Silicon Hill

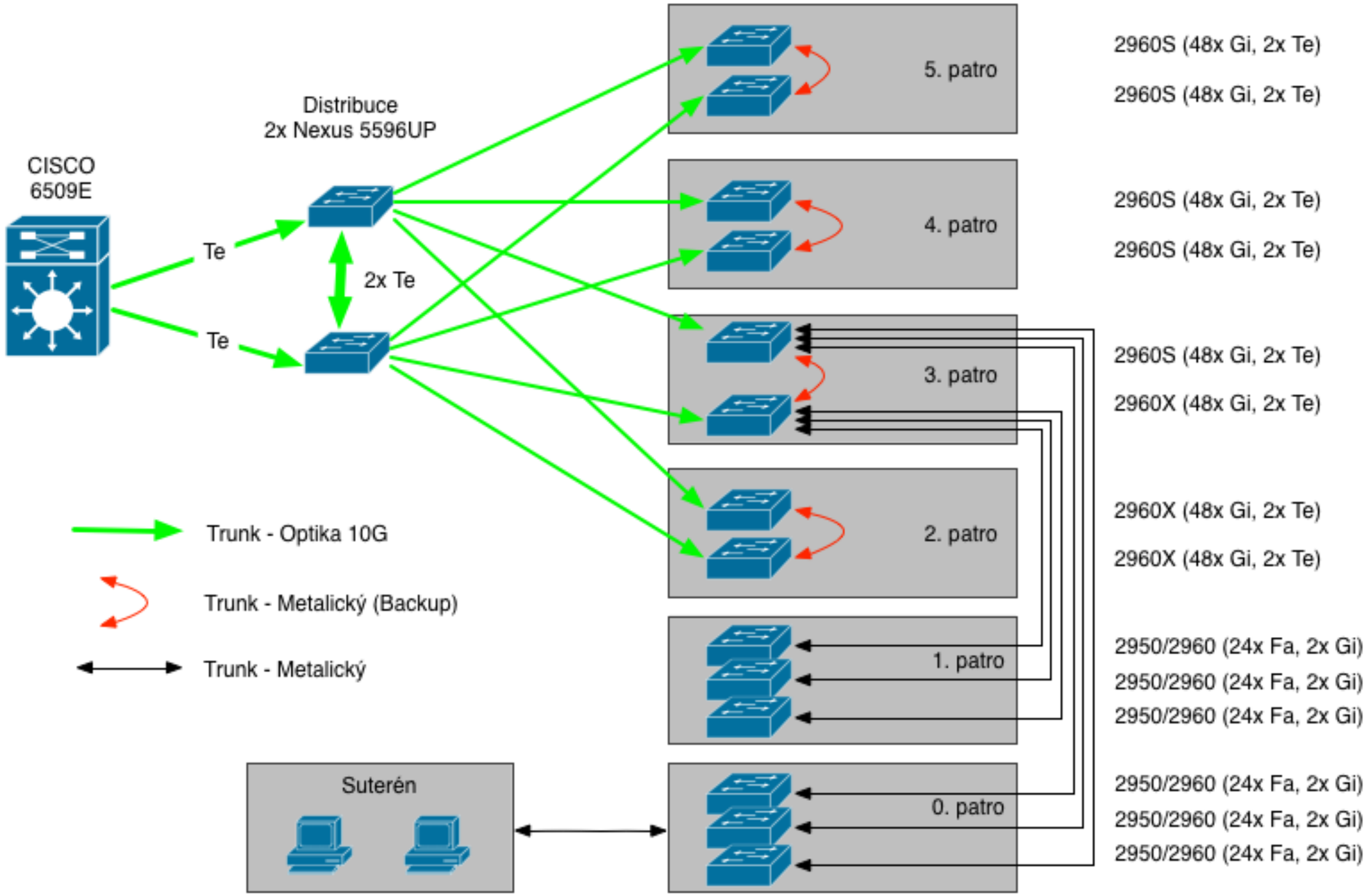
IPv6 na Strahově

Bronislav Robenek, 1. Březen 2014

Silicon Hill

- Největší a zakládající klub SU ČVUT (1998)
- Členské příspěvky
- Největší studenty spravovaná síť
- ~ 4000 členů
  ~ 4000 zařízení
  ~ 150 aktivních členů

Síť leden 2014



IPv4 řešení

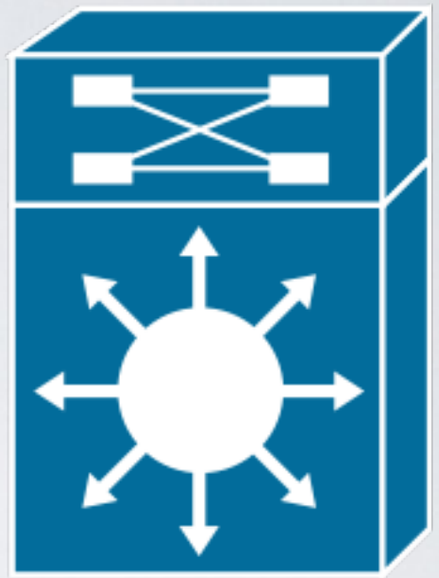
- Staticky přidělované IP adresy uživatelům
- Na portech
  - MAC port security
  - IP access list (anti-spoofing)
  - DHCP Snooping
- Pro uživatele:
  - DHCP dle MAC (PostgreSQL), DHCP Relay
  - Statické nastavení

IPv4 Konfigurace portu

```
 1 interface GigabitEthernet1/0/15
 2  description 515A
 3  switchport access vlan 61
 4  switchport mode access
 5  switchport port-security
 6  switchport port-security mac-address 00##.####.d622
 7  ip access-group ACL-Gi1/0/15 in
 8  no cdp enable
 9  spanning-tree portfast
10  spanning-tree bpduguard enable
11 end
12
13 Standard IP access list ACL-Gi1/0/15
14     10 permit 0.0.0.0
15     20 permit 147.32.116.56
16     30 deny   any
```

IPv4		IPv6
2^32 0.0.0.0 až 255.255.255.255	→	2^128 :: až ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Unicast, Multicast, Anycast	→	Unicast, Multicast, Anycast
Broadcast	→	**N/A**
Link-local adresy 169.254.1.0 - 169.254.254.255	→	Link-local adresy ff80::/10
RFC1918 priv. internet 172.16/12, 10/8, 192.168/16	→	RFC4193 ULA fc00::/7
ICMP, IGMP	→	ICMPv6
DNS A	→	DNS AAAA
DHCP (Broadcast)	→	DHCPv6 (**Multicast**)
ARP (Broadcast)	→	NDP (**Multicast**)

Router advertisement (RA)



- Router Link-local address
- Prefix sítě (/64)
- Managed config flag (DHCPv6)
- Other config flag (Stateless DHCPv6)

```
1  interface Vlan61
    ...
3   ipv6 address 2001:718:2:61::1/64
4   ipv6 nd prefix 2001:718:2:61::/64 7200 3600 no-autoconfig
5   ipv6 nd managed-config-flag
6   ipv6 nd other-config-flag
7   ipv6 nd router-preference High
```

Přiřazování adres

- **SLAAC** (Stateless address auto configuration)
  - EUI-64 -> Prefix “+” MAC
  - Temporary address -> Prefix “+” rand()
- **DHCPv6**
  - Multicast adresa serverů [ff02::1:2]
  - Request neobsahuje MAC adresu, ale DUID!
  - Nelze nastavit default gateway

Autokonfigurace zařízení

	SLAAC	RA	DHCPv6	DHCPv4
Adresa	**ANO***	N/A	**ANO**	**ANO**
Default route	N/A	**ANO**	NE	**ANO**
Nastavení DNS	N/A	RFC6106	**ANO**	**ANO**
DHCP Options	N/A	N/A	**ANO**	**ANO**

Naše požadavky

- Nasazení nemá zasáhnout uživatele
- Fail-safe podpora zařízení
- L3 bezpečnost (Identifikace uživatelů)
- Jednotná správa s IPv4

IPv6 řešení

- Staticky přidělované IP adresy uživatelům
- Na portech
  - MAC port security
  - IPv6 access list (anti-spoofing)
  - DHCPv6 Guard
- Pro uživatele:
  - DHCPv6 dle MAC (binding z PostgreSQL)
  - Statické nastavení

IPv6 Konfigurace portu

```
 1  interface GigabitEthernet1/0/15
     ...
 8   ipv6 traffic-filter ACLv6-Gi1/0/15 in
 9   ipv6 nd raguard
10   ipv6 dhcp guard attach-policy dhcp-client
     ...
14  end
15
    ...
20
21  IPv6 access list ACLv6-Gi1/0/15
22      permit ipv6 host 2001:718:2:61::5A any sequence 10
23      permit ipv6 FE80::/64 any sequence 20
24      deny ipv6 any any sequence 30
25
```

dhcpy6d

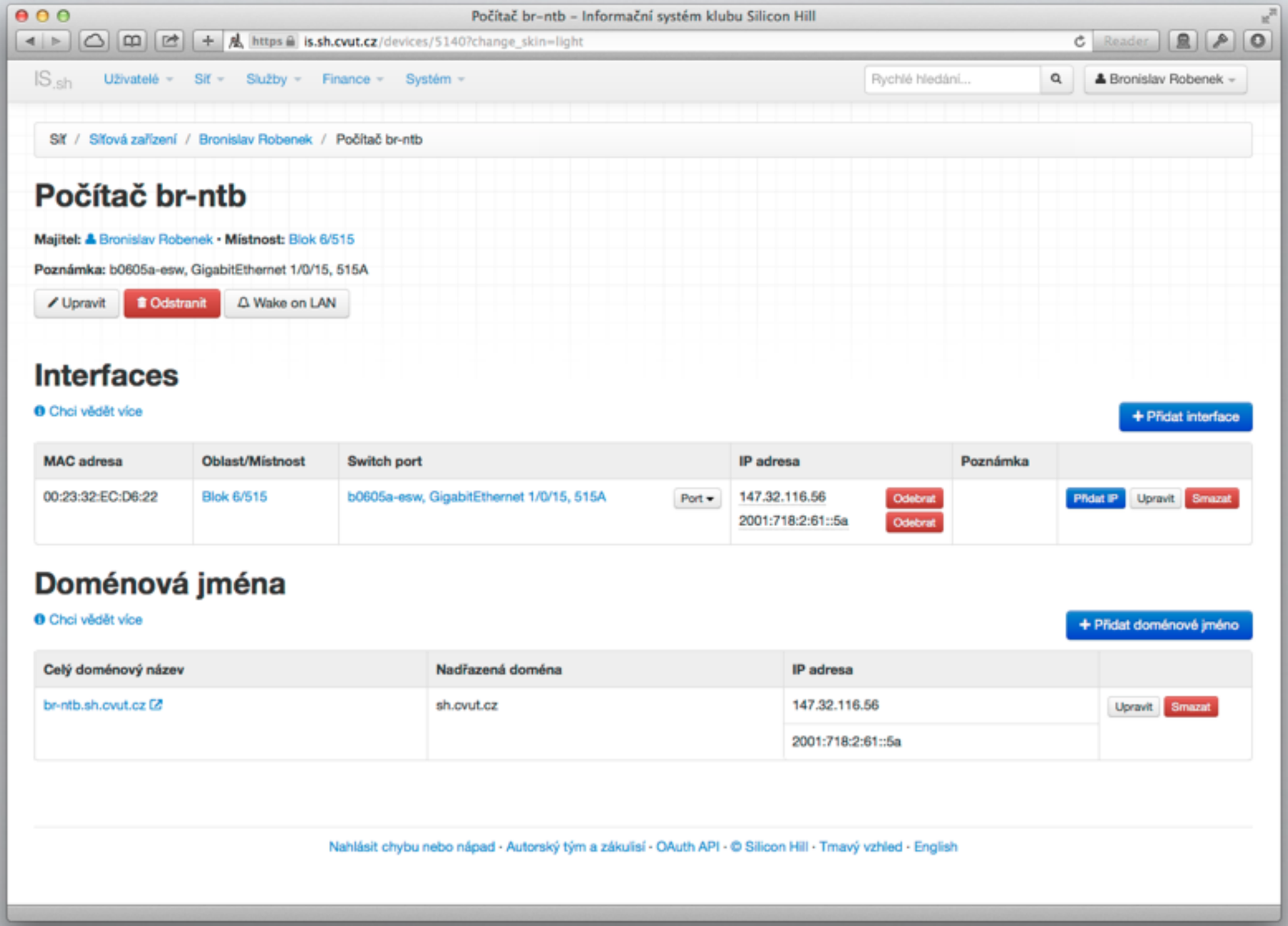
- http://dhcpy6d.ifw-dresden.de

- Static bind only, PostgreSQL https://github.com/brona/dhcpy6d
- IPv6 adresy dle MAC, Hostname, DUID
- Python, 1360 řádků, GPLv2

Jak to funguje?

- Interface v každé z 50 VLAN
- Bind na [ff02::1:2] pro každý interface
- Tabulka: LL adresa <-> MAC adresa
- Pokud LL adresa v request/solicit paketu není v tabulce -> “ping”
  (LL adresa nemusí obsahovat MAC)
- Parsování Neighboor tabulky
  /sbin/ip -6 neigh show

Správa a konfigurace – IS



Závěr

- Pokud zařízení nemá v “ISu” adresu -> nedostane adresu
- Statické ACL -> statické nastavení + nezávislost na IPv6 FHS, případně DHCPv6
- Inkrementální/hezké adresy
- Uživatelé si mohou kdykoliv nechat přiřadit novou adresu

Závěr II.

- Strahováci bezpečně síťují na IPv6
- IPv6 adresy lze přidělovat podle MAC adresy
- Funguje ve většině případů (fail-safe)
- Do budoucna:
  - Fix problémů s FHS na C2960S/X (nelze používat !!!)
  - RFC6939 Client Link-Layer Address Option in DHCP
  - Wi-Fi (Problémy s L3 bezpečností)

Dotazy

Autoři a poděkování

- Bronislav Robenek <b.robenek@sh.cvut.cz>
  (dhcpy6d fork, konfigurace prvků a serveru)
- Vladimír Kincl <v.kincl@sh.cvut.cz>
  (Instalace serveru, skripty pro práci s vlan interface)
- Dominik Mališ <d.malis@sh.cvut.cz>
  (Vývoj Informačního systému klubu SH pro nasazení IPv6)
- Henri Wahl <h.wahl@ifw-dresden.de>
  (dhcpy6d)