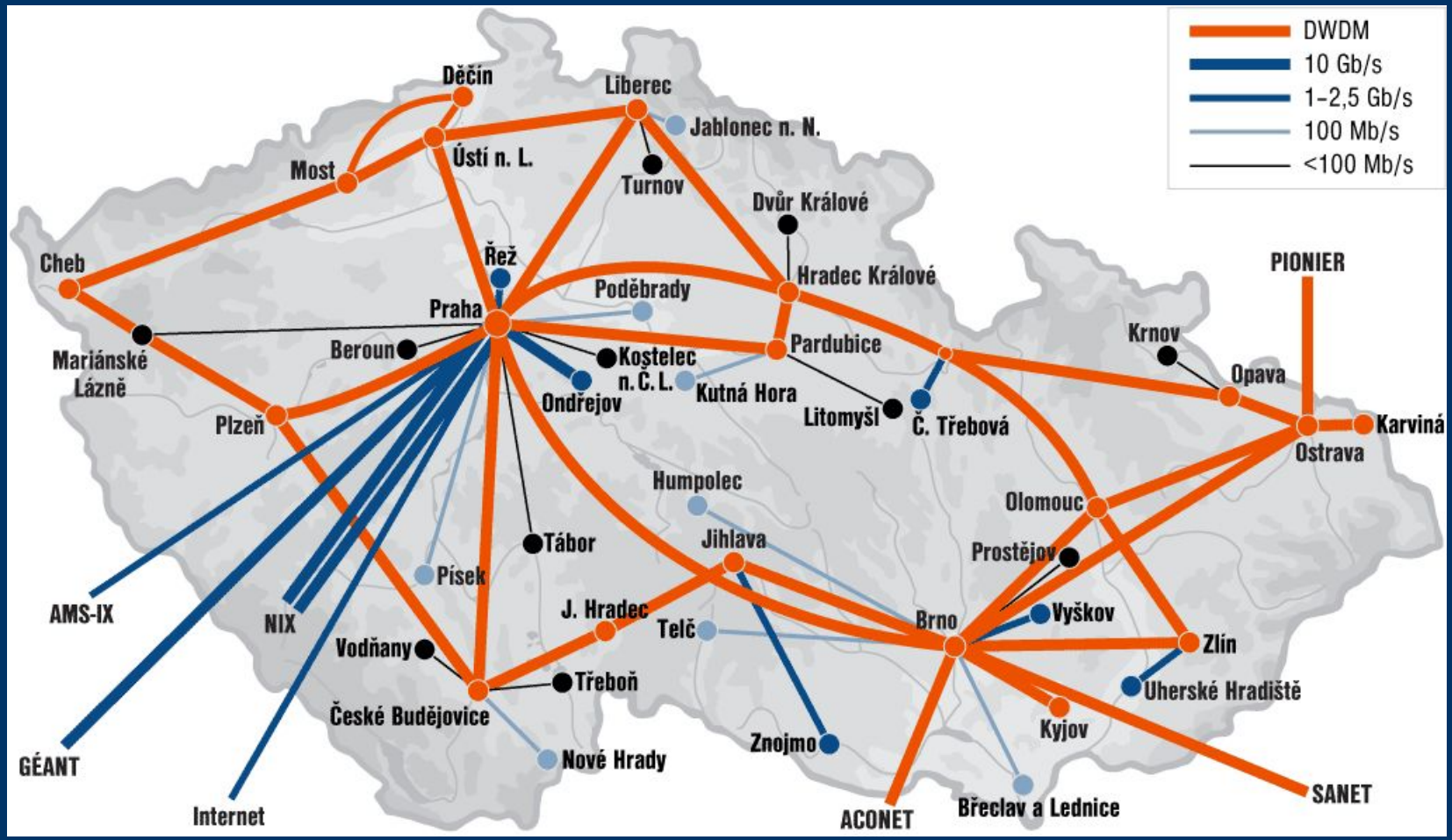
Jak funguje SH Síť

Ondřej Caletka
o.caletka@sh.cvut.cz
http://shell.sh.cvut.cz/~oskar

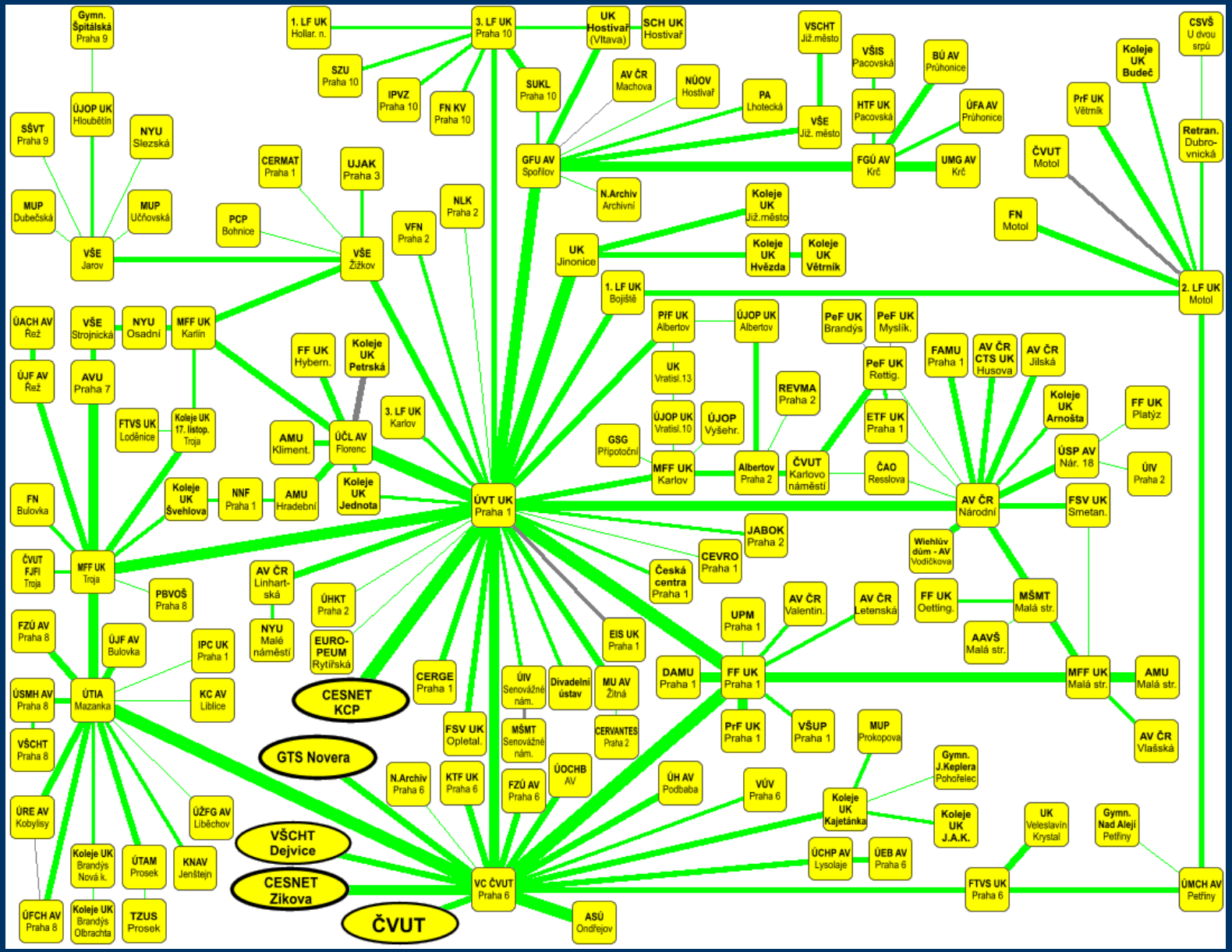
Osnova

- Mapy sítí
- Topologie
- IP adresy, VLANy
- DUSPS
- Účty na serverech, přístupy
- Zabezpečení – Port Security
- NAT a IPv6
- Pošta
- Multicast

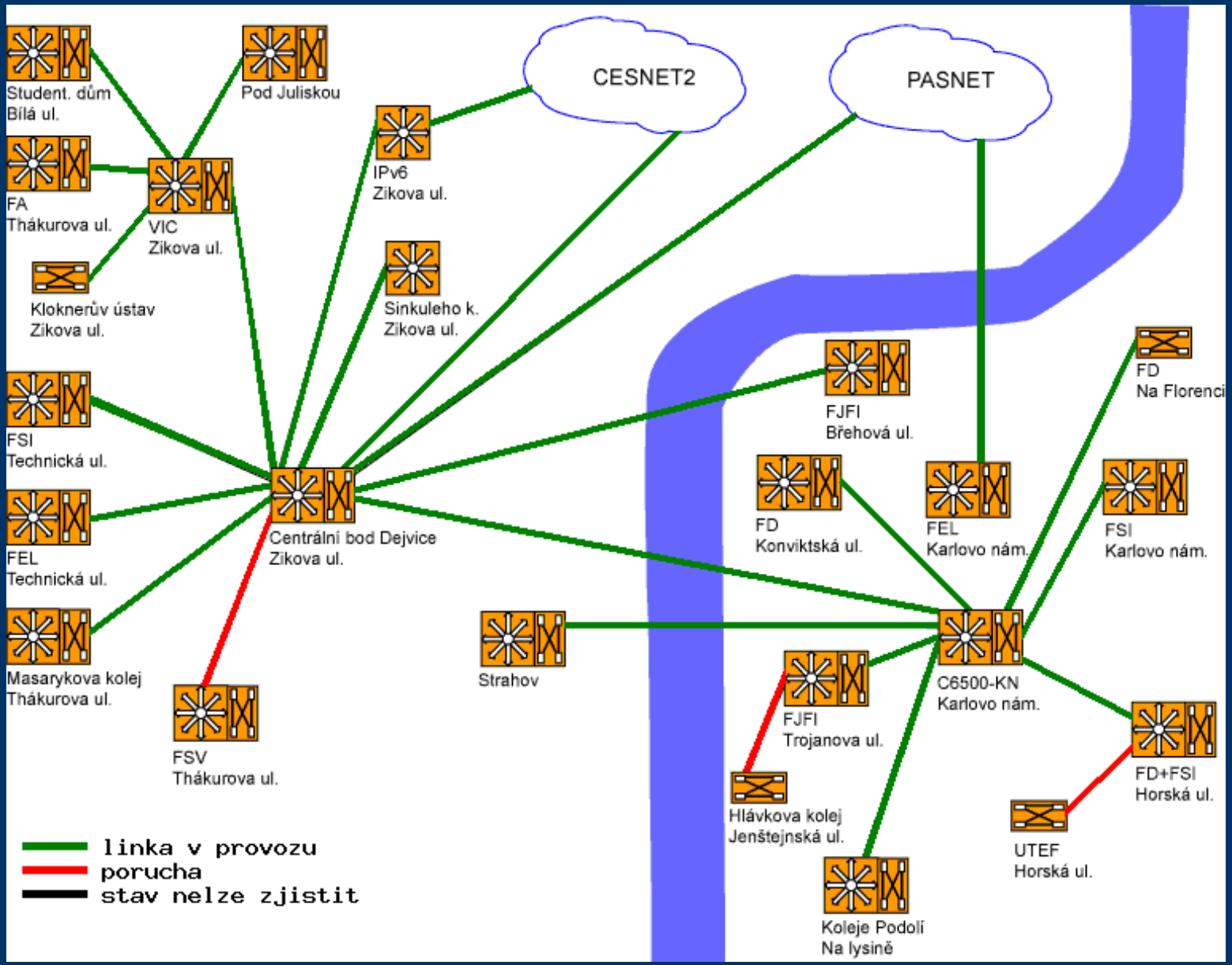
Mapa sítě CESNET



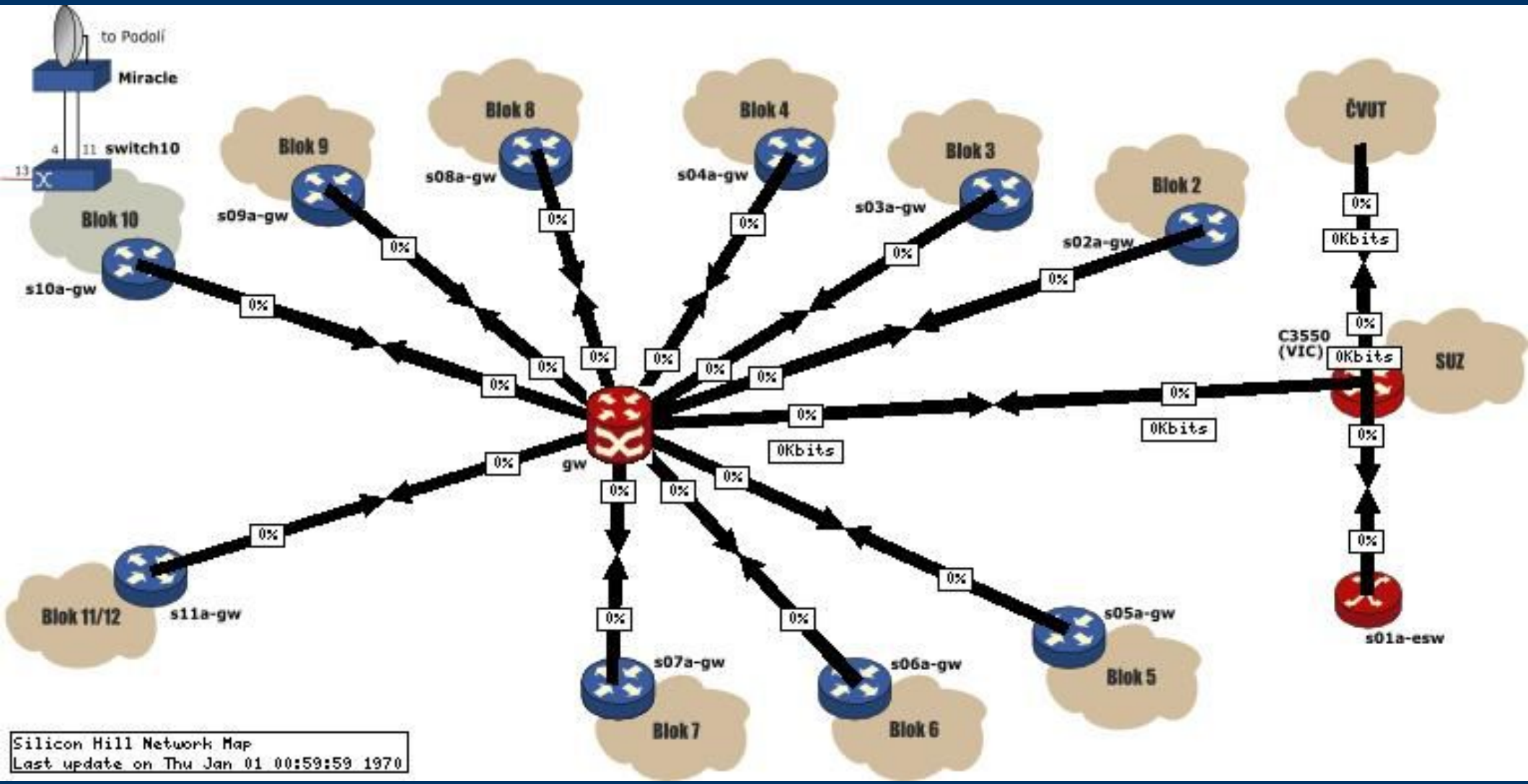
Mapa PASNET


Gymn. Špitálská Praha 9
1. LF UK Hollar. n.
3. LF UK Praha 10
UK Hostivař (Vltava)
SCH UK Hostivař
VSCHT Již.město
VŠIS Pacovská
BÚ AV Průhonice
CSVŠ U dvou srpů
Koleje UK Budeč
SZU Praha 10
IPVZ Praha 10
FN KV Praha 10
SUKL Praha 10
AV ČR Machova
NÚOV Hostivař
PA Lhotecká
VŠE Již. město
HTF UK Pacovská
ÚFA AV Průhonice
PrF UK Větrník
ÚJOP UK Hloubětín
SŠVT Praha 9
NYU Slezská
GFU AV Spořilov
FGÚ AV Krč
UMG AV Krč
ČVUT Motol
Retran. Dubrovnická
CERMAT Praha 1
UJAK Praha 3
N.Archiv Archivní
MUP Dubečská
MUP Učňovská
PCP Bohnice
NLK Praha 2
VFN Praha 2
Koleje UK Již.město
FN Motol
UK Jinonice
Koleje UK Hvězda
Koleje UK Větrník
VŠE Jarov
VŠE Žižkov
1. LF UK Bojiště
2. LF UK Motol
ÚACH AV Řež
VŠE Strojnická
NYU Osadní
MFF UK Karlín
PřF UK Albertov
ÚJOP UK Albertov
PeF UK Brandýs
PeF UK Myslík.
FF UK Hybern.
Koleje UK Petrská
UK Vratisl.13
PeF UK Rettig.
FAMU Praha 1
AV ČR CTS UK Husova
AV ČR Jilská
ÚJF AV Řež
AVU Praha 7
REVMA Praha 2
Koleje UK Arnošta
FF UK Platýz
FTVS UK Loděnice
Koleje UK 17. listop. Troja
3. LF UK Karlov
AMU Kliment.
ÚČL AV Florenc
ÚJOP UK Vratisl.10
ÚJOP Vyšehr.
ETF UK Praha 1
ÚSP AV Nár. 18
ÚIV Praha 2
GSG Přípotoční
MFF UK Karlov
Albertov Praha 2
ČVUT Karlovo náměstí
ČAO Resslova
FN Bulovka
Koleje UK Švehlova
NNF Praha 1
AMU Hradební
Koleje UK Jednota
ÚVT UK Praha 1
AV ČR Národní
FSV UK Smetan.
JABOK Praha 2
Wiehlův dům - AV Vodičkova
ČVUT FJFI Troja
MFF UK Troja
PBVOŠ Praha 8
AV ČR Linhart-ská
ÚHKT Praha 2
NYU Malé náměstí
EURO-PEUM Rytířská
Česká centra Praha 1
CEVRO Praha 1
UPM Praha 1
AV ČR Valentin.
AV ČR Letenská
FF UK Oetting.
MŠMT Malá str.
AAVŠ Malá str.
FZÚ AV Praha 8
ÚJF AV Bulovka
IPC UK Praha 1
EIS UK Praha 1
DAMU Praha 1
FF UK Praha 1
MFF UK Malá str.
AMU Malá str.
ÚSMH AV Praha 8
ÚTIA Mazanka
KC AV Liblice
CESNET KCP
CERGE Praha 1
ÚIV Senovážné nám.
Divadelní ústav
MU AV Žitná
VŠCHT Praha 8
FSV UK Opletal.
MŠMT Senovážné nám.
CERVANTES Praha 2
PrF UK Praha 1
VŠUP Praha 1
MUP Prokopova
AV ČR Vlašská
GTS Novera
N.Archiv Praha 6
KTF UK Praha 6
FZÚ AV Praha 6
ÚOCHB AV
ÚH AV Podbaba
VÚV Praha 6
Gymn. J.Keplera Pohořelec
ÚRE AV Kobylisy
ÚŽFG AV Liběchov
Koleje UK Kajetánka
Koleje UK J.A.K.
VŠCHT Dejvice
Koleje UK Brandýs Nová k.
ÚTAM Prosek
KNAV Jenštejn
UK Veleslavín Krystal
Gymn. Nad Alejí Petřiny
ÚCHP AV Lysolaje
ÚEB AV Praha 6
CESNET Zikova
VC ČVUT Praha 6
FTVS UK Praha 6
ÚMCH AV Petřiny
ÚFCH AV Praha 8
Koleje UK Brandýs Olbrachta
TZUS Prosek
ČVUT
ASÚ Ondřejov

Mapa sítě ČVUT

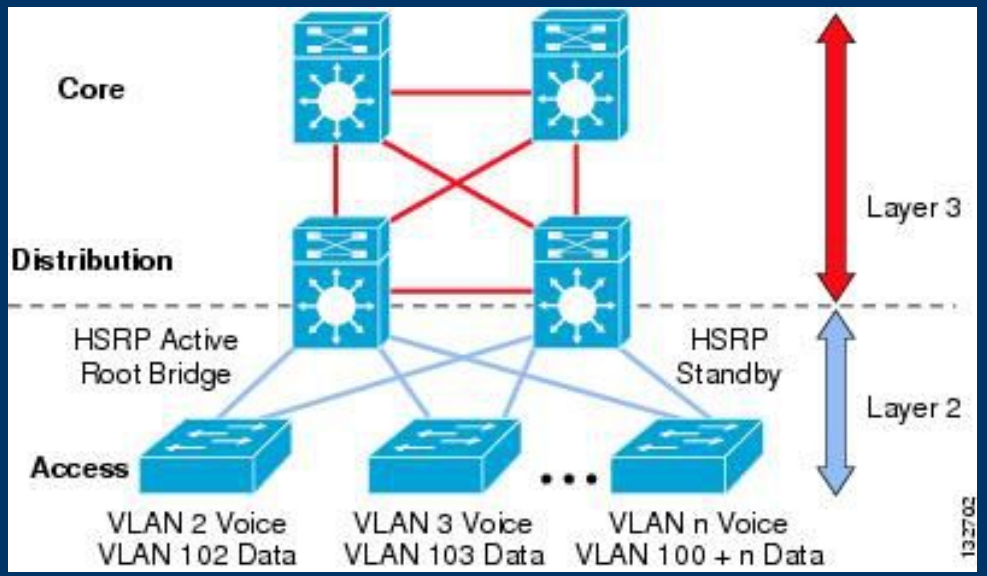


Mapa sítě SH


to Podolí
Miracle
switch10
4
11
13
Blok 10
s10a-gw
Blok 9
s09a-gw
Blok 8
s08a-gw
Blok 4
s04a-gw
Blok 3
s03a-gw
Blok 2
s02a-gw
ČVUT
C3550
(VIC)
SUZ
s01a-esw
gw
Blok 11/12
s11a-gw
s07a-gw
Blok 7
s06a-gw
Blok 6
s05a-gw
Blok 5
0%
0Kbits
Silicon Hill Network Map
Last update on Thu Jan 01 00:59:59 1970

Topologie

- Cisco Hieararchical Network Model
  - bez redundance
  - **Core:** Catalyst 6509 v Centrální serverovně
  - **Distribution:** Catalyst 3750 v blokových serverovnách (místnost číslo 345)
  - **Access:** Catalyst 2950 3× v každém patře
- Optická páteř:
  - 6 párů SM na každý blok
  - Do sítě ČVUT přes blok 1, dále FS na Karlově náměstí, dále VIC Zikova

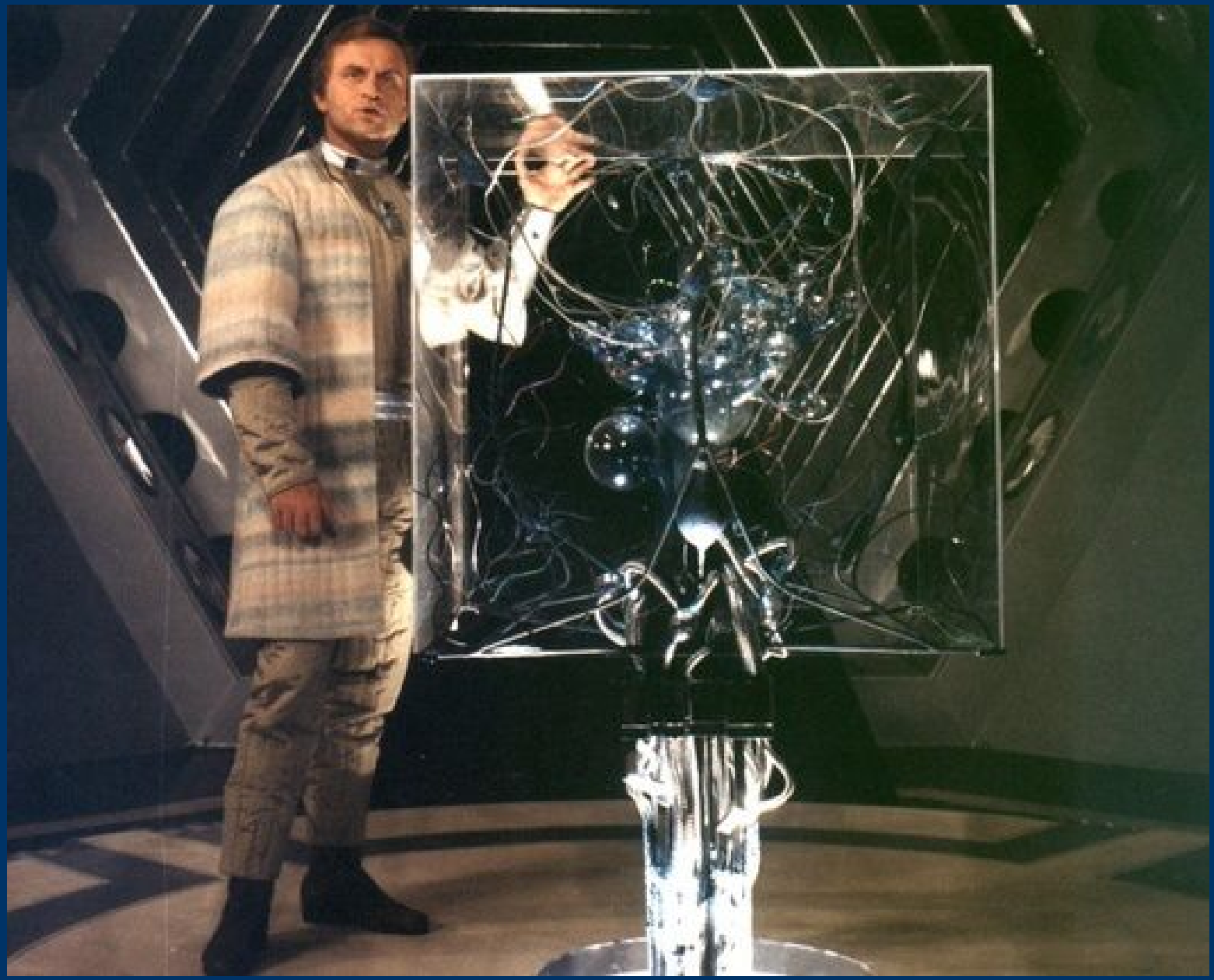


IP adresy, VLANy

- ČVUT: 147.32.*.*, 2001:718:2:...
- SH: 147.32.112-127.*, 147.32.30-31.*, 2001:718:2:00xx:...
- VLAN: Logické sítě s maximálně 253 PC
  - Číslovány v sérii (<č. bloku>*10+n), kde n:
    - 1 – První veřejný rozsah (147.32.110+<č.b.>.*)
    - 2 – Druhý veřejný rozsah (C/2 122-126)
    - 3 – Třetí veřejný rozsah (C/8-C/4 127)
    - 8 – NATovaný rozsah (2C 172.16.<VLAN ID>...)
  - Serverová VLAN ID 6 – 147.32.127.129-253
  - Management VLAN ID 201 – 10.<č.b.>.x.y
  - Housing VLAN ID 40 – 147.32.30.2-126

http://wiki.siliconhill.cz/FAQ/Důležité_IP_adresy_a_servery

DUSPS



DUSPS

- Centrální backend pro evidenci uživatelů
- Současná verze cca. 2002 – PHP, Sybase
  - daleko za svou životností
  - v současné době je dokončován nový
- Automatická evidence plateb
  - e-mailová avíza z banky o došlé platbě
- Automatická konfigurace aktivních prvků
  - Každou hodinu dojde k přepsání konfigurace patrových switchů a blokových L3 switchů
- Automatická konfigurace síťových služeb
  - Každou hodinu si DHCP a DNS servery stáhnou konfigurační soubory

Účty na serverech, přístupy

- Účty na serverech – eviduje DUSPS
  - PERL skript, který se stáhne export, a založí/smaže uživatele.
  - Při založení nastaví default heslo, to si může uživatel změnit.
  - Toto bude brzy minulost, nastoupí LDAP a soustředěná správa uživatelů (podobně, jako má ČVUT usermap.cvut.cz).
- Přístupy do místností
  - Běžné účty v DUSPSu.
  - Aktualizace přístupového systému probíhá ručně
  - Uživatel musí mít platnou kartičku ČVUT, zadané osobní číslo v DUSPS.

Zabezpečení sítě – Port Security

- Na každém portu switche je povolena pouze konkrétní MAC adresa.
  - Jiná MAC vyvolá vypnutí portu, po 30 sekundách restart.
  - Neobsazené porty jsou vypnuté trvale.
  - Také BPDU Guard (Spanning Tree), DHCP Snoop.
- Neobsazené IP adresy jsou filtrovány na blokovém GW.
- Obsazeným adresám je na GW staticky generován ARP záznam.
- => Nelze ukrást cizí IP adresu.

NAT a IPv6

- IPv4 adresy brzy globálně dojdou.
  - Na SH k tomu došlo už kolem r. 2005
  - NAT se pro SH síť poměrně složitě škáluje.
    - Existovala povinnost používat proxy pro port 80.
  - Cca od roku 2004 na SH paralelně funguje IPv6.
    - Problém to ale nevyřešilo, svět na IPv6 nepřešel.
- Konfigurace je fundamentálně odlišná!
  - Používáme automatickou bezestavovou konfiguraci – síť dodá 64b prefix, stanice 64b zbytek.
  - Od roku 2009 se na blokových L3 switchích filtrují pouze povolené IPv6 adresy.

IPv6 – důsledky

- Je potřeba používat IPv6 adresu, jejíchž spodních 64 bitů pochází z MAC adresy
  - Jinak bude IPv6 provoz filtrován a např. návštěva některých webů dlouho trvat.
  - Typický problém u Windows Vista a vyšších.
- Serverové – krátké – IPv6 adresy – spodních 64 bitů odpovídá číselně IPv4 adrese.
  - Je třeba ručně nastavit.
  - Na rozdíl od IPv4 nekonfigurujeme bránu – konfiguruje se automaticky.
- Rozkonfigurované Windows stanice se občas chovají jako IPv6 6to4 routery, naše switche tomu neumí zabránit (RA-guard draft)

Pošta

- Pošta, stejně jako DHCP a DNS běží na serverech service1 a service2, společný název mail.sh.cvut.cz.
- Port 25 (SMTP) je blokován pro přímý přístup.
- Přes mailservery projde jen pošta, jejíž adresa **From:** je registrována v DUSPSu jako uživatelská, nebo externí adresa.
- Kromě toho je možné zařídit si šifrované posílání pošty přes mail.sh.cvut.cz odkudkoli kamkoli – tedy bez vazby na adresu **From:**
- Veškerá pošta z domény SH by měla odcházet z mail.sh.cvut.cz (Sender Policy Framework).

Multicast

- Standard pro šíření dat počítačovou sítí metodou one-to-many
- K duplikaci dochází na aktivních prvcích, nehrozí přetížení centrálního uzlu.
- V globálním Internetu nefunguje, v akademických sítích ano.
- SH Streamy běží na privátních adresách 239.194.10-11.*, jsou filtrovány na gw (6509).
- K funkci je potřeba neblokovat protokol IGMP (stará se o přihlašování a odhlašování skupin).

Závěr

- Díky za pozornost!
- Sledujte SUT!
- Prostor pro dotazy.
- EOF □