Sieť na Fakulte informatiky

PV005 Služby počítačových sítí

Roman Lacko

30. 11. 2022

Fakulta informatiky
Masarykova univerzita
xlacko1@fi.muni.cz

Cieľ prednášky

- opakovanie základných sieťových konceptov a protokolov
- ich aplikácia na Fakulte informatiky MU
- prehľad súvisiacich služieb

Obsah

Úvod

Prehľad siete MU

Masarykova univerzita

- poskytovateľ CESNET

- adresný rozsah **IPv4**: `147.251.0.0/16`
- $\simeq 2^{32-16}$

- adresný rozsah **IPv6**: `2001:718:801::/48`
- $\simeq 2^{128-48}$

- spravuje Ústav Výpočetní Techniky (ÚVT) MU
- časti rozsahu pridelené fakultám a pracoviskám

Prehľad siete MU

Masarykova univerzita

- poskytovateľ CESNET

- adresný rozsah **IPv4**: `147.251.0.0/16`
- $\simeq 2^{32-16} = 65.536$ adries

- adresný rozsah **IPv6**: `2001:718:801::/48`
- $\simeq 2^{128-48}$

- spravuje Ústav Výpočetní Techniky (ÚVT) MU
- časti rozsahu pridelené fakultám a pracoviskám

Prehľad siete MU

Masarykova univerzita

- poskytovateľ CESNET

- adresný rozsah **IPv4**: `147.251.0.0/16`
- $\simeq 2^{32-16} = 65.536$ adries

- adresný rozsah **IPv6**: `2001:718:801::/48`
- $\simeq 2^{128-48} = 1.208.925.819.614.629.174.706.176$ adries

- spravuje Ústav Výpočetní Techniky (ÚVT) MU
- časti rozsahu pridelené fakultám a pracoviskám

Podsiete, VLAN

Podsiete

- rozdelenie rozsahu adries na menšie časti
- *L3 OSI*

Príklad: rozdelenie rozsahu na 4 podsiete

```
147.251.0.0/16

(1) 147.251.0.0/18  (147.251.0.0  - 147.251.63.255)
    (byte C: 00000000 - 00111111)

(2) 147.251.64.0/18 (147.251.64.0 - 147.251.127.255)
    (byte C: 01000000 - 01111111)

...
```

Podsiete, VLAN

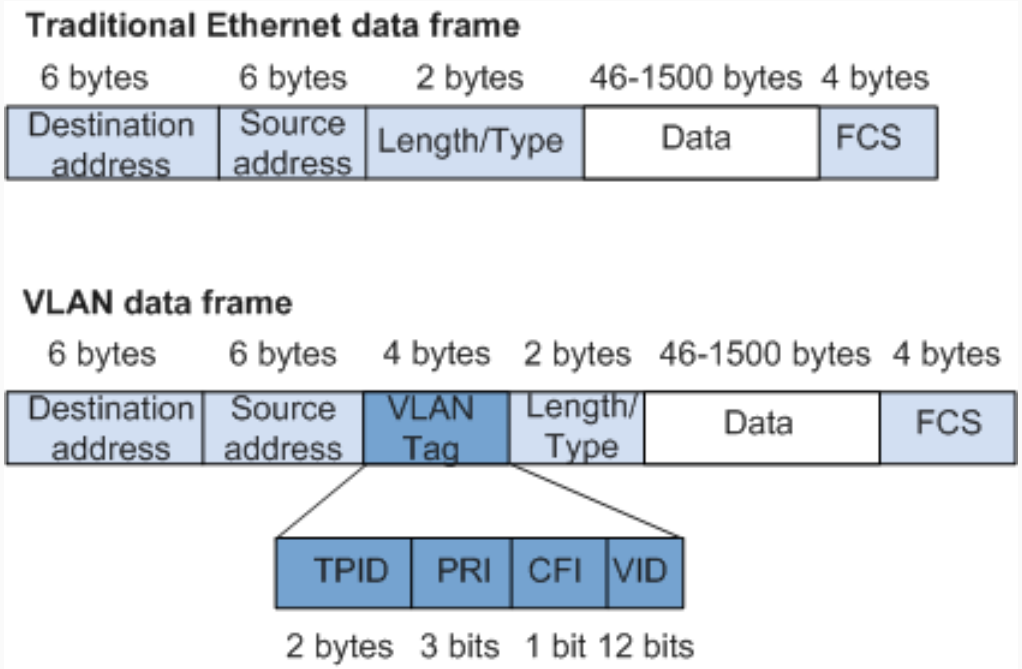
Virtual LAN (`802.1Q`)

- logické rozdelenie siete
- jedna fyzická LAN môže obsahovať viac VLAN
- modifikácia rámcov na vrstve *L2 OSI*

- *access port* $\rightarrow$ *untagged* VLAN
- *trunk port* $\rightarrow$ *tagged* VLAN

✔ robustnejší návrh siete
✔ vyššia bezpečnosť
✘ potrebný *router* na komunikáciu medzi VLAN

Podsiete, VLAN



Podsiete, VLAN

Fakulta informatiky

VLAN 1–9	správa siete, privátne rozsahy, ...
VLAN 43	147.251.43.0/24, wlan_fi
VLAN 44	147.251.44.0/22, Eduroam
VLAN 48	147.251.48.0/24, servery, PC zamestnancov
VLAN 49	147.251.49.0/24, Informačný systém
VLAN 53	147.251.53.0/24, PC učebnenymfe
VLAN 58	147.251.58.0/24, verejné virtuály Stratus.FI
VLAN 300–399	firmy VTP
VLAN 503	172.26.0.0/16, privátne virtuály Stratus.FI

- celkom 64 VLAN

IPv6 konvencia

147.251.N.0/24 (alebo VLAN N) → 2001:718:801:02NN::/64

Sieťová infraštruktúra FI

Router

`ares.fi.muni.cz`

- 16 CPU, 128 GB RAM
- Debian
- 10 GbE a 1 GbE pripojenie (*uplink*)

Router

ares.fi.muni.cz

- 16 CPU, 128 GB RAM
- Debian
- 10 GbE a 1 GbE pripojenie (*uplink*)

Linux ako router?

```
root@ares:~# ip route show
default via 147.251.240.1 dev uplink
...
147.251.48.0/24 dev vlan48  proto kernel  scope link  src 147.251.48.254
...

root@ares:~# ip route add 147.251.42.0/24 via 147.251.42.1 dev eth0
```

Router

ares.fi.muni.cz

- firewall postavený nad `iptables`
- pravidlá pre prístup do podsietí
- predikáty nad paketmi

Aj toto zvládne váš Linux

```
root@ares:~# iptables -A INPUT -d 172.16.14.11 -p tcp --dport http -j ACCEPT
root@ares:~# iptables -A INPUT -p tcp -j REJECT
```

Alternatívne nástroje: `nftables`, `firewalld`, `ufw`, ...

Router

Redundancia

- `ares.fi.muni.cz` je v skutočnosti jedno z
  - `ares1.fi.muni.cz`
  - `ares2.fi.muni.cz`
- *Active-Passive High Availability*
- jeden stroj pracuje, druhý čaká
- informácie o stave cez *heartbeat*

Výpadok

- pasívny stroj nedostáva pulz z aktívneho
- spustí sa *takeover* (v literatúre aj *failover*)
- pasívny stroj prevezme prostriedky a činnost neaktívneho stroja

Router

Prenos prostriedkov a dát

- niektoré služby sa synchronizujú samostatne
- napr. `conntrackd`

Distributed Replicated Block Device (DRBD)

- replikácia disku medzi dvoma strojmi
- zmeny *primárneho* disku sa propagujú medzi ostatné kópie
- pri výpadku sa vyberie iný *primárny* disk
- obsahuje napr. stav `dhcpd`

Switche

Switche

- 6 hlavných
- optické spojenia až 40 GbE
- typ konektora LC, *Multi-Mode* (MM), šírka pásma OM4
- 270× 10 GbE, 10× 40 GbE porty

- 100 distribučných a koncových
- *Category 6A* káble
- 10 GbE porty v serverovniach
- 1 GbE porty v učebniach a kanceláriách

Značky

- HP Comware
- HP ProCurve
- Juniper JunOS

Switche

Správa a nastavenie

- iniciálna manuálna konfigurácia
- *Simple Network Management Protocol* (SNMP)
  monitoring a zmeny

Ďalšie technológie

- *Power over Ethernet* (PoE)
  napájanie menších zariadení (AP, RPi, kamery)
- *DHCP Snooping*
  ochrana siete pred niektorými druhmi DHCP útokov
- *Router Advertisement Guard*
  ekvivalent *DHCP Snooping* pre IPv6

Autentizácia

- *Port-Based Network Access Control* (PNAC, `802.1X`)
- autentizácia počítačov
- obmedzuje prístup neznámym počítačom do podsiete
- využíva sa hlavne v počítačových učebniach
- na pozadí používa RADIUS server

- *Remote Authentication Dial-In User Service* (RADIUS)
- protokol na autentizáciu, autorizáciu a prístup k sieťovým službám
- Eduroam

Switche

Redundancia?

- hviezdicové zapojenie je citlivé na výpadok
- cyklus v sieti na L2 OSI má fatálne následky
- *broadcast storms*

Spanning Tree Protocol (STP)

- nadbytočné spoje cyklu prepne do pohotovostného režimu
- pri výpadku aktívneho spoja sa pasívny spoj preberie

Shortest Path Bridging (SPB)

- novšia alternatíva

Bezdrôtové zariadenia

Access Points

- celkom 120 kusov
- 802.11g, n, ac
- 2.4 GHz a 5 GHz pásma

Značky

- RouterBOARD (40 ks)
- UniFi (80 ks)

Služby

Web

Hypertext Transfer Protocol (HTTP)

- prenos dokumentov
- rozšírenia (MIME, RPC)
- model klient-server
- textový (do `v1.1`)
- binárny (od `v2`)
- postavený nad TCP (UDP od `v3`)
- *HTTP Secure* (HTTPS): TLS

Apache Server

- jedna z implementácií HTTP servera
- komplexné nastavenia, virtuálne servery, `suexec`, ...
- `www.fi.muni.cz` (`aisa.fi.muni.cz`)
- `webhost.fi.muni.cz` (`aisa.fi.muni.cz`, iná IP adresa)
- `is.muni.cz`

Prenos súborov

File Transfer Protocol (FTP)

- prenos súborov medzi počítačmi
- sám je málo zabezpečený
  často v kombinácii s ďalšími protokolmi (napr. SSH)
- verejne dostupné repozitáre

Zrkadlo distribúcií na FI

- `ftp.fi.muni.cz` (`odysseus.fi.muni.cz`)
- `ftp.linux.cz` (`odysseus.linux.cz`)
- Ubuntu, Debian, Fedora, CentOS, ArchLinux, Gentoo, ...

Adresár údajov

Lightweight Directory Access Protocol (LDAP)

- adresárový server
- záznamy uložené v hierarchii
- informácie o používateľoch, skupinách, službách, ...

- `ldap.fi.muni.cz` (`thetis.fi.muni.cz`)
- `ldap1.fi.muni.cz` (`pyrrha.fi.muni.cz`)

Adresár údajov

Príklad LDAP: Informácie o používateľovi

```
login@aisa:~$ ldapsearch -h ldap.fi.muni.cz -x -b \
              ou=People,dc=fi,dc=muni,dc=cz uid=xlacko1
dn: uid=xlacko1,ou=People,dc=fi,dc=muni,dc=cz
uid: xlacko1
cn: xlacko1
uidNumber: 15291
gidNumber: 10100
homeDirectory: /home/xlacko1
gecos: Roman Lacko
...
```

Autentizácia

Kerberos

- *vzájomná autentizácia*
- používateľ overí identitu služby
- služba overí identitu používateľa
- *tickets*

- náchylný na rozdiely v čase ($\rightarrow$ NTP)

Heimdal

- implementácia protokolu
- `krb.fi.muni.cz` (`thetis.fi.muni.cz`)
- `krb1.fi.muni.cz` (`pyrrha.fi.muni.cz`)

Pošta

Simple Mail Transfer Protocol (SMTP)

- textový protokol na výmenu elektronických správ (*e-mail*)
- doručovanie podľa domény (`user@`*`fi.muni.cz`*)
- ***MUA*** $\rightarrow$ ***MSA*** $\rightarrow$ ***MTA*** $\rightarrow$ ***MDA*** $\rightarrow$ *MRA*/*MUA*

Post Office Protocol 3 (POP3)

Internet Message Access Protocol (IMAP)

- prístup k elektronickej pošte

Poštové servery FI

- `mail.fi.muni.cz` (`anxur.fi.muni.cz`, zamestnanecký)
- `aisa.fi.muni.cz` (študentský)
- `mail.muni.cz` (`arethusa.fi.muni.cz`, IS)
- `postfix` (SMTP), `dovecot` (POP3, IMAP)

Presný čas

Network Time Protocol (NTP)

- synchronizácia hodín počítačov v sieti
- presnosť na ms až μs
- hierarchický systém zdrojov presného času (*stratum 0*, *1*, ...)
- berie do úvahy latenciu paketov
- náhrada za starší *Time Protocol*

Čas v sieti FI

- `time.fi.muni.cz` (`pyrrha.fi.muni.cz`)
- používa aj IS MU

Doménový systém

Domain Name System (DNS)

- zabezpečuje preklad mien strojov na ich IP adresy
- hierarchický
- decentralizovaný

- `ns.fi.muni.cz` (`anxur.fi.muni.cz`, autoritatívny)
- ďalšie servery (`aisa.fi.muni.cz`, `thetis.fi.muni.cz`, ...)

```
login@aisa:~$ host www.fi.muni.cz
www.fi.muni.cz is an alias for aisa.fi.muni.cz
aisa.fi.muni.cz address 147.251.48.1
aisa.fi.muni.cz IPv6 address 2001:718:801:230::1
aisa.fi.muni.cz mail is handled by 50 relay.muni.cz
```

Dynamické prideľovanie IP adries

Dynamic Host Configuration Protocol (DHCP)

- automatické sieťové nastavenia klientov
- obvykle IP adresy a brána

- **dynamická alokácia** (*DHCP pool*)
- výber IP adresy z definovanej množiny
- Eduroam, `wlan_fi`

- **statická alokácia**
- rezervácia konkrétnej adresy pre klienta
- obvykle podľa *MAC* adresy
- zamestnanecké pracovné stanice

- `ares.fi.muni.cz`

Vzdialená správa zariadení

Simple Network Management Protocol (SNMP)

- získavanie a nastavovanie parametrov sieťových zariadení
- hierarchická organizácia premenných v strome
- premenné majú typy a obmedzenia

- **monitoring**
- servery a počítače (využitie zdrojov)
- switche (stav portov)
- kamery, rozvrhové panely, ...

- **regulácia**
- systém chladenia datacentier

Príklad SNMP: Prietok vody chladiacou jednotkou

```
login@thetis:~$ snmpget -v2c lcp-2-1.m2.fi.muni.cz 'cmcIIIVarName.2.75'
RITTAL-CMC-III-MIB::cmcIIIVarName.2.75 = STRING: "Water.Flowrate.Value"

login@thetis:~$ snmpget -v2c lcp-2-1.m2.fi.muni.cz 'cmcIIIVarValueInt.2.75'
RITTAL-CMC-III-MIB::cmcIIIVarValueInt.2.75 = INTEGER: 118

login@thetis:~$ snmpget -v2c lcp-2-1.m2.fi.muni.cz 'cmcIIIVarValueStr.2.75'
RITTAL-CMC-III-MIB::cmcIIIVarValueStr.2.75 = STRING: "11.8 l/min"
```

Sieťové súborové systémy

Network File System (NFS)

- sprístupnenie disku alebo adresára po sieti inému stroju
- transparentný prístup k súborom
- podpora väčšiny UNIXových súborových operácií
  - ✔ práva
  - ✔ rozšírené atribúty
  - ✔ zámky
  - ✘ notifikácie o zmenách (`inotify`)

Domovské adresáre

- `home.fi.muni.cz` (`anxur.fi.muni.cz`)
- SSD pole s kapacitou 12 TB
- `aisa`, `aura`, `adonis`, `nymfe*`, `musa*`, `luna*`
- prístup v sieti MU pre vlastné stroje
- adresáre `/home/${LOGIN}` a `/data/${LOGIN}`

Sieťové súborové systémy

Server Message Block (SMB)

- historický názov *Common Internet File System* (CIFS)
- pôvod zo sveta Microsoft Windows
- zdieľanie súborov
- prístup k sieťovým tlačiarňam (okrem CUPS)

Samba

- voľná implementácia protokolu
- podpora pre niektoré UNIX atribúty súborov
- prístupné ako `J:` v učebniach s MS Windows (`titan`, ...)

Sieťové súborové systémy

Ceph

- distribuované úložisko dát
- dekompozícia na viacero samostatných démonov
- efektívna replikácia
- vysoká škálovateľnosť

Stratus.FI

- virtualizačný systém *OpenNebula*
- obrazy uložené v Ceph
- kapacita $\approx$ 500 TB

Privátne adresy

Network Address Translation (NAT)

- mapovanie adresného priestoru na iný
- sprístupnenie Internetu strojom, ktoré z Internetu prístupné byť nemajú
- (historicky) uľahčenie zmeny adresácie
- (dnes) spomalenie vyčerpávania IPv4

IP masquerading

- skrývanie privátnych rozsahov za verejnú IP adresu
- typicky na úrovni routera
- `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16`
- (privátne) virtuálne stroje
- laboratórne siete
- *CERIT Science Park*

Privátne adresy

Virtual Private Network (VPN)

- tunel do inej, obvykle nedostupnej siete
- virtuálne sieťové rozhranie
- nastavenie ciest (`ip route`)
- často nutná autentizácia a šifrovanie

OpenVPN

- privátne siete v *CERIT Science Park*
- MU (ÚVT)
- FI (CVT)

Bezpečný shell

Secure Shell (SSH)

- príkazový riadok na vzdialenom počítači

- vytváranie tunelov
- grafické aplikácie (X11)
- prenos súborov (SFTP, SCP)
- súborový systém (SSHFS)

Mobile Shell (MOSH)

- alternatíva SSH
- menej citlivé na nestabilnú sieť (WiFi)

Dostupnosť zo sveta

`aisa.fi.muni.cz`, `anxur.fi.muni.cz`

Príklad SSH: Vytvorenie tunelu

```
david@hal9000:~$ ssh -fN -L 2242:nymfe42:22 login@aisa.fi.muni.cz
david@hal9000:~$ ssh -p 2242 login@localhost # connecting to nymfe42
david@hal9000:~$
```

Príklad SSH: Súborový systém

```
david@hal9000:~$ sshfs xlacko1@aisa.fi.muni.cz:public_html/ /mnt/www
david@hal9000:~$ vim /mnt/www/index.html
```

Monitoring

Nagios

- kontrola dostupnosti služieb
- notifikácie (e-mail, SMS, ...)
- SNMP, SSH
- textová konfigurácia
- dostupné množstvo rozšírení

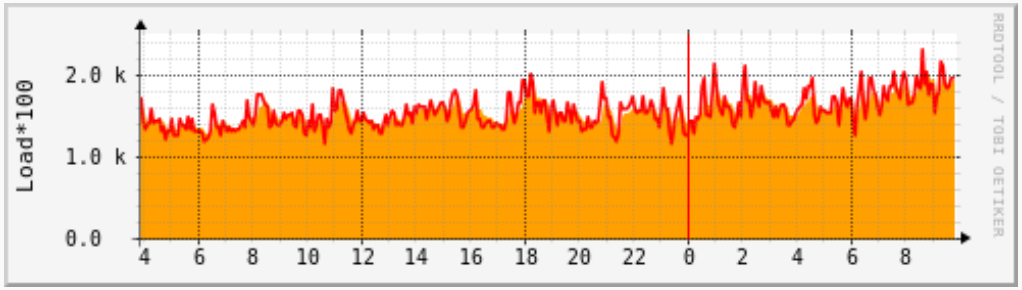
- modernejšia alternatíva Icinga

Monitoring

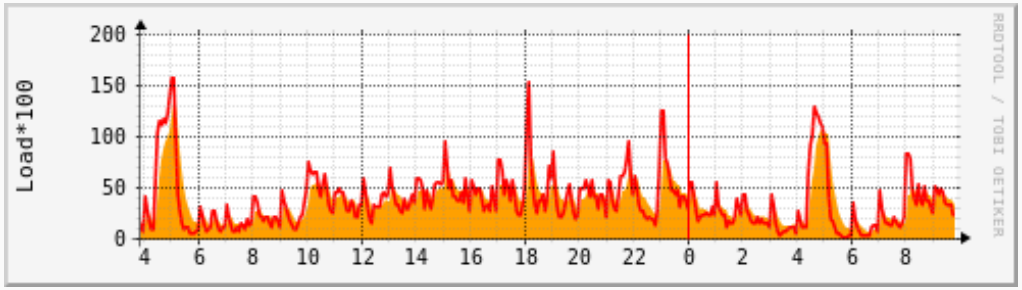
Multi-Router Traffic Grapher (MRTG)

- vykresľovanie grafov
- sledovanie meraných veličín

MRTG – Vyťaženie Aisy



MRTG – Vyťaženie GitLabu



Bezdrôtová sieť

Výhody a nevýhody bezdrôtových sietí

Výhody

- pohodlnejšie než káblové pripojenie
- prístup pre viac ľudí
- mobilita

Nevýhody

- horšia kvalita v porovnaní s káblom
- nižšia tolerancia šumu

Princíp

Káblové pripojenie

- ✔ analógové signály
- ✔ digitálne signály

Bezdrôtové pripojenie

- ✔ analógové signály
- ✘ digitálne signály
  - vzduch za normálnych okolností nie je vodivý
  - *nosná frekvencia*
  - rôzne možnosti kódovania dát
    - amplitúdová modulácia
    - frekvenčná modulácia
    - fázový posun (*Phase-Shift Keying*, PSK)

Pásma pre nosné frekvencie

Pásma

- intervaly rezervovaných frekvencií
- použitie môže vyžadovať licenciu (*licenčné pásma*)
- rozdelené na *kanály*

WiFi

- bezlicenčné
- 2,4 GHz (`802.11b,g,n,ax`)
- 14 kanálov 5 MHz od seba
  - kanál 1: 2.412 MHz (2.401 MHz - 2.423 MHz)
  - kanál 2: 2.417 MHz (2.406 MHz - 2.428 MHz)
  - ...
- 5 GHz (`802.11a,n,ac,ax,be`)
- rozsahy 5.030 MHz - 5.875 MHz
- 10, 20, 40, 80 a 160 MHz široké kanály

Pásma pre nosné frekvencie

Spread Spectrum

- prenos viacerých signálov naraz
- obmedzenie rušenia

- *Frequency-Hopping Spread Spectrum* (FHSS)
- *Direct-Sequence Spread Spectrum* (DSSS)
- *Orthogonal Frequency-Division Multiplex* (OFDM)
- *Multiple-Input, Multiple-Output* (MIMO)

Riadenie prístupu

Carrier Sense, Multiple Access with Collision Avoidance

(CSMA/CA)

- detekcia kolízií (CSMA/CD) je veľmi nepraktická
- stroj čaká na moment, kedy je médium dostatočne dlho voľné
- vyšle žiadosť o povolenie vysielania
- ak dostane odpoveď, môže vysielať
- ak odpoveď nepríde, pravdepodobne došlo ku kolízii

Základné typy bezdrôtových sietí

Ad-Hoc

- bez centrálneho prístupného bodu
- stroje komunikujú priamo medzi sebou

Sieť s prístupovým bodom

- prístupový bod (*(Wireless) Access Point*, (W)AP)
- komunikácia výhradne cez AP
- brána do iných sietí
- *Service Set ID* (SSID)

Bezpečnosť

Odpočúvanie paketov

- na kábli prakticky len koncové zariadenia
- vo vzduchu paket dostane každý stroj v dosahu

Zabezpečenie bezdrôtovej siete

- filter adries
- *Open WiFi* (bez zabezpečenia)
- *Wired Equivalent Privacy* (WEP)
- *WiFi Protected Access* (WPA, WPA2, WPA3)
  (WPA3: *Opportunistic Wireless Encryption* (OWE))

Hardware

Access Point (AP)

- výkon ovplyvňuje, koľko používateľov dokáže obslúžiť
- počet antén
- napájanie
- zabezpečenie

Antény

- zabudované alebo vymeniteľné

- všesmerové, viacsmerové, sektorové, (jedno)smerové

Hardware

MikroTik RouterBOARD

- externá anténa
- `802.11g,n`
- 2,4 a 5 GHz
- napájanie PoE
- operačný systém OpenWRT (UNIX-like)

MikroTik RouterBOARD

UniFi

- `802.11g,n,ac`
- 2,4 a 5 GHz
- napájanie PoE+
- operačný systém OpenWRT (UNIX-like)

- vlastný kontrolér v Jave
- centrálna správa AP

Hardware

UniFi

Dostupné siete

Education Roaming (Eduroam)

- univerzitná bezdrôtová sieť
- SSID obvykle `eduroam`
- WPA/WPA2, RADIUS
- `147.251.44.0/22`
- `2001:718:801:22c::/64`

Dostupné siete

Fakultná bezdrôtová sieť

- SSID `wlan_fi`
- po pripojení prístup len na `wifi.fi.muni.cz` (`fadmin.fi.muni.cz`, `thetis.fi.muni.cz`)
- autentizácia fakultným loginom a heslom
- prístup povolený na firewalle pre (MAC, IP)

Dostupné siete

Captive portal

- presmerovanie na autentizačnú stránku
- klient po pripojení do siete skúsi stiahnuť známu stránku
- brána spojenie presmeruje na autentizáciu
- nefunguje s HTTPS


The End