

Správa sítí

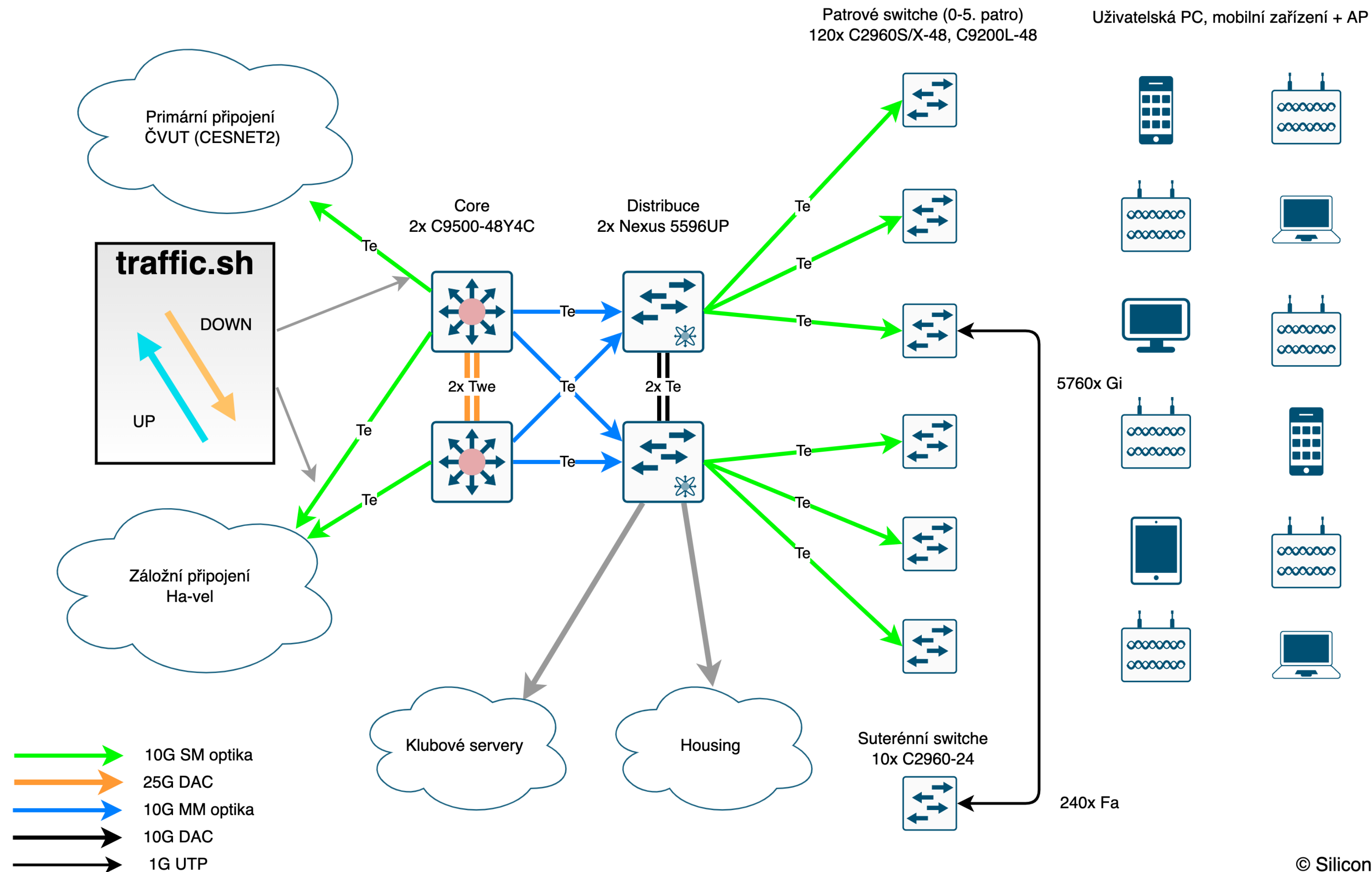
od studentů pro studenty

Jaroslav Zdeněk, 21. 6. 2022

Silicon Hill

- Největší a zakládající klub SU ČVUT (1998)
- Největší studenty spravovaná síť* (začátky v 1993)
 - Doom
- ~3000 členů
- 5760 gigabit access portů
- 385 access pointů (14. 6. 2022)

Fyzická topologie sítě



Logická topologie sítě

- ~90 VLAN, 1 router (Catalyst 9500)
- LAN s veřejnými IPv4 a IPv6 rozsahy
 - ~1,5 /24 per blok + /64 per VLAN
- DHCPv4 + DHCPv6 s identifikací dle MAC
 - RFC 6939
- Port-security + IPv4/v6 ACL FHS (+BCP38)

Ukázka konfigurace portu

```
1. interface TenGigabitEthernet1/0/40
2.   description R4
3.   switchport access vlan 144
4.   switchport mode access
5.   switchport port-security mac-address 30##.####.ff15
6.   switchport port-security
7.   ip access-group ACL-Te1/0/40 in
8.   no cdp enable
9.   ipv6 traffic-filter ACLv6-Te1/0/40 in
10.  no lldp transmit
11.  no lldp receive
12.  spanning-tree portfast
13.  spanning-tree bpduguard enable
14. end

16. Standard IP access list ACL-Te1/0/40
17.   10 permit 0.0.0.0
18.   20 permit 172.16.144.30
19.   30 deny    any

21. IPv6 access list ACLv6-Te1/0/40
22.   permit ipv6 host 2001:718:2:E4::DEAD:BEEF:CAFE any sequence 10
23.   permit ipv6 FE80::/64 any sequence 20
24.   deny ipv6 any any sequence 30
```

WiFi

- Privátní IPv4 + veřejné IPv6 adresy
- IPv6 problém - absence DHCPv6 klienta u jedné platformy
 - => DHCPv4 dle MAC + SLAAC + dot1x accounting
- IoT zařízení ... problém ověřování
 - Menší koleje používají per user VLAN s NATem (neřeší IoT PSK)
 - Kolegové z AGDSN.de implementují SPB-M IP fabriku s PSK na WiFi
 - Strahov: MPSK / iPSK

Sneak peaks

- “desítka” na pokoj :)))
 - Koax
 - FTTr
- 10 a 25 Gb pro koncové zařízení
 - Workstations - připojení k NAS storage
 - FTP open-source mirror
- Dante campus-wide compliant network
- Streaming router s LTE zálohou + VPN callhome



Informační systém

- Evidence členů, členských příspěvků
- Konfigurace sítě (fretka)
- DHCPv4, DHCPv6, DNS, 802.1x, TACACS+, SMTP
- OAuth
- Vlastnosti, které usnadní život
 - Detekce portu (DHCP Option 82)
 - Identifikace člena z IP na loginu

Nejčastější zdroje výpadků

historicky - dosud

- Odpojené Tčka
- Došlo místo na disku (DHCP), fretka
- Údržba trafostanice na Karláku, UPS v centrální serverovně (SHapokalypsa)
- switchport trunk allowed vlan 123
 - add :)
- spanning-tree bpdufilter enabled
- Za poslední rok overall uptime SLA ~99.92% (neplánovaných výpadků/odstávek)
- Do prosince předchozí dva roky ~99.999%

Nestandardní situace



Nestandardní situace

- CESNET2 AUP
- Sdílení účtů / routery - neevidované cizí zařízení
 - -> Odpojení od sítě (ban)
- Stížnosti směrem k děkanům fakult, studijní oddělení...
- Ambasády...

Q&A

demo?

Děkuji za pozornost