhým nejnižším portem taktéž nainstalujte roli DHCP server, binding stejně.
- Zajistěte, aby jeden DHCP server přiděloval IP na LAN adaptéru z rozsahu 10.10.10.100-10.10.10.200
- Pro VM s nejvyšší portem vytvořte rezervaci na IP 10.10.10.50
- Ověřte, že všechny vaše VM mohou mezi sebou komunikovat pomocí adaptérů LAN a mají IP ze správného rozsahu

DHCP PowerShell

- *#Nainstalvovat roli*
- *Add-WindowsFeature DHCP -IncludeManagementTools*
- *Set-DhcpServerv4Binding -BindingState $true -InterfaceAlias "Local Area Connection"*
- *Add-DhcpServerv4Scope -Name "Friendly Name of Scope" -StartRange 10.10.10.100 -EndRange 10.10.10.200 -SubnetMask 255.255.255.0*
- *Add-DhcpServerv4Reservation -IPAddress 10.10.10.50 -ClientId F0-DE-F1-7A-11-6A -Description "Friendly name of reservation"*
  - *Get-DhcpServerV4Lease -IPAddress 10.10.10.x | Add-DhcpServerV4Reservation*

Case study

- Firma Kredenc
  - 20 počítačů mix ntb a pracovních stanic
  - Jedna velká kancelář
  - Všechna zařízení zapojená ethernet kabelem do centrálního switche
  - Malý domácí router
  - Internetové připojení pro domácnost
  - 3 PC slouží jako „servery“ (WS 2008 R2)

Case study

- Majitel firmy má na svém ntb vývojovou verzi web aplikace, potřebuje aby tato verze byla dostupná z internetu (pokud je v práci)
  - Na routeru je možné vytvořit port-forwarding na specifickou IP
- Zajistěte aby ntb majitele firmy dostával stále stejnou IP adresu
- Zajistěte aby v případě selhání jednoho DHCP serveru nadále fungovalo síťová komunikace i pro nově příchozí klienty
- Karel, kterého se firmy chystá brzo propustit (končí mu roční smlouva) neustále nosí do práce vlastní notebook a využívá firemní internet. Existuje na DHCP serveru nějaké nastavení, které by mu jeho počínání znemožnilo/zkomplikovalo?

- I

IPv6

IPv6 přehled

- Zápis IPv6 definuje RFC 4291, aplikace musí být schopna zpracovat všechny způsoby zápisu!
- Stále se vyvíjející definice – různá podpora ze strany výrobců HW a SW
- Typy IPv6 adres
- Přidělené rozsahy
  - http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml
  - http://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xml

Terminologie

- Node - Equipment handling IPv6 in any way
- Router- Equipment doing IPv6 routing
- Host - Equipment that does NOT route packages
- Link - A LAN or WAN network
- Neighbor - A node in the same link

IPv6 a přidělování IP adres

- Na počátku byla dobrá myšlenka – proč konfigurovat specifické IP adresy zařízením, když si zařízení může zvolit svoji IP adresu AUTOMATICKY samo?
  - Adresa klienta (Interface ID) může být odvozena z například z MAC adresy zařízení nebo i zcela náhodně
    1. EUI-64 mechanismus
    2. Náhodné generování adresy (privacy)

IPv6 a přidělování IP adres 2

- Zbývá vyřešit problém jak sdělit zařízení jeho Global Network Prefix (ekvivalent Network ID z IPv4)
  - Kdo musí vědět Global Network Prefix v daném segmentu sítě? ROUTER
    - Musí doručit data do ostatních sítí a musí znát informace o ostatních sítí…
  - Router nějakým způsobem sdělí klientům jaký si mají nastavit Global Network Prefix
    - SLAAC (bez stavová autokonfigurace)

IPv6 a přidělování IP adres 3

- SLAAC (Stateless Adress Autoconfiguration)
  - Pomocí ICMPv6
- SLAAC ale neřeší DNS a další nastavení sítě (které bylo dříve možné konfigurovat pomocí DHCPv4)
  - Vznikla celá řada řešení tohoto „drobného“ problému

IPv6 a přidělování IP adres 4

Řešení 1.

- RFC 6106 přidává do mechanismu SLAAC informaci o DNS serverech – router je tak stále jediné zařízení, které je potřeba pro konfiguraci IPv6
- Nevýhoda:
  - MS se rozhodl neimplementovat do žádného ze svých OS.

IPv6 a přidělování IP adres 5

Řešení 2.

- Vždy stejná adresa DNS serveru na libovolné síti
- Anycast adresy:
  - fec0:0:0:ffff::1
  - fec0:0:0:ffff::2
  - fec0:0:0:ffff::3
- Implementováno ve Windows (tj. je možné to použít)
- Nevýhoda:
  - Používá Site-Local adresy, které byly zrušeny (nemají se používat)
  - Chybí RFC standard
  - Kromě MS neimplementoval nikdo z velkých výrobců

IPv6 a přidělování IP adres 6

Řešení 3.

- Informace poskytne jiný mechanismus, jiným protokolem: DHCPv6
- Je nutné zkombinovat oba dva přístupy
- Jak klient pozná, koho se má zeptat na IP adresu? Má si ji nastavit sám? Má ji dostat od DHCP, nebo má od DHCP dostat jenom DNS servery…
  - Klient komunikuje s Routerem a router předává (mimo jiné) informaci klientovi prostřednictvím 3 bitů:
  - Managed
  - Options
  - Autonomous flag

IPv6 a přidělování IP adres 7

- Příklad:
  - Klient pošle dotaz Routeru (Router Solicitation) na multicast adresu „všechny routery“
    - Router odpoví (Router Advertisment) A=1,M=1,O=1 (+ další informace)
  - Klient si nastaví SLAAC adresu podle prefixu z odpovědi od routeru a zároveň klient pošle dotaz DHCPv6 na multicast adresu „všechny DHCPv6“
    - DHCP server odpoví IP adresu, DNS servery atd.
  - Klient si nastaví další IP adresu podle informací z DHCPv6

IPv6 a přidělování IP adres 8

- Jakou IP bude klient používat záleží na konkrétní implementaci v OS. Jak dále uvidíme, Windows navíc generuje tzv. temporary IPv6 adresy (pro ještě větší anonymitu), které se neustále mění
  - Spoustu pravidel na síti je vytvořeno na základě IP adres + zákonné povinnosti + diagnostika: vyhledávání problematických klientů s viry, dětské porno atd… Provozovatel sítě musí vědět kdo je kdo
  - Nabízí se deaktivovat mechanismus SLAAC a nechat pouze DHCPv6 aby nastavil veškeré informace
  - Problém:
    - DHCPv6 neumožňuje nastavit výchozí bránu!
    - Výchozí brána se nastavuje pouze pomocí mechanismu ICMPv6 (Router Advertisement)
  - Pro úspěšnou konfiguraci IPv6 ve Windows je potřeba použít Router Advertisement a DHCPv6 dohromady.
  - Zabránit generování SLAAC adresy je možné pomocí nastavení Autonomous flag na 0. Bohužel ne všechny zařízení toto nastavení podporují!

IPv6 a přidělování IP adres 9

Autonomous Flag	Managed	Options	DHCPv6	SLAAC
1	0	0	Žádná	**IP + DNS***
1	1	0	IP	IP
0	0	1	DNS	žádná
0	1	1	**IP + DNS**	Žádná
1	1	1	**IP + DNS**	**IP + DNS***

*** DNS dostanou pouze ti klienti, kteří implementovali RFC 6106, což NENÍ Windows!**

IPv6 a přidělování IP adres 10

Autonomous Flag	Managed	Options	DHCPv6	SLAAC
0	1	1	**DNS+IP**	žádná

- Zdá se jako perfektní řešení ale nefunguje na všech OS – zejména ne na Android platformě…
  - http://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_operating_systems

IPv6 a přidělování IP adres 11

- Rozhodli jsme se přidělovat adresy pomocí DHCPv6.
  - DHCPv4 používá MAC adresy
  - DHCPv6 nepoužívá MAC adresy ale DUID (DHCP Unique Indentifier)
  - Výhoda – pokud změním adaptér (např. WiFi / Ethernet) a jsem připojen do stejné sítě, vystupuji jako stále stejný uživatel
  - Nevýhoda – Generování je závisle na nastavení OS. Mění se s reinstalací (ve Windows) OS.
    - Pokud potřebuji okamžitě zjistit kdo je kdo, potřebuji další mechanismy

IPv6 a přidělování IP adres 12

- SLAAC mechanismus ve výchozím nastavení Windows generuje pseudonáhodnou adresu pro Interface ID
  - Mechanismus EUI-64, který ji generuje z MAC adresy (abychom mohli jako provozovatel sítě lépe vyhledat klienta) není z důvodu ochrany soukromí aktivní (je možné ho aktivovat na klientovi dodatečně)
  - Zároveň ve Windows Vista, 7, 8… (nikoliv server edice) pro každou globální a ULA IPv6 adresu vygeneruje navíc další Temporary adresu
    - Používá se POUZE pro odchozí připojení a nevkládá se do DNS
    - Mění se periodicky v závislosti na nastavených parametrech v Router Advertisment
    - Proto budou u adaptéru postupem času vidět „expirované“ IPv6 Temporary adresy

IPv6 a dualstack

- Kdy Windows použije jakou IPv6 a kdy IPv4?
  - Komplexní proces rozhodování s mnoha proměnnými (počínaje verzí OS, konče konfigurací sítě) > RFC 6724 a RFC 3484 + MS vylepšení v podobě NCSI
- Pozor – aplikace mohou mít vlastní logiku, např. Chrome, se pokusí připojit pomocí první IP, kterou dostal v DNS odpovědi a pokud nedostane odpověď během 300ms zkusí další

Demo

Úkol 1

- Vygenerovat ULA prefix - http://unique-local-ipv6.com/
- Nastavit DHCPv6 aby přidělovalo klientům IP na ULA
  - Pozor – na pořadí konfigurace (stejné jako u IPv4 – nejprve statická IP pro server…)
  - Funguje ping mezi klienty?
    - Route print - /64 prefix nebo /128 prefix pro naši ULA síť?
    - Prefix Advertisment v DHCPv6 u Windows – nikoliv.
    - **Vždy je nutné kombinovat Router + DHCPv6!**
    - http://rakhesh.com/windows/enabling-ipv6-router-advertisements-on-windows/