IPv6 – nové (ne)bezpečí?

Ondřej Caletka

Studentská unie ČVUT v Praze, klub Silicon Hill

22. února 2011

Silicon Hill

- Studentský klub Studentské unie ČVUT
- Zajišťuje provoz sítě na kolejích Strahov
  - Technologie Cisco Catalyst 6509, 3750, 29xx
  - 10 Gbps připojení do sítě ČVUT, $n \times 1$ Gbps páteř
- Více než 4000 připojených uživatelů
  - 147.32.112.0/20 - 4096 IPv4 adres
  - IPv4 adresy došly kolem roku 2005
- IPv6 v provozu od roku 2004

IPv6

- Nový protokol síťové vrstvy:
  - Vytváří novou síť, nekompatibilní s IPv4.
  - Kompatibilní s protokoly jiných vrstev (TCP, UDP, HTTP, FTP, Ethernet, PPP).
- IPv6 adresa:
  - Globálně/lokálně unikátní identifikátor a lokátor.
  - 48 bitů globální prefix.
  - 16 bitů identifikátor podsítě.
  - 64 bitů identifikátor rozhraní (10^{18} adres).
- Nepočítá s používáním NAT:
  - Bezpečnost mají zajišťovat firewally.
  - I další „výhody“ NATu mají v IPv6 alternativní řešení.

Proč zavádět IPv6

- Nastala fáze vyčerpání IPv4 adres. Používání IPv4 představuje překážku v rozvoji Internetu.
- Začnou se objevovat služby jen na IPv6.
- Je možné, že nějaká autorita IPv4 adresy odebere pro narovnání situace na trhu.
- Potřebujeme-li veřejné IP adresy, jsou IPv6 adresy výrazně dostupnější.

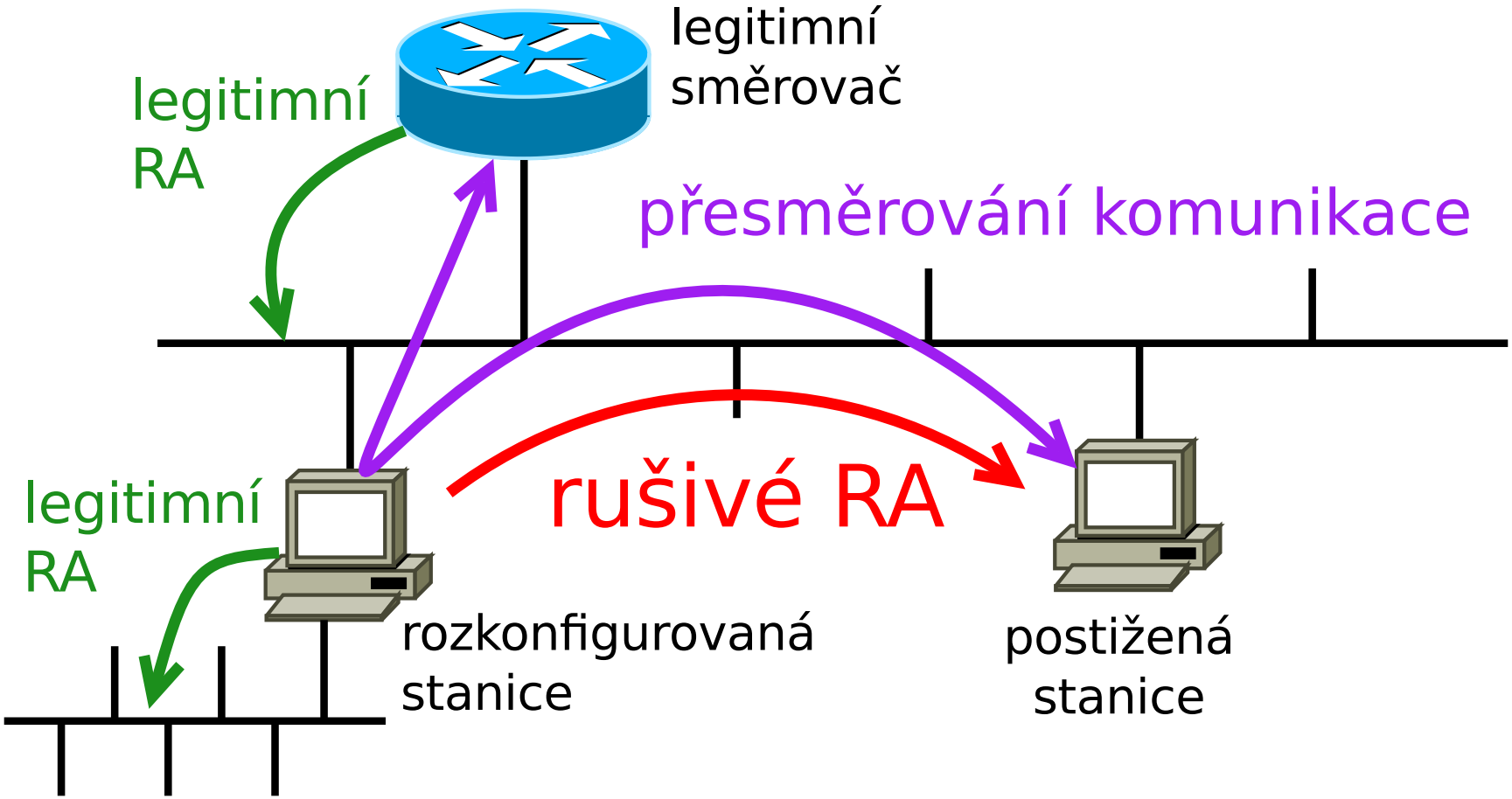
IPv6 v lokální síti

- Neexistuje spolehlivý způsob, jak přistupovat z IPv4 do IPv6 sítě a naopak.
- Doporučeným řešením je *dual-stack*, tedy současný provoz IPv6 a IPv4 sítě.
  - Je třeba současně udržovat dvě nezávislé sítě.
  - Není jednoduché udržet pevnou vazbu mezi IPv4 adresou a IPv6 adresou.
- Směrování se v lokálních sítích IPv6 se konfiguruje automaticky:
  - Směrovače vysílají do sítě *ohlášení* (Router Advertisment)
  - Stanice po přijetí ohlášení *okamžitě* konfigurují své směrovací tabulky.

Nebezpečí automatické konfigurace

- Současné implementace IPv6 (Windows, Linux) nepodporují kryptografické zabezpečení autokonfigurace (SeND).
- Útočník může např. předstírat směrovač a převzít veškerý IPv6 provoz:
  - Nejčastější útočník: Windows Vista a vyšší plus služba Internet Connection Sharing.
  - Záznamy ve směrovací tabulce zůstávají i po odstranění *škodlivého* směrovače a způsobují nefunkčnost konektivity.
- Také je možné zneužít detekci duplicitních adres k útoku typu DoS.

Přesměrování komunikace



Obrana proti falešným směrovačům

- RA-guard na přístupové vrstvě:
  - Přijde-li RA z neautorizovaného portu, není propuštěno a port se vypne.
  - Vyžaduje přepínače, které rozumí IPv6.
  - Obdoba DHCP snoopingu pro IPv4.
- RAmond na libovolném počítači na segmentu:
  - Vysílá protiohlášení, kterým ruší účinky původního.
  - Pouze workaround, nejedná se o systémové řešení.
- Vysoká priorita autoritativních směrovačů:
  - Pouze částečná obrana proti rozkonfigurovaným MS Windows, nezabrání útočníkovi.
- Ruční konfigurace.

Automatická konfigurace IPv6 adres

- Bezestavová autokonfigurace (SLAAC)
  - Vychází z automatické konfigurace směrování.
  - Směrovač v *ohlášení* sděluje 64-bitový prefix.
  - Klient k prefixu připojí vlastní identifikátor rozhraní, tak vytvoří svou adresu.
- DHCPv6
  - Obdoba protokolu DHCP pro IPv4.
  - Umožňuje mj. i přidělovat adresní prefix pro domácí směrovače.
  - Není soběstačný, potřebuje RA.

Úskalí bezestavové autokonfigurace

- Dokáže přidělit pouze IP adresu, nikoli DNS, NTP, SIP server, atd.
- Problém s identifikátory rozhraní:
  - Identifikátor rozhraní je obecně náhodné číslo.
  - Některé implementace ho odvozují z MAC adresy.
  - Náhodný identifikátor se může v čase měnit.
- Problém s de-anonymizací počítačů.
  Možná řešení:
  - Filtrovat pouze adresy, které jsou odvozeny z MAC adres a každý počítač zkonfigurovat.
  - Zaznamenávat tabulky sousedů na směrovačích (MAC adresy odpovídající IPv6 adresám).

DHCPv6

- K identifikaci počítače se nepoužívá MAC adresa, ale *DHCP Unique Identifier* (DUID):
  - Identifikátor společný pro celý počítač.
  - Nezávislý na obměně HW.
  - Obvykle se používá linková adresa libovolné síťové karty a čas prvního startu operačního systému.
- Narozdíl od SLAAC:
  - Pracuje i s delšími prefixy, než 64 bitů.
  - Přiděluje kompletní sadu informací.
  - Dokáže přidělit i adresní prefix (pro domácí směrovače).
  - DHCPv6 server má přehled, které adresy byly přiděleny, ostatní mohou být např. filtrovány.

Jak se vyhnout dual-stacku

- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
  - Tunelování IPv6 provozu po IPv4 v lokálních sítích.
  - IPv6 adresa je odvozena od IPv4 adresy.
  - Nativně podporováno ve Windows.
- Aplikační proxy servery
  - Vhodné pro start – stačí zavést IPv6 na proxy server.
  - HTTP proxy Squid podporuje IPv6 od verze 3.1.
  - SOCKS protokol verze 5 podporuje IPv6.
- NAT64
  - Navrhovaný standard pro připojení IPv6 klientů k IPv4 serverům.
  - Umožní eliminovat v koncové síti IPv4.

Další postřehy

- Pozor na blokování ICMP zpráv, zejména v kombinaci s filtrováním povolených IPv6 adres.
  - Toto je bohužel výchozí konfigurace Windows.
  - Prakticky se projevuje zdržením cca. 30 sekund při pokusu o přístup na *dual-stack* službu.
  - Podle výzkumu Google se tento problém týká 0,5% uživatelů Internetu.
- Někdy může být vhodné upravit tabulku preferovaných adres:
  - Například preferovat IPv4 před IPv6.

Konec

Děkuji za pozornost.

5. – 6. března 2011