Tunelování pomocí 6to4 a Teredo – po roce

Jaromír Talíř / *jaromir.talir@nic.cz*
8.6.2011
Internet a Technologie 2011

CZ DOMAIN REGISTRY

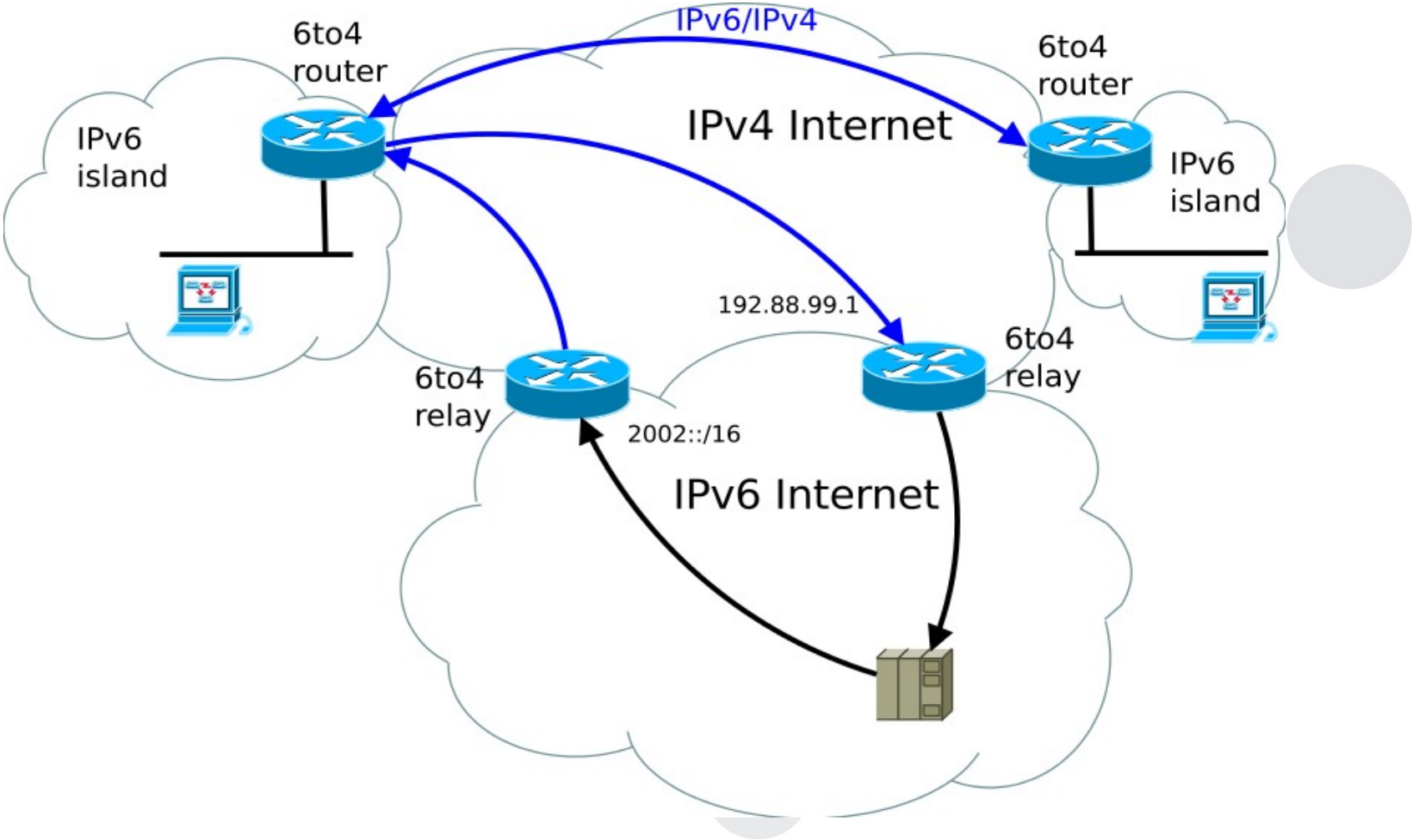
Obsah

- 6to4
- Teredo
- Grafy toků
- Zkušenosti z provozu
- Bezpečnost
- Problémy
- Aktuálně z IETF

6to4

- Definováno v RFC3056 a RFC3068 (rok 2001)
- IPv6 datagramy baleny do IPv4 datagramu typu 41
- Dedikovaný IPv6 adresní prostor – 2002::/16
  - Vložena IPv4 adresa hraničního routeru - 2002:V4ADDR::/48
- Komunikace s nativní IPv6 pomocí relay
  - Anycastová adresa 192.88.99.1 pro 6to4 -> nativní IPv6
  - 2002::/16 pro nativní IPv6 -> 6to4
- Jednoduchá aktivace
  - Některé verze Windows nastaví automaticky
  - V Linuxu i MacOS pár příkazů

6to4


6to4
router
IPv6/IPv4
6to4
router
IPv4 Internet
IPv6
island
IPv6
island
192.88.99.1
6to4
relay
6to4
relay
2002::/16
IPv6 Internet

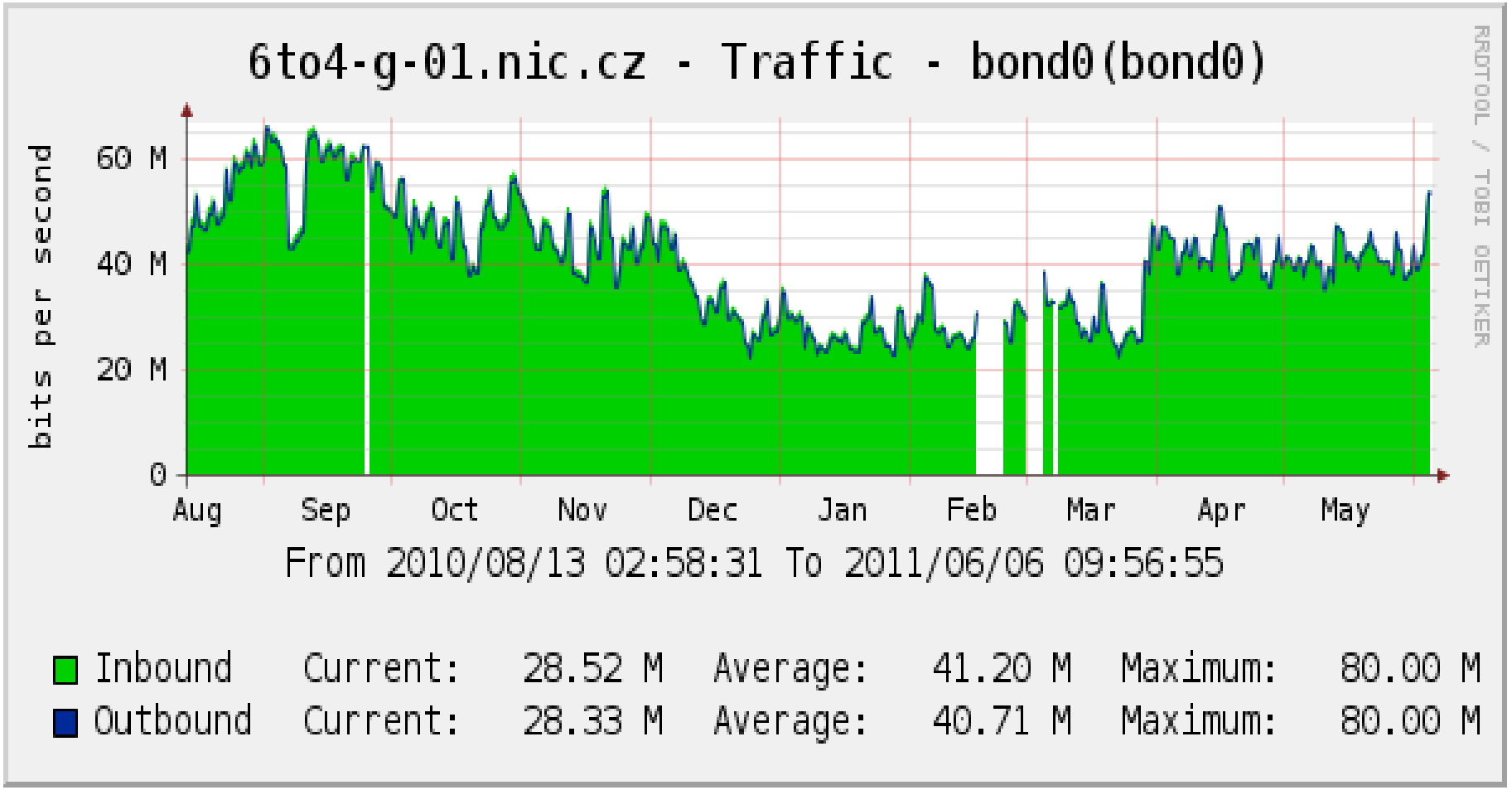
Teredo

- Definováno v RFC 4380 (rok 2006)
- IPv6 datagramy baleny do IPv4 jako UDP pakety
- Dedikovaný IPv6 adresní prostor – 2001::/16
  - V IPv6 adrese jsou obsaženy – IPv4 adresa Teredo serveru, IPv4 adresa a port NATu
- Je nutné nakonfigurovat Teredo server
  - Otevírá cestu v NAT a přiřazuje Teredo adresu
- Pro komunikaci s nativním Ipv6 se opět použije libovolný Teredo relay propagující prefix 2001::/16
- Jednoduchá aktivace
  - V některých Windows zapnuto automaticky pokud je detekována privátníIPv4
  - V Linuxu a MacOS je třeba nainstaloval software Miredot

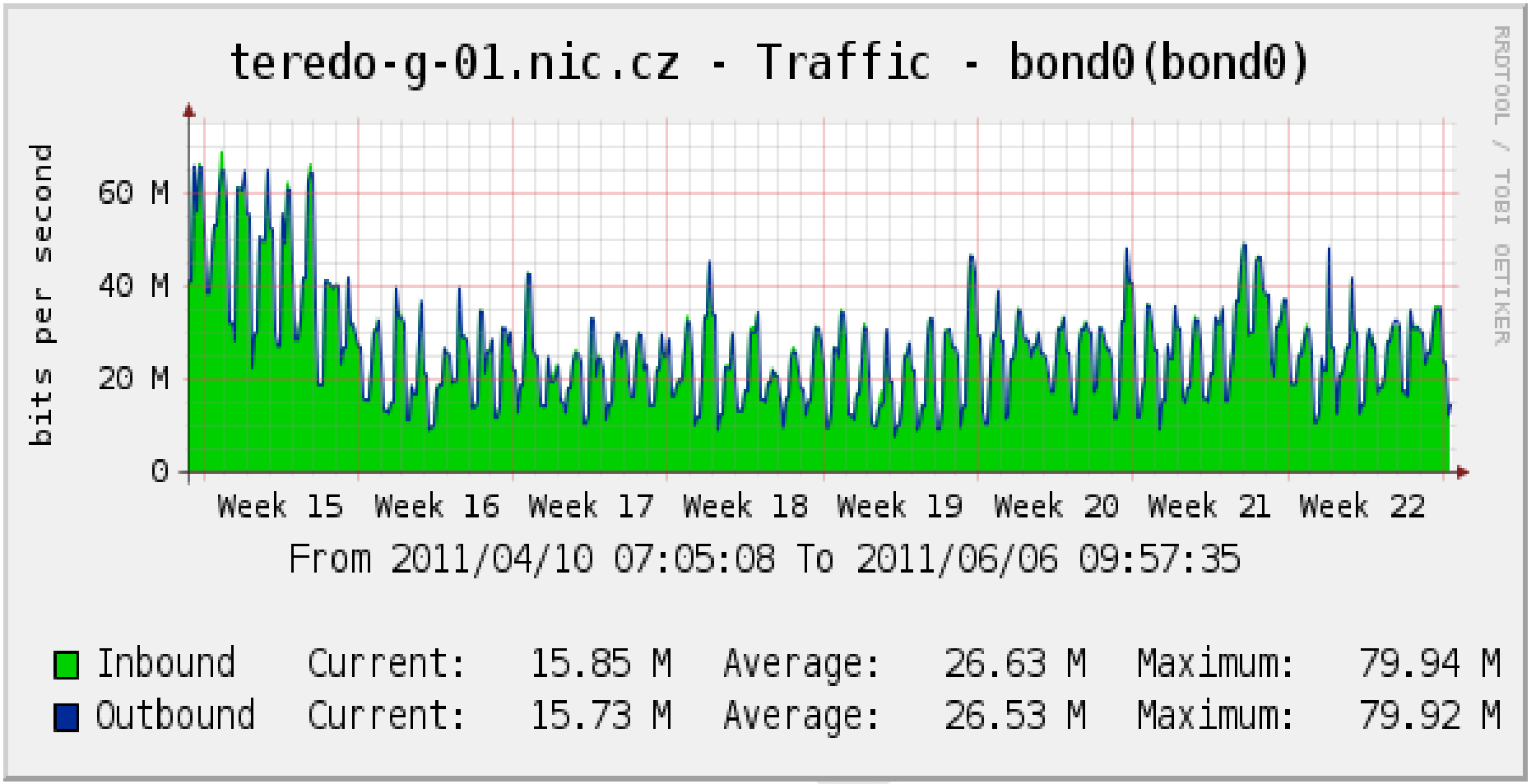
Podpora ze strany CZ.NIC

- Zrychlení připojení uživatelům 6to4 a Teredo
- Dříve existovali překladové server (relay) pouze v zahraničí
- Červen 2010
  - 6to4 relay
- Duben 2011
  - Teredo server
  - Teredo relay

6to4 provoz


6to4-g-01.nic.cz - Traffic - bond0(bond0)
bits per second
60 M
40 M
20 M
0
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
From 2010/08/13 02:58:31 To 2011/06/06 09:56:55
Inbound Current: 28.52 M Average: 41.20 M Maximum: 80.00 M
Outbound Current: 28.33 M Average: 40.71 M Maximum: 80.00 M
RRDTOOL / TOBI OETIKER

Teredo provoz



Zkušenosti z provozu

- Virtualizované řešení nefungovalo spolehlivě
- Fyzický HP server se starou verzí Broadcom síťové karty také nefungoval spolehlivě
- Finální konfigurace
  - HP ProLiant DL360 G5, 4GB RAM, Intel Xeon 1.6GHz
  - Ubuntu Lucid + BIRD routing demon
- Shaping není nutný – toky jsou malé, existuje limit HW
- 1.dubna masivní nárůst toků
  - Vypnutí jedné zatížené relay a přesměrování na nás
  - Zastavení propagace do jednoho upstreamu

Bezpečnost

- Pokud je tunel vytvořen bez vědomí správce sítě, může tím být porušena bezpečnostní politika.
- Je nutné dbát na správné nastavení firewallu i pro IPv6
- RFC3964 - Security Considerations for 6to4
  - Zabývá se zejména možným zneužitím pomocí podvržení adres v 6to4 komunikaci a doporučuje sérii kontrol
  - Kontrolování použití privátních či jinak nepovolených IPv4 adres v 6to4 adresách
  - Kontrolování zdrojových a cílových adres datagramů, které odporují standardním způsobám 6to4 komunikace

Problémy 6to4

- PMTUD – Path MTU Discovery
  - Standardní MTU 1500 se tunelováním snižuje na 1480
  - V případě PPP protokolu ještě na 1472
  - Některé implementace PMTUD (Ubuntu 8.08 LTS) si s tím nedokáží poradit
- Filtrováni protokolu 41
  - Některé firewally po cestě odmítají tento protokol propustit
- Studie Geoffa Hustona – 13% 6to4 spojení neprojde
  - Prosinec 2010
  - http://www.potaroo.net/ispcol/2010-12/6to4fail.html

Aktuálně z IETF

- Pracovní skupina v6ops na IET80 na konci května v Praze publikovala dva nové drafty
- draft-ietf-v6ops-6to4-advisory-01
  - Rekapituluje všechny problémy 6to4 a některá řešení jak se jim vyhnout
- draft-ietf-v6ops-6to4-to-historic-04
  - Navrhuje obě RFC týkající se 6to4 přesunout do “historického” stavu
  - IPv6 zařízení by měli chápat 6to4 jako poslední možný způsob pro IPv6 konektivitu
  - IPv6 zařízení by nikdy neměli zapínat 6to4 automaticky

Závěr

- Automatické tunelovací technologie jsou velmi jednoduchou cestou jak si pořídit IPv6 připojení
- Jejich spolehlivost nelze dost dobře garantovat
- Jako alternativu pro ISP je možné použít 6rd
  - Obecný prefix 2001::/16 je nahrazen IPv6 prefixem vlastněným tímto ISP
- Spolehlivost zajistí jen plný dual stack

Otázky?

http://www.nic.cz
jaromir.talir@nic.cz