Nasazení protokolu IPv6 v prostředí univerzitní sítě VŠB-TU Ostrava

Martin Pustka
Martin.Pustka@vsb.cz

VŠB-TU Ostrava

Europen, Pavlov 9.5.2011

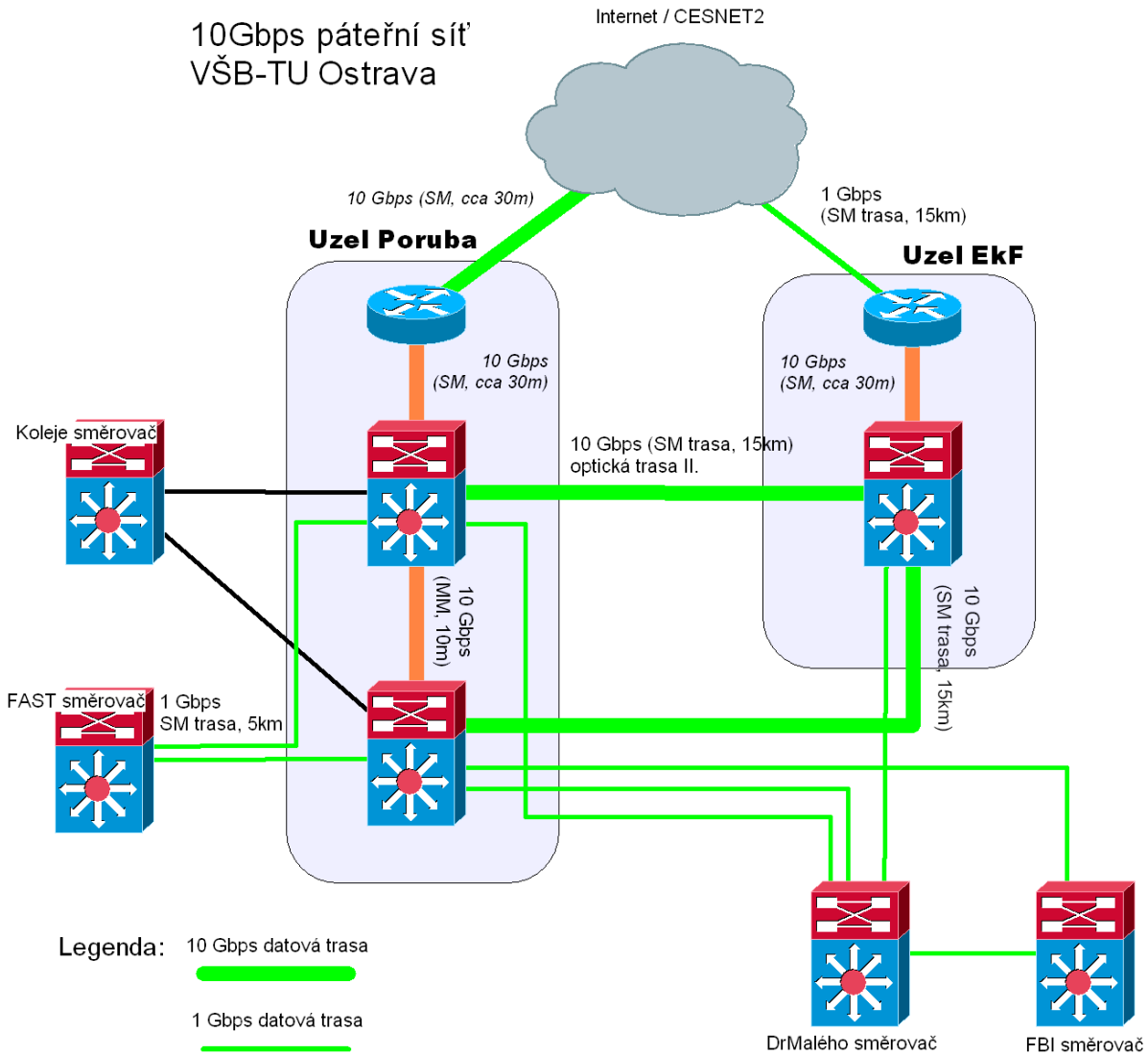
Charakteristika počítačové sítě

- Počítačová síť Vysoké školy báňské - Technické univerzity Ostrava,
- metropolitní síť - spojuje několik budov/fakult v rámci města,
- páteřní síť využívá 1/10Gbps technologie,
- 20 tis. uživatelů počítačové sítě,
- cca 10 tis. registrovaných stanic.

Fyzická topologie

- Centrální kampus se nachází v Ostravě-Porubě,
- v rámci města Ostrava další čtyři lokality propojené optickými vlákny,
- využívány jsou rámci města dvě nezávislé optické trasy,
- každý uzel připojen minimálně k dalším dvěma,
- dvě MPLS VPN (poskytuje síť CESNET2) využity pro propojení poboček v rámci ČR (Most, Uherské Hradiště).

Páteřní síť


10Gbps páteřní síť
VŠB-TU Ostrava
Internet / CESNET2
10 Gbps (SM, cca 30m)
1 Gbps
(SM trasa, 15km)
Uzel Poruba
Uzel EkF
10 Gbps
(SM, cca 30m)
10 Gbps
(SM, cca 30m)
Koleje směrovač
10 Gbps (SM trasa, 15km)
optická trasa II.
10 Gbps
(MM, 10m)
10 Gbps
(SM trasa, 15km)
FAST směrovač
1 Gbps
SM trasa, 5km
Legenda:
10 Gbps datová trasa
1 Gbps datová trasa
DrMalého směrovač
FBI směrovač

Topologie počítačové sítě

- Klasické rozdělení: páteřní - agregační - přístupová vrstva,
- centralizovaná virtuální infrastruktura (VMWARE) - 9 uzlů, zálohované připojení,
- bezdrátová počítačová síť (250+ přístupových bodů),
- přidělena IPv4 síť typu B (maska /16),
- přidělena IPv6 síť s délkou prefixu 48 bitů.

Historie nasazení IPv6

- První implementace od r.2000, využívány PC směrovače (Linux/BSD, RIPng, Zebra),
- při budování páteřní sítě v letech 2006-2007 bylo počítáno s nasazením dual-stack prvků,
- průběžně nasazovány serverové služby (DNS, WWW, FTP, SMTP, Windows/AD servery).

Pravidla při implementaci IPv6

- Dual-stack prvky, jednotná topologie,
- podpora přechodových mechanismů,
- tvorba nových sítí s podporou IPv4 i IPv6,
- nepoužívat technologie NAT a privátní adresy,
- nebudovat IPv6 only sítě.

Pravidla při implementaci IPv6

- Dual-stack prvky, jednotná topologie,
- podpora přechodových mechanismů,
- tvorba nových sítí s podporou IPv4 i IPv6,
- nepoužívat technologie NAT a privátní adresy,
- nebudovat IPv6 only sítě.

Pravidla při implementaci IPv6

- Dual-stack prvky, jednotná topologie,
- podpora přechodových mechanismů,
- tvorba nových sítí s podporou IPv4 i IPv6,
- nepoužívat technologie NAT a privátní adresy,
- nebudovat IPv6 only sítě.

Pravidla při implementaci IPv6

- Dual-stack prvky, jednotná topologie,
- podpora přechodových mechanismů,
- tvorba nových sítí s podporou IPv4 i IPv6,
- nepoužívat technologie NAT a privátní adresy,
- nebudovat IPv6 only sítě.

Pravidla při implementaci IPv6

- Dual-stack prvky, jednotná topologie,
- podpora přechodových mechanismů,
- tvorba nových sítí s podporou IPv4 i IPv6,
- nepoužívat technologie NAT a privátní adresy,
- nebudovat IPv6 only sítě.

Topologie IPv6 sítě

- Je snahou mít shodnou topologii pro IPv4/6 a dual-stack prvky,
- v IPv6 agregujeme adresní prostory přidělené lokalitám (/56),
- směrovací protokoly (OSPF, BGP) v IPv4/6,
- spojovací sítě s délkou prefixu 64 bitů,
- podpora přechodových mechanismů - nestavové ISATAP tunely.

Topologie IPv6 sítě

- Je snahou mít shodnou topologii pro IPv4/6 a dual-stack prvky,
- v IPv6 agregujeme adresní prostory přidělené lokalitám (/56),
- směrovací protokoly (OSPF, BGP) v IPv4/6,
- spojovací sítě s délkou prefixu 64 bitů,
- podpora přechodových mechanismů - nestavové ISATAP tunely.

Topologie IPv6 sítě

- Je snahou mít shodnou topologii pro IPv4/6 a dual-stack prvky,
- v IPv6 agregujeme adresní prostory přidělené lokalitám (/56),
- směrovací protokoly (OSPF, BGP) v IPv4/6,
- spojovací sítě s délkou prefixu 64 bitů,
- podpora přechodových mechanismů - nestavové ISATAP tunely.

Topologie IPv6 sítě

- Je snahou mít shodnou topologii pro IPv4/6 a dual-stack prvky,
- v IPv6 agregujeme adresní prostory přidělené lokalitám (/56),
- směrovací protokoly (OSPF, BGP) v IPv4/6,
- spojovací sítě s délkou prefixu 64 bitů,
- podpora přechodových mechanismů - nestavové ISATAP tunely.

Topologie IPv6 sítě

- Je snahou mít shodnou topologii pro IPv4/6 a dual-stack prvky,
- v IPv6 agregujeme adresní prostory přidělené lokalitám (/56),
- směrovací protokoly (OSPF, BGP) v IPv4/6,
- spojovací sítě s délkou prefixu 64 bitů,
- podpora přechodových mechanismů - nestavové ISATAP tunely.

Koncové sítě

- Je nutno rozlišovat serverové a ne-serverové sítě,
- v sítích koncových stanic je podporována autokonfigurace,
- v serverových sítích není podporována autokonfigurace, v praxi způsobuje problémy,
- v IPv4 only sítích je dostupná IPv6 konektivita přes ISATAP, vyžadována podpora DHCP u koncových stanic.

Koncové sítě

- Je nutno rozlišovat serverové a ne-serverové sítě,
- v sítích koncových stanic je podporována autokonfigurace,
- v serverových sítích není podporována autokonfigurace, v praxi způsobuje problémy,
- v IPv4 only sítích je dostupná IPv6 konektivita přes ISATAP, vyžadována podpora DHCP u koncových stanic.

Koncové sítě

- Je nutno rozlišovat serverové a ne-serverové sítě,
- v sítích koncových stanic je podporována autokonfigurace,
- v serverových sítích není podporována autokonfigurace, v praxi způsobuje problémy,
- v IPv4 only sítích je dostupná IPv6 konektivita přes ISATAP, vyžadována podpora DHCP u koncových stanic.

Koncové sítě

- Je nutno rozlišovat serverové a ne-serverové sítě,
- v sítích koncových stanic je podporována autokonfigurace,
- v serverových sítích není podporována autokonfigurace, v praxi způsobuje problémy,
- v IPv4 only sítích je dostupná IPv6 konektivita přes ISATAP, vyžadována podpora DHCP u koncových stanic.

IPv6 konektivita koncových systémů

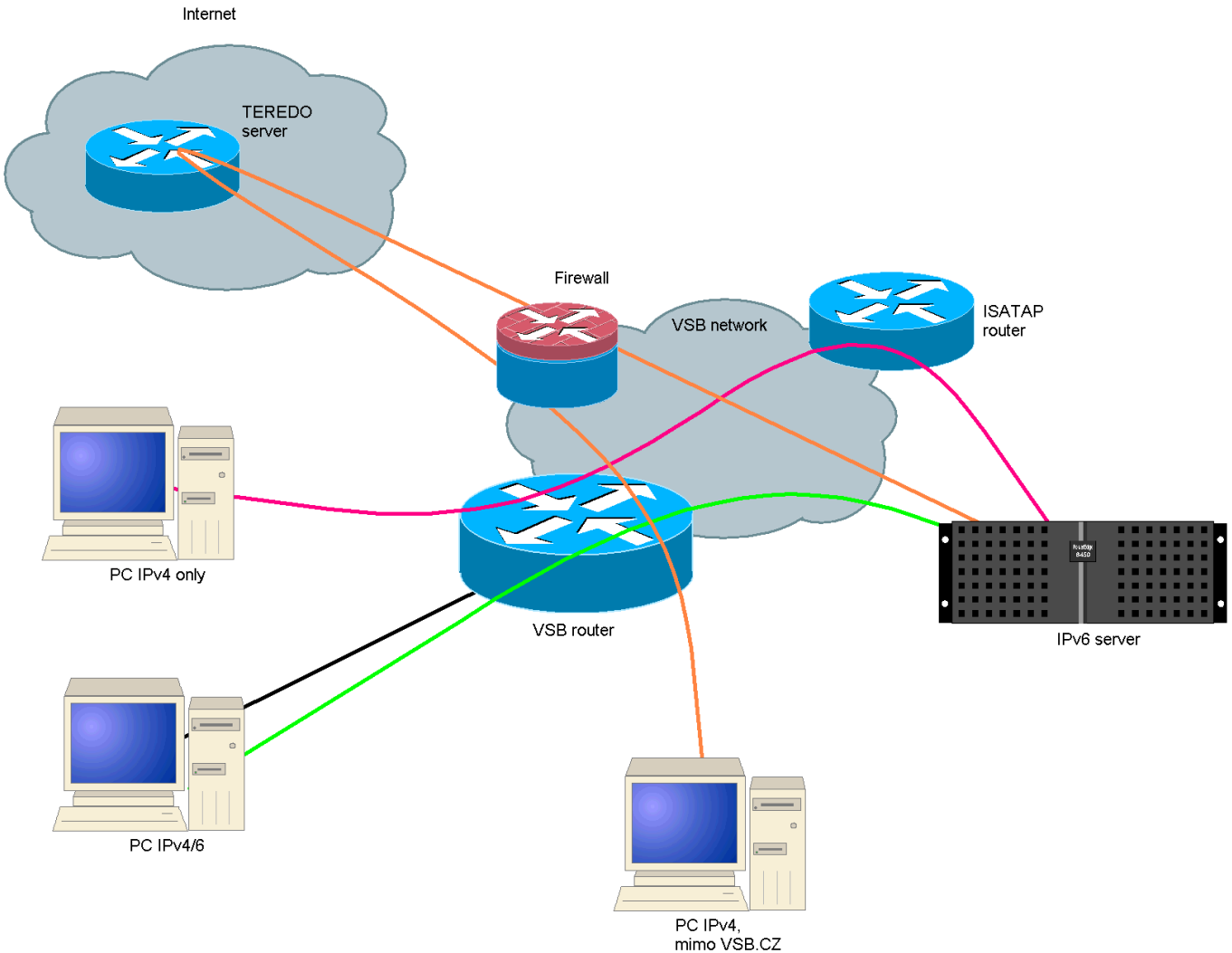
- Koncové uživatelské stanice
  - nativní připojení, vyžaduje konfiguraci sítě,
  - ISATAP tunely, automaticky navazují Windows systémy na isatap.vsb.cz,
  - TEREDO tunely, navazují Windows systémy na tunelové servery mimo síť VŠB (snaha eliminovat).
- Servery
  - princip stejný jako u uživatelských stanic (nativní, ISATAP, TEREDO),
  - preferované a doporučované je POUZE nativní připojení se staticky definovanou adresou.
  - u serverových služeb pečlivě nastavovat IPv6 varianty (sítě pro SMTP, přístupy, ...).

IPv6 konektivita koncových systémů

- Koncové uživatelské stanice
  - nativní připojení, vyžaduje konfiguraci sítě,
  - ISATAP tunely, automaticky navazují Windows systémy na isatap.vsb.cz,
  - TEREDO tunely, navazují Windows systémy na tunelové servery mimo síť VŠB (snaha eliminovat).

- Servery
  - princip stejný jako u uživatelských stanic (nativní, ISATAP, TEREDO),
  - preferované a doporučované je POUZE nativní připojení se staticky definovanou adresou.
  - u serverových služeb pečlivě nastavovat IPv6 varianty (sítě pro SMTP, přístupy, ...).

IPv6 a koncové systémy



HW/SW vybavení síťových prvků

- Celkově přes 600 aktivních prvků,
- hraniční směrovače Cisco ASR1000,
- L3 přepínače Cisco Catalyst 6500 (IOS 12.2(33)SXI), Sup32/Sup720,
- agregační přepínače Cisco Catalyst 3560/3750 (IOS 12.2(55)SE),
- přístupové přepínače Cisco Catalyst 2960 (IOS 12.2(55)SE),
- přístupové přepínače Cisco Catalyst 2950 (nijak nepodporují IPv6).
- WiFi moduly - Cisco WiSM + Cisco Aironet 1121/1131/1231/1242/1252.

HW/SW vybavení síťových prvků

- Celkově přes 600 aktivních prvků,
- hraniční směrovače Cisco ASR1000,
- L3 přepínače Cisco Catalyst 6500 (IOS 12.2(33)SXI), Sup32/Sup720,
- agregační přepínače Cisco Catalyst 3560/3750 (IOS 12.2(55)SE),
- přístupové přepínače Cisco Catalyst 2960 (IOS 12.2(55)SE),
- přístupové přepínače Cisco Catalyst 2950 (nijak nepodporují IPv6).
- WiFi moduly - Cisco WiSM + Cisco Aironet 1121/1131/1231/1242/1252.

HW/SW vybavení síťových prvků

- Celkově přes 600 aktivních prvků,
- hraniční směrovače Cisco ASR1000,
- L3 přepínače Cisco Catalyst 6500 (IOS 12.2(33)SXI), Sup32/Sup720,
- agregační přepínače Cisco Catalyst 3560/3750 (IOS 12.2(55)SE),
- přístupové přepínače Cisco Catalyst 2960 (IOS 12.2(55)SE),
- přístupové přepínače Cisco Catalyst 2950 (nijak nepodporují IPv6).
- WiFi moduly - Cisco WiSM + Cisco Aironet 1121/1131/1231/1242/1252.

HW/SW vybavení síťových prvků

- Celkově přes 600 aktivních prvků,
- hraniční směrovače Cisco ASR1000,
- L3 přepínače Cisco Catalyst 6500 (IOS 12.2(33)SXI), Sup32/Sup720,
- agregační přepínače Cisco Catalyst 3560/3750 (IOS 12.2(55)SE),
- přístupové přepínače Cisco Catalyst 2960 (IOS 12.2(55)SE),
- přístupové přepínače Cisco Catalyst 2950 (nijak nepodporují IPv6).
- WiFi moduly - Cisco WiSM + Cisco Aironet 1121/1131/1231/1242/1252.

HW/SW vybavení síťových prvků

- Celkově přes 600 aktivních prvků,
- hraniční směrovače Cisco ASR1000,
- L3 přepínače Cisco Catalyst 6500 (IOS 12.2(33)SXI), Sup32/Sup720,
- agregační přepínače Cisco Catalyst 3560/3750 (IOS 12.2(55)SE),
- přístupové přepínače Cisco Catalyst 2960 (IOS 12.2(55)SE),
- přístupové přepínače Cisco Catalyst 2950 (nijak nepodporují IPv6).
- WiFi moduly - Cisco WiSM + Cisco Aironet 1121/1131/1231/1242/1252.

HW/SW vybavení síťových prvků

- Celkově přes 600 aktivních prvků,
- hraniční směrovače Cisco ASR1000,
- L3 přepínače Cisco Catalyst 6500 (IOS 12.2(33)SXI), Sup32/Sup720,
- agregační přepínače Cisco Catalyst 3560/3750 (IOS 12.2(55)SE),
- přístupové přepínače Cisco Catalyst 2960 (IOS 12.2(55)SE),
- přístupové přepínače Cisco Catalyst 2950 (nijak nepodporují IPv6).
- WiFi moduly - Cisco WiSM + Cisco Aironet 1121/1131/1231/1242/1252.

HW/SW vybavení síťových prvků

- Celkově přes 600 aktivních prvků,
- hraniční směrovače Cisco ASR1000,
- L3 přepínače Cisco Catalyst 6500 (IOS 12.2(33)SXI), Sup32/Sup720,
- agregační přepínače Cisco Catalyst 3560/3750 (IOS 12.2(55)SE),
- přístupové přepínače Cisco Catalyst 2960 (IOS 12.2(55)SE),
- přístupové přepínače Cisco Catalyst 2950 (nijak nepodporují IPv6).
- WiFi moduly - Cisco WiSM + Cisco Aironet 1121/1131/1231/1242/1252.

Bezdrátová síť

- centralizované řešení - dva řídicí moduly WiFi sítě - Cisco WiSM,
- Cisco Aironet 1121/1131/1231/1242/1252,
- 250+ bezdrátových přístupových bodů,
- ve špičkách 1200+ uživatelů on-line,
- problém s RA, řešeno detekcí a zneplatňováním RA/směrovačů (RAMON/RAFIX),
- podpora IPv6 je rozvíjena v novějších modulech postavených na řadách 5500.

Monitoring počítačové sítě

- open-source produkt Nagios,
- Nagios moduly obvykle podporují IPv6,
- kontrola služeb je nutná pro IPv4 i IPv6 (monitorujeme služby web serveru, tedy dvě služby - např. HTTP a HTTP6),
- je vhodné sledovat výkonnostní charakteristiky služby na obou protokolech.

Google: zkušenosti s IPv6 přístupem

- většina Google služeb je dostupná po IPv6,
- založeno na poskytování AAAA záznamům domluveným IPv4/6 sítím,
- nutno se s Google domluvit (viz http://www.google.com/ipv6),
- cca 1.5 roku v podstatě bez problémů,
- kvalitativně je přístup přes IPv4/6 shodný,
- dobrá a okamžitá indikace problémů s IPv6 („vše mi jde, jen YouTube ne“).

Provozní problémy

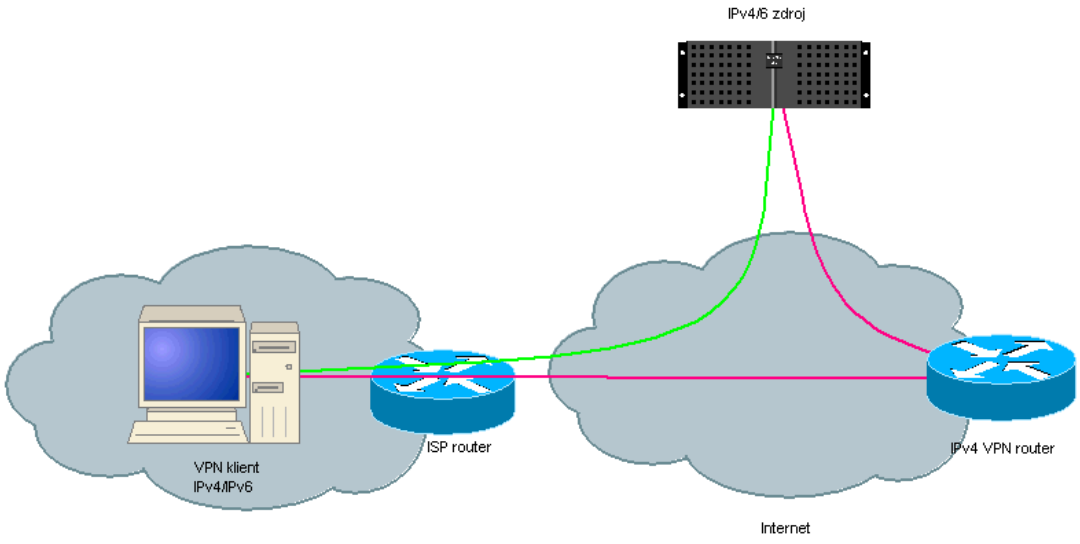
- automaticky navazované tunely
  - horší konektivita (propustnost, latence),
  - problémy s filtrací provozu, odesíláním pošty, atd.

- virtualizované systémy koncových stanic
  - často používají technologie NAT,
  - nemají možnost získat nativní IPv6 konektivitu,
  - navazují se tunely (nerealizuje se ISATAP, nemají doménu vsb.cz),

Provozní problémy

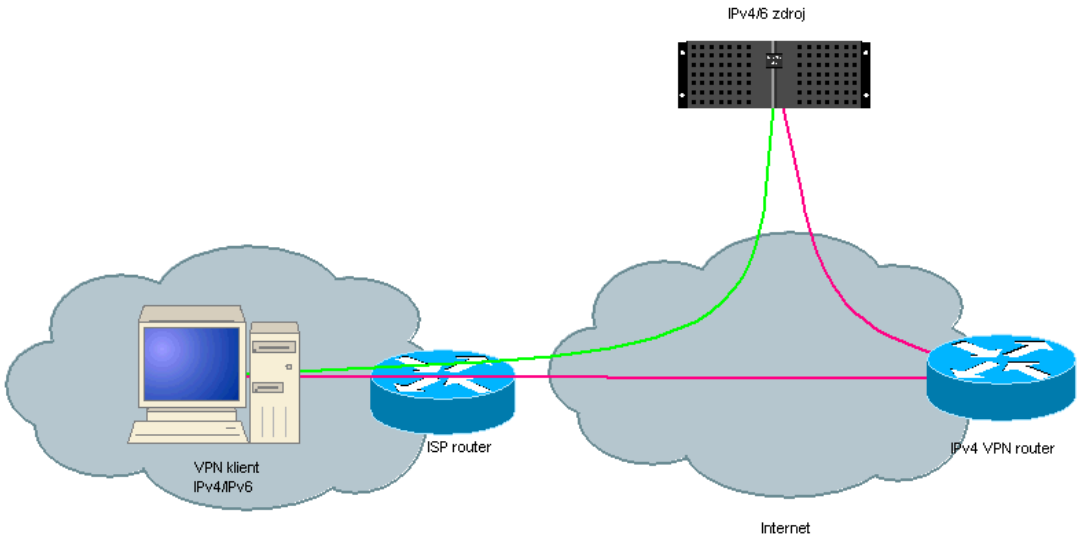
- automaticky navazované tunely
  - horší konektivita (propustnost, latence),
  - problémy s filtrací provozu, odesíláním pošty, atd.
- virtualizované systémy koncových stanic
  - často používají technologie NAT,
  - nemají možnost získat nativní IPv6 konektivitu,
  - navazují se tunely (nerealizuje se ISATAP, nemají doménu vsb.cz),

Provozní problémy II. - VPN



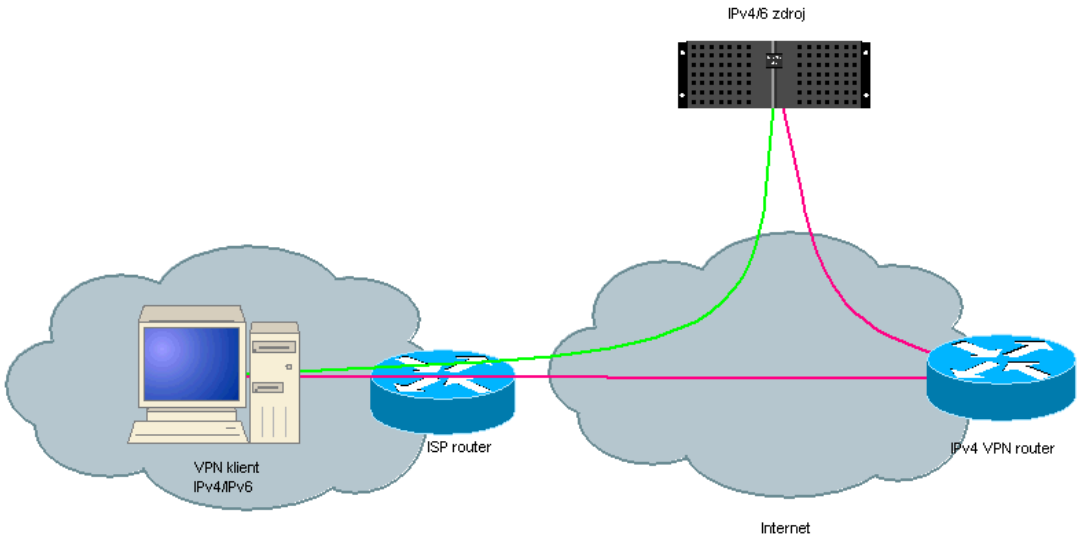
- zdánlivá bezpečnost - jsem připojen přes VPN,
- nutná podpora na straně VPN serverů i klientů,
- v současné době testujeme SSL VPN Cisco řešení.

Provozní problémy II. - VPN



- zdánlivá bezpečnost - jsem připojen přes VPN,
- nutná podpora na straně VPN serverů i klientů,
- v současné době testujeme SSL VPN Cisco řešení.

Provozní problémy II. - VPN



- zdánlivá bezpečnost - jsem připojen přes VPN,
- nutná podpora na straně VPN serverů i klientů,
- v současné době testujeme SSL VPN Cisco řešení.

Provozní problémy III.

- bezpečnostní mechanismy nejsou na úrovni IPv4
  - RA Guard (RFC 6105),
  - funkcionalita firewallů,
- funkční problémy
  - DHCPv6 a SLAAC,
  - neexistující DHCPv6 klienti v mnoha distribucích OS,
  - i pokud je DHCPv6 klient, stejně jsou použity i SLAAC adresy,
  - je třeba myslet na to, že směrovače a DNS servery nejsou v DHCPv6 poskytovány,
- další technické i netechnické problémy
  - problémy při výběru vhodných síťových prvků,
  - implementace IPv6 funkcionalit v SW místo HW snižuje výkon,
  - implementace pokročilejších síťových prvků,
  - znalosti technických pracovníků.

Provozní problémy III.

- bezpečnostní mechanismy nejsou na úrovni IPv4
  - RA Guard (RFC 6105),
  - funkcionalita firewallů,
- funkční problémy
  - DHCPv6 a SLAAC,
  - neexistující DHCPv6 klienti v mnoha distribucích OS,
  - i pokud je DHCPv6 klient, stejně jsou použity i SLAAC adresy,
  - je třeba myslet na to, že směrovače a DNS servery nejsou v DHCPv6 poskytovány,
- další technické i netechnické problémy
  - problémy při výběru vhodných síťových prvků,
  - implementace IPv6 funkcionalit v SW místo HW snižuje výkon,
  - implementace pokročilejších síťových prvků,
  - znalosti technických pracovníků.

Provozní problémy III.

- bezpečnostní mechanismy nejsou na úrovni IPv4
  - RA Guard (RFC 6105),
  - funkcionalita firewallů,
- funkční problémy
  - DHCPv6 a SLAAC,
  - neexistující DHCPv6 klienti v mnoha distribucích OS,
  - i pokud je DHCPv6 klient, stejně jsou použity i SLAAC adresy,
  - je třeba myslet na to, že směrovače a DNS servery nejsou v DHCPv6 poskytovány,
- další technické i netechnické problémy
  - problémy při výběru vhodných síťových prvků,
  - implementace IPv6 funkcionalit v SW místo HW snižuje výkon,
  - implementace pokročilejších síťových prvků,
  - znalosti technických pracovníků.

Konec...

Díky za pozornost.

Dotazy?