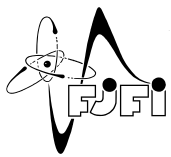
Schůzka správců — únor 2008

Petr Vokáč
vokac@kmlinux.fjfi.cvut.cz

České vysoké učení technické, FJFI

20. 2. 2008

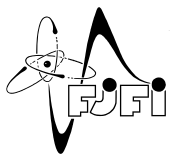
Motto: make it robust



1 DNS, DHCP, WiFi a privátní IP na FJFI
- DNS, DHCP
- WiFi
- Rozdělení privátních IP

2 Registrace síťových zařízení
- Motivace, popis řešení
- Detekce lokálních problémů
- Řešení stížností

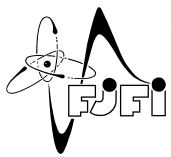
3 Ostatní
- Notes



1 DNS, DHCP, WiFi a privátní IP na FJFI
- DNS, DHCP
- WiFi
- Rozdělení privátních IP

2 Registrace síťových zařízení
- Motivace, popis řešení
- Detekce lokálních problémů
- Řešení stížností

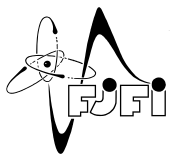
3 Ostatní
- Notes



1 DNS, DHCP, WiFi a privátní IP na FJFI
- DNS, DHCP
- WiFi
- Rozdělení privátních IP

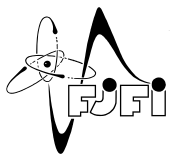
2 Registrace síťových zařízení
- Motivace, popis řešení
- Detekce lokálních problémů
- Řešení stížností

3 Ostatní
- Notes



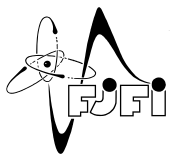
Konfigurace DNS

- Aktuální informace na NMS wiki (Doména FJFI)
- Přechod na ISC Bind 9.5 (beta 2)
  - Podpora GSS-TSIG (zabezpečené DDNS s M$ Windows)
  - Plnohodnotná náhrada Windows DNS serveru
  - Doménovým kontrolerům povolen zápis
    - ANY do zón `_tcp`, `_udp`, `_msdcs`, `_sites`, `DomainDnsZones`, `ForestDnsZones`
    - A, PTR pro vlastní jména / reverzy DC
  - DNS na Windows je možné (vhodné) úplně vypnout
- DNSSec
  - V plánu až bude podepsané `.cz` resp `.cvut.cz` (letos)
  - Podporováno cca od roku 2000 (Windows DNS nepodporuje)
  - Nezanedbatelný vliv na velikost zón a výkon
- TSIG podepsané transfery na slave (otestovat na Děčín?)



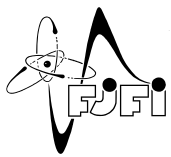
Konfigurace DNS

- Aktuální informace na NMS wiki (Doména FJFI)
- Přechod na ISC Bind 9.5 (beta 2)
  - Podpora GSS-TSIG (zabezpečené DDNS s M$ Windows)
  - Plnohodnotná náhrada Windows DNS serveru
  - Doménovým kontrolerům povolen zápis
    - ANY do zón `_tcp`, `_udp`, `_msdcs`, `_sites`, `DomainDnsZones`, `ForestDnsZones`
    - A, PTR pro vlastní jména / reverzy DC
  - DNS na Windows je možné (vhodné) úplně vypnout
- DNSSec
  - V plánu až bude podepsané `.cz` resp `.cvut.cz` (letos)
  - Podporováno cca od roku 2000 (Windows DNS nepodporuje)
  - Nezanedbatelný vliv na velikost zón a výkon
- TSIG podepsané transfery na slave (otestovat na Děčín?)



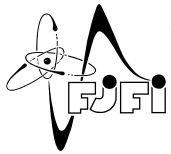
Konfigurace DNS

- Aktuální informace na NMS wiki (Doména FJFI)
- Přechod na ISC Bind 9.5 (beta 2)
  - Podpora GSS-TSIG (zabezpečené DDNS s M$ Windows)
  - Plnohodnotná náhrada Windows DNS serveru
  - Doménovým kontrolerům povolen zápis
    - ANY do zón `_tcp`, `_udp`, `_msdcs`, `_sites`, `DomainDnsZones`, `ForestDnsZones`
    - A, PTR pro vlastní jména / reverzy DC
  - DNS na Windows je možné (vhodné) úplně vypnout
- DNSSec
  - V plánu až bude podepsané `.cz` resp `.cvut.cz` (letos)
  - Podporováno cca od roku 2000 (Windows DNS nepodporuje)
  - Nezanedbatelný vliv na velikost zón a výkon
- TSIG podepsané transfery na slave (otestovat na Děčín?)



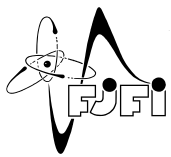
Konfigurace DNS

- Aktuální informace na NMS wiki (Doména FJFI)
- Přechod na ISC Bind 9.5 (beta 2)
  - Podpora GSS-TSIG (zabezpečené DDNS s M$ Windows)
  - Plnohodnotná náhrada Windows DNS serveru
  - Doménovým kontrolerům povolen zápis
    - ANY do zón `_tcp`, `_udp`, `_msdcs`, `_sites`, `DomainDnsZones`, `ForestDnsZones`
    - A, PTR pro vlastní jména / reverzy DC
  - DNS na Windows je možné (vhodné) úplně vypnout
- DNSSec
  - V plánu až bude podepsané `.cz` resp `.cvut.cz` (letos)
  - Podporováno cca od roku 2000 (Windows DNS nepodporuje)
  - Nezanedbatelný vliv na velikost zón a výkon
- TSIG podepsané transfery na slave (otestovat na Děčín?)



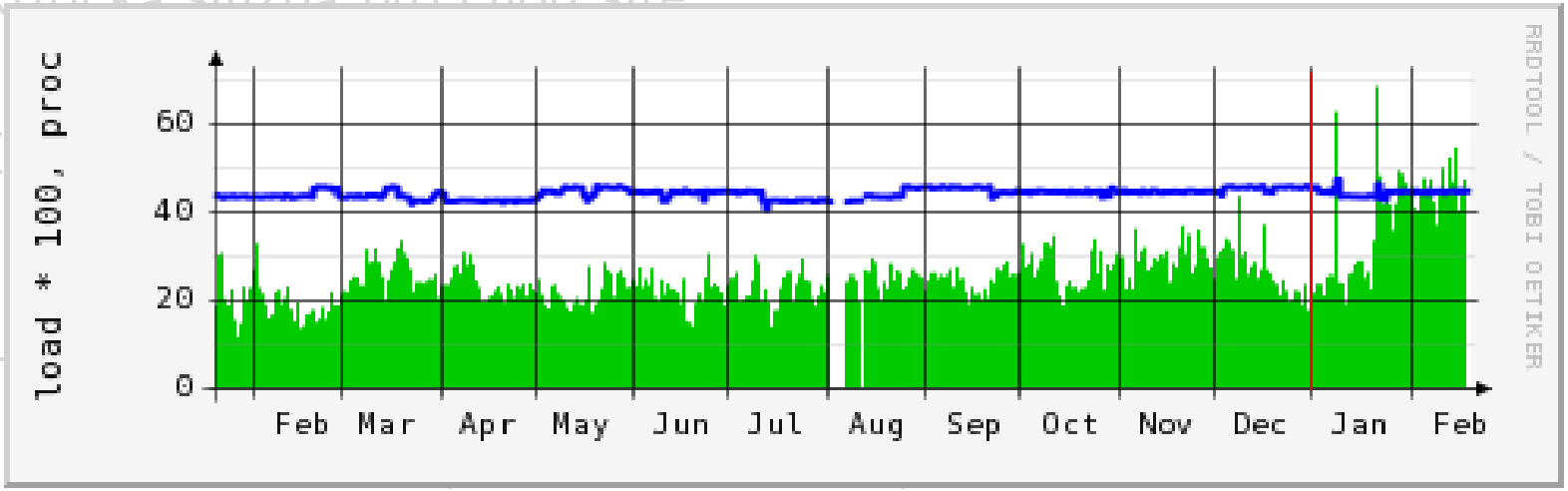
HW, spolehlivost, cluster

- Současná konfigurace (Pentium 100Mhz, 64MB RAM) nestačí
- Kritická služba pro chod sítě
  - Sekundární DNS nemusí být někdy vhodná (resolver)
- Zajištění vysoké dostupnosti s spolehlivosti ⇒ cluster
  - Anycast — perfektní, ale bohužel "nejde" realizovat
  - Lokální cluster
- Testovací konfigurace
  - nsv.fjfi.cvut.cz (Xen host na kmvirt), nms.fjfi.cvut.cz
  - heartbeat+drbd+IP — cca 10–30s výpadek DNS
  - `147.32.9.17` — výhledově nahradí `147.32.9.4`
  - Výkonostní testy OK (bez DNSSec)



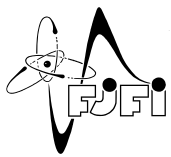
HW, spolehlivost, cluster

- Současná konfigurace (Pentium 100Mhz, 64MB RAM) nestačí
- Kritická služba pro chod sítě
- Z
- T
  - heartbeat+drbd+IP — cca 10–30s výpadek DNS
  - 147.32.9.17 — výhledově nahradí 147.32.9.4
  - Výkonostní testy OK (bez DNSSec)



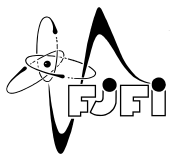
HW, spolehlivost, cluster

- Současná konfigurace (Pentium 100Mhz, 64MB RAM) nestačí
- Kritická služba pro chod sítě
  - Sekundární DNS nemusí být někdy vhodná (resolver)
- Zajištění vysoké dostupnosti s spolehlivosti ⇒ cluster
  - Anycast — perfektní, ale bohužel "nejde" realizovat
  - Lokální cluster
- Testovací konfigurace
  - nsv.fjfi.cvut.cz (Xen host na kmvirt), nms.fjfi.cvut.cz
  - heartbeat+drbd+IP — cca 10–30s výpadek DNS
  - `147.32.9.17` — výhledově nahradí `147.32.9.4`
  - Výkonostní testy OK (bez DNSSec)



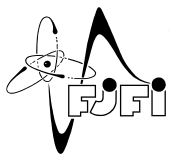
HW, spolehlivost, cluster

- Současná konfigurace (Pentium 100Mhz, 64MB RAM) nestačí
- Kritická služba pro chod sítě
  - Sekundární DNS nemusí být někdy vhodná (resolver)
- Zajištění vysoké dostupnosti s spolehlivosti ⇒ cluster
  - Anycast — perfektní, ale bohužel "nejde" realizovat
  - Lokální cluster
- Testovací konfigurace
  - nsv.fjfi.cvut.cz (Xen host na kmvirt), nms.fjfi.cvut.cz
  - heartbeat+drbd+IP — cca 10–30s výpadek DNS
  - `147.32.9.17` — výhledově nahradí `147.32.9.4`
  - Výkonostní testy OK (bez DNSSec)



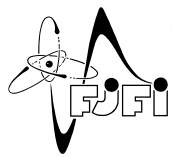
HW, spolehlivost, cluster

- Současná konfigurace (Pentium 100Mhz, 64MB RAM) nestačí
- Kritická služba pro chod sítě
  - Sekundární DNS nemusí být někdy vhodná (resolver)
- Zajištění vysoké dostupnosti s spolehlivosti ⇒ cluster
  - Anycast — perfektní, ale bohužel "nejde" realizovat
  - Lokální cluster
- Testovací konfigurace
  - nsv.fjfi.cvut.cz (Xen host na kmvirt), nms.fjfi.cvut.cz
  - heartbeat+drbd+IP — cca 10–30s výpadek DNS
  - `147.32.9.17` — výhledově nahradí `147.32.9.4`
  - Výkonostní testy OK (bez DNSSec)



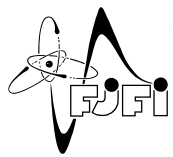
Úpravy záznamů v DNS

- Admin web rozhraní na NMS
  - Možnost editovat všechny zóny
    - Nutná minimální znalost struktury DNS záznamů
    - `@`, `NS`, `SOA` vyžadují speciální práva
    - Včetně privátních adres (dostupné lokálně)
  - Audit změn
  - Kdo má mít přístup?
- Automatické změny
  - DHCP+DDNS v `.dhcp.fjfi.cvut.cz` + reverzy
  - Speciální záznamy propagované z DC
  - "HA" aliasy `smtp`, `ldap`, `krb`, ...
- Přímá úprava lokalních souborů
  - nedoporučuji (nejde-li o rozsáhlé změny)
  - `rndc freeze [zone_name]` resp. `rndc thaw [zone_name]`



Úpravy záznamů v DNS

- Admin web rozhraní na NMS
  - Možnost editovat všechny zóny
    - Nutná minimální znalost struktury DNS záznamů
    - `@`, `NS`, `SOA` vyžadují speciální práva
    - Včetně privátních adres (dostupné lokálně)
  - Audit změn
  - Kdo má mít přístup?
- Automatické změny
  - DHCP+DDNS v `.dhcp.fjfi.cvut.cz` + reverzy
  - Speciální záznamy propagované z DC
  - "HA" aliasy `smtp`, `ldap`, `krb`, ...
- Přímá úprava lokalních souborů
  - nedoporučuji (nejde-li o rozsáhlé změny)
  - `rndc freeze [zone_name]` resp. `rndc thaw [zone_name]`



Úpravy záznamů v DNS

- Admin web rozhr
  - Možnost edit
    - Nutná m
    - @, NS, SO
    - Včetně p
  - Audit změn
  - Kdo má mít p
- Automatické změ
  - DHCP+DDN
  - Speciální záz
  - "HA" aliasy s
- Přímá úprava lok
  - nedoporučuji
  - rndc freeze

přihlášen: ***Petr Vokáč*** (vokac) | set session never expire | odhlásit

Informace | Účty | Mail | WiFi | Databáze | MAC | Zálohy | Who | Stat | Admin

Uživatelská nastavení - admin

Informace | Audit | Účty | Mail | WiFiFJFI/Eduroam | Ldap | Who | MAC/DHCP/DDNS | Log

Správa síťových zařízení, DHCP a DDNS

Seznam | Registrace | Vyhledávání | Export | Topologie | Konflikty | Arpwatch | DHCP | DDNS

Správa DNS serveru

Add record | Add host | fjfi | dhcp | ipv6 | test | 147.32.4.0 | 147.32.5.0 | 147.32.6.0 | 147.32.7.0 | 147.32.8.0 | 147.32.9.0 | 147.32.10.0 | 147.32.11.0 | 147.32.25.0 | IPv6 Břehová | IPv6 Trojanova | IPv6 Trója | 172.16.0.0 | vpn.local | mgmt.local | wififjfi.local | blocked-eduroam.local | blocked-wififjfi.local

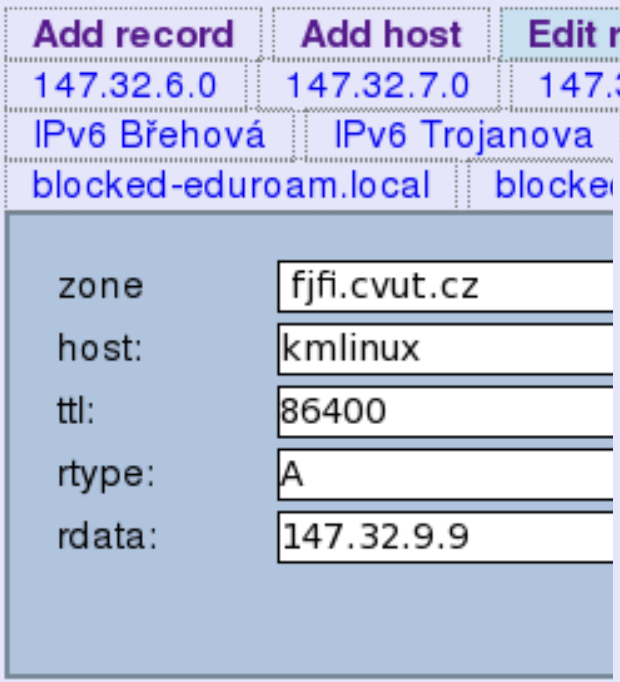
command: ddns zone zone=dhcp.fjfi.cvut.cz
status: success
text:

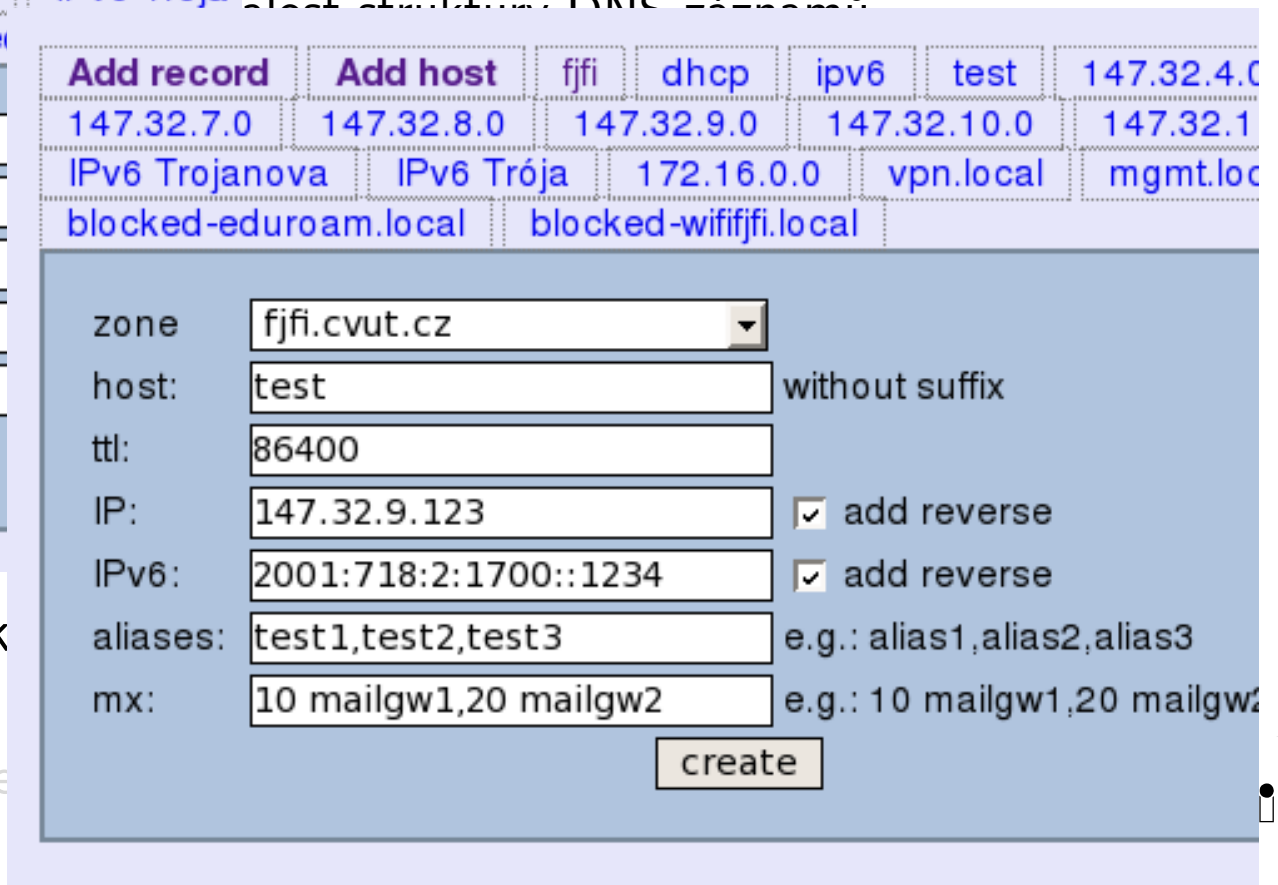
action	host	ttl	rtype	rdata
e / d	@	86400	SOA	ns.fjfi.cvut.cz. vokac.fjfi.cvut.cz. 2004105022 300 150 86400 300
e / d	@	86400	NS	ns.fjfi.cvut.cz.
e / d / da	Hobza	600	A	147.32.8.47 D/P/A
e / d	Hobza	600	TXT	"31f2f5c3175f5818227fcbfff7be96343e"
e / d	HomeCenter	600	TXT	"31187fe3f57069ae70b74db1a9f0aff163"
e / d / da	HomeCenter	600	A	147.32.11.254 D/P/A
e / d	KFE-KN	600	TXT	"31472ba4d6bbe26c518606142b3835c026"
e / d / da	KFE-KN	600	A	147.32.7.174 D/P/A
e / d / da	KFE234	600	A	147.32.7.227 D/P/A
e / d	KFE234	600	TXT	"31788ded6069369121c8e459df21f54cb4"
e / d	KFE241vyh	600	TXT	"31eeb61b5fd55e660539fe4be051c94c9f"
e / d / da	KFE241vyh	600	A	147.32.7.245 D/P/A
e / d	KM-WKST-03	600	TXT	"310641e1dc3b9a8fb01bc83b18eef28921"

Úpravy záznamů v DNS

MS

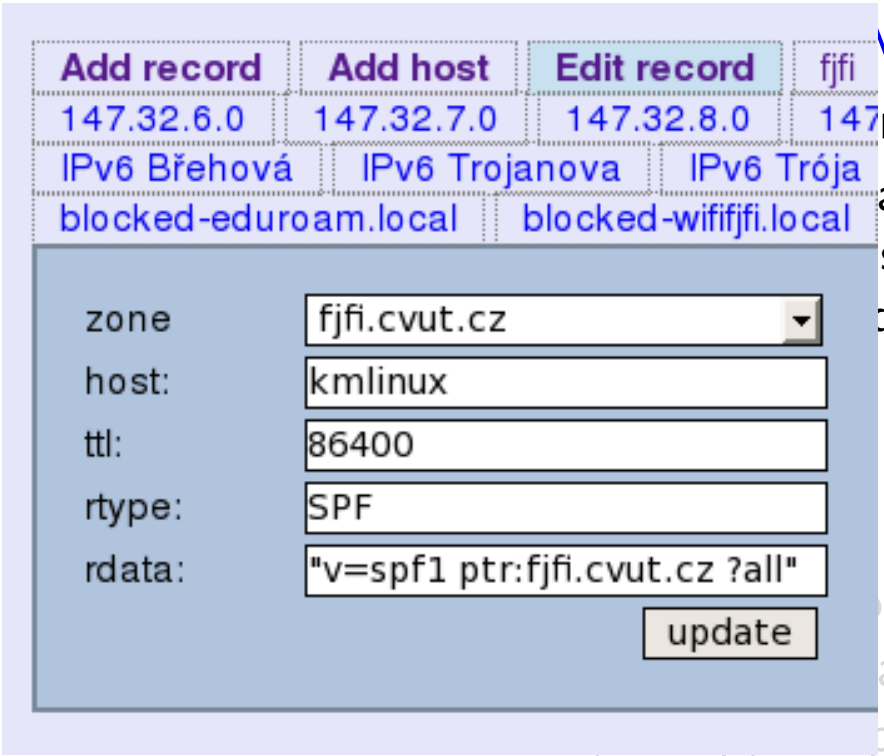
ny zóny





- Přímá úprava lok
  - nedoporučuji
  - `rndc freeze`

Úpravy záznamů v DNS



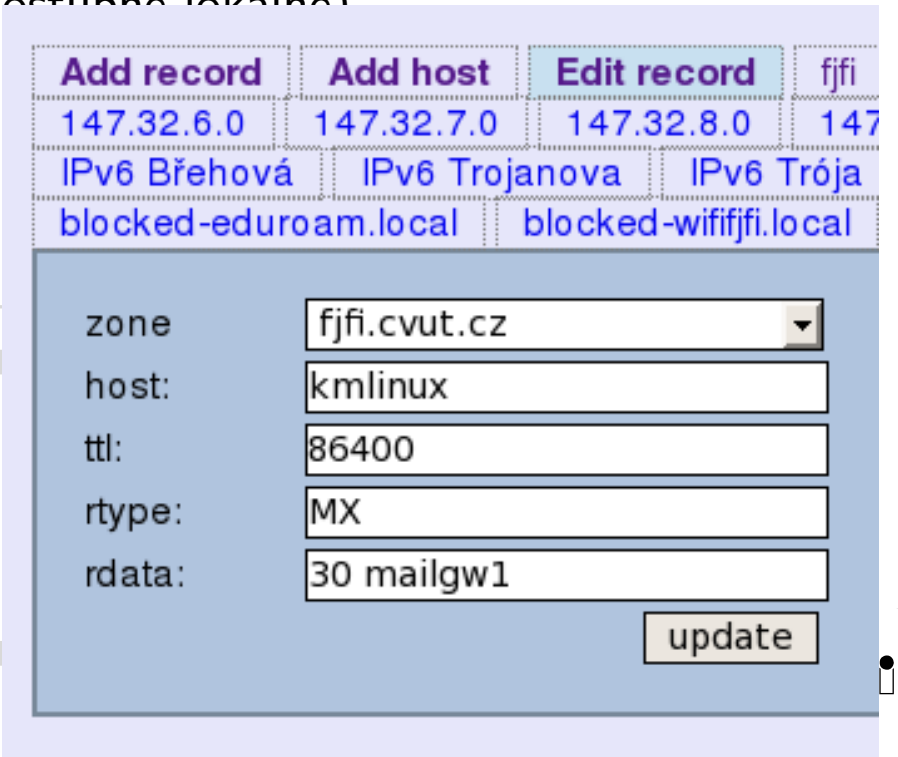
MS

ny zóny

alost struktury DNS záznamů

speciální práva

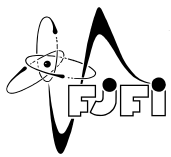
dres (dostupné lokálně)



- Přímá úprava lokalních souborů
  - nedoporučuji (nejde-li o rozsá
  - `rndc freeze [zone_name]`

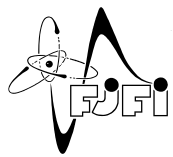
Úpravy záznamů v DNS

- Admin web rozhraní na NMS
  - Možnost editovat všechny zóny
    - Nutná minimální znalost struktury DNS záznamů
    - `@`, `NS`, `SOA` vyžadují speciální práva
    - Včetně privátních adres (dostupné lokálně)
  - Audit změn
  - Kdo má mít přístup?
- Automatické změny
  - DHCP+DDNS v `.dhcp.fjfi.cvut.cz` + reverzy
  - Speciální záznamy propagované z DC
  - "HA" aliasy `smtp`, `ldap`, `krb`, ...
- Přímá úprava lokalních souborů
  - nedoporučuji (nejde-li o rozsáhlé změny)
  - `rndc freeze [zone_name]` resp. `rndc thaw [zone_name]`



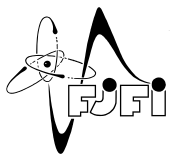
Úpravy záznamů v DNS

- Admin web rozhraní na NMS
  - Možnost editovat všechny zóny
    - Nutná minimální znalost struktury DNS záznamů
    - `@`, `NS`, `SOA` vyžadují speciální práva
    - Včetně privátních adres (dostupné lokálně)
  - Audit změn
  - Kdo má mít přístup?
- Automatické změny
  - DHCP+DDNS v `.dhcp.fjfi.cvut.cz` + reverzy
  - Speciální záznamy propagované z DC
  - "HA" aliasy `smtp`, `ldap`, `krb`, ...
- Přímá úprava lokalních souborů
  - nedoporučuji (nejde-li o rozsáhlé změny)
  - `rndc freeze [zone_name]` resp. `rndc thaw [zone_name]`



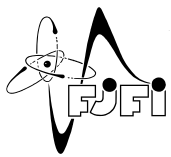
Úpravy záznamů v DNS

- Admin web rozhraní na NMS
  - Možnost editovat všechny zóny
    - Nutná minimální znalost struktury DNS záznamů
    - `@`, `NS`, `SOA` vyžadují speciální práva
    - Včetně privátních adres (dostupné lokálně)
  - Audit změn
  - Kdo má mít přístup?
- Automatické změny
  - DHCP+DDNS v `.dhcp.fjfi.cvut.cz` + reverzy
  - Speciální záznamy propagované z DC
  - "HA" aliasy `smtp`, `ldap`, `krb`, ...
- Přímá úprava lokalních souborů
  - nedoporučuji (nejde-li o rozsáhlé změny)
  - `rndc freeze [zone_name]` resp. `rndc thaw [zone_name]`



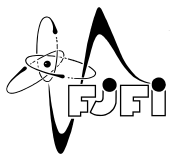
Konfigurace DHCP

- Konfigurace generovaná z infomací zadaných na NMS
  - Některé údaje (rezervace IP) zadávají jen správci (kdo?)
  - Dodržovat přidělování IP podle plánu na NMS wiki
  - Nelze dělat rezervace na rozsah pro dynamicky přidělované IP
- Klíčová komponenta pro registrace MAC
- Na každé síti (VLAN) musí běžet server nebo relay
- Důležitá služba $\Rightarrow$ spolehlivost $\Rightarrow$ failover konfigurace
  - Zatím není realizováno
  - Podpora přímo v ISC DHCP + DHCP Relay na CISCO
  - Jen pro dva DHCP servery (pro různé rozsahy lze různé)
    - Trojanka + Břehovka, Břehovka + Trója, Trója + Trojanka
    - Lze nakonfigurovat dhcp relay v Tróji?



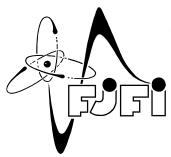
Konfigurace DHCP

- Konfigurace generovaná z infomací zadaných na NMS
  - Některé údaje (rezervace IP) zadávají jen správci (kdo?)
  - Dodržovat přidělování IP podle plánu na NMS wiki
  - Nelze dělat rezervace na rozsah pro dynamicky přidělované IP
- Klíčová komponenta pro registrace MAC
- Na každé síti (VLAN) musí běžet server nebo relay
- Důležitá služba ⇒ spolehlivost ⇒ failover konfigurace
  - Zatím není realizováno
  - Podpora přímo v ISC DHCP + DHCP Relay na CISCO
  - Jen pro dva DHCP servery (pro různé rozsahy lze různé)
    - Trojanka + Břehovka, Břehovka + Trója, Trója + Trojanka
    - Lze nakonfigurovat dhcp relay v Tróji?



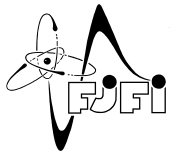
Konfigurace DHCP

- Konfigurace generovaná z infomací zadaných na NMS
  - Některé údaje (rezervace IP) zadávají jen správci (kdo?)
  - Dodržovat přidělování IP podle plánu na NMS wiki
  - Nelze dělat rezervace na rozsah pro dynamicky přidělované IP
- Klíčová komponenta pro registrace MAC
- Na každé síti (VLAN) musí běžet server nebo relay
- Důležitá služba ⇒ spolehlivost ⇒ failover konfigurace
  - Zatím není realizováno
  - Podpora přímo v ISC DHCP + DHCP Relay na CISCO
  - Jen pro dva DHCP servery (pro různé rozsahy lze různé)
    - Trojanka + Břehovka, Břehovka + Trója, Trója + Trojanka
    - Lze nakonfigurovat dhcp relay v Tróji?



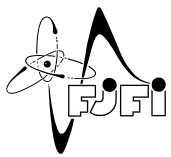
Konfigurace DHCP

- Konfigurace generovaná z infomací zadaných na NMS
  - Některé údaje (rezervace IP) zadávají jen správci (kdo?)
  - Dodržovat přidělování IP podle plánu na NMS wiki
  - Nelze dělat rezervace na rozsah pro dynamicky přidělované IP
- Klíčová komponenta pro registrace MAC
- Na každé síti (VLAN) musí běžet server nebo relay
- Důležitá služba $\Rightarrow$ spolehlivost $\Rightarrow$ failover konfigurace
  - Zatím není realizováno
  - Podpora přímo v ISC DHCP + DHCP Relay na CISCO
  - Jen pro dva DHCP servery (pro různé rozsahy lze různé)
    - Trojanka + Břehovka, Břehovka + Trója, Trója + Trojanka
    - Lze nakonfigurovat dhcp relay v Tróji?



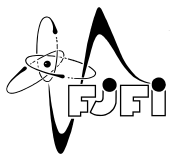
WiFi sítě na FJFI

- Plán pokrytí
  - soukromá AP buď podle plánu nebo na kanál 13
- Dvě standardní sítě s různým zabezpečením
  - Eduroam (pouze na CISCO, VLAN 13, 147.32.11.0/24)
  - WiFiFJFI (všechny AP, web autentizace, VLAN 15, NAT)
- V případě potřeby (konference, . . .) lze zprovoznit další SSID
- Účty v AD (hosté), každá síť vlastní heslo (Eduroam politika)
- Infomace o konfiguraci AP na NMS wiki
- Rozmístění AP v Břehovce, do kdy?
- Požadavky na další pokrytí?



WiFi sítě na FJFI

- Plán pokrytí
  - soukromá AP buď podle plánu nebo na kanál 13
- Dvě standardní sítě s různým zabezpečením
  - Eduroam (pouze na CISCO, VLAN 13, `147.32.11.0/24`)
  - WiFiFJFI (všechny AP, web autentizace, VLAN 15, NAT)
- V případě potřeby (konference, . . .) lze zprovoznit další SSID
- Účty v AD (hosté), každá síť vlastní heslo (Eduroam politika)
- Infomace o konfiguraci AP na NMS wiki
- Rozmístění AP v Břehovce, do kdy?
- Požadavky na další pokrytí?

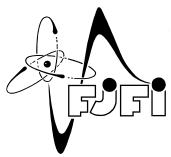


WiFi sítě na FJFI

- Plán pokrytí
  - soukromá AP buď podle plánu nebo na kanál 13
- Dvě standardní sítě s různým zabezpečením
  - Eduroam (pouze na CISCO, VLAN 13, `147.32.11.0/24`)
  - WiFiFJFI (všechny AP, web autentizace, VLAN 15, NAT)
- V případě potřeby (konference, . . .) lze zprovoznit další SSID
- Účty v AD (hosté), každá síť vlastní heslo (Eduroam politika)
- Infomace o konfiguraci AP na NMS wiki
- Rozmístění AP v Břehovce, do kdy?
- Požadavky na další pokrytí?

WiFi sítě na FJFI

- Plán pokrytí
  - soukromá AP buď podle plánu nebo na kanál 13
- Dvě standardní sítě s různým zabezpečením
  - Eduroam (pouze na CISCO, VLAN 13, `147.32.11.0/24`)
  - WiFiFJFI (všechny AP, web autentizace, VLAN 15, NAT)
- V případě potřeby (konference, . . .) lze zprovoznit další SSID
- Účty v AD (hosté), každá síť vlastní heslo (Eduroam politika)
- Infomace o konfiguraci AP na NMS wiki
- Rozmístění AP v Břehovce, do kdy?
- Požadavky na další pokrytí?



WiFi sítě na FJFI

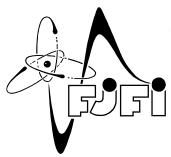
- Plán pokrytí
  - soukromá AP buď podle plánu nebo na kanál 13
- Dvě standardní sítě s různým zabezpečením
  - Eduroam (pouze na CISCO, VLAN 13, `147.32.11.0/24`)
  - WiFiFJFI (všechny AP, web autentizace, VLAN 15, NAT)
- V případě potřeby (konference, . . .) lze zprovoznit další SSID
- Účty v AD (hosté), každá síť vlastní heslo (Eduroam politika)
- Infomace o konfiguraci AP na NMS wiki
- Rozmístění AP v Břehovce, do kdy?
- Požadavky na další pokrytí?

WiFi sítě na FJFI

- Plán pokrytí
  - soukromá AP buď podle plánu nebo na kanál 13
- Dvě standardní sítě s různým zabezpečením
  - Eduroam (pouze na CISCO, VLAN 13, `147.32.11.0/24`)
  - WiFiFJFI (všechny AP, web autentizace, VLAN 15, NAT)
- V případě potřeby (konference, . . .) lze zprovoznit další SSID
- Účty v AD (hosté), každá síť vlastní heslo (Eduroam politika)
- Infomace o konfiguraci AP na NMS wiki
- Rozmístění AP v Břehovce, do kdy?
- Požadavky na další pokrytí?

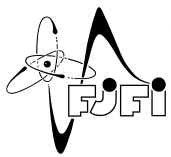
WiFi sítě na FJFI

- Plán pokrytí
  - soukromá AP buď podle plánu nebo na kanál 13
- Dvě standardní sítě s různým zabezpečením
  - Eduroam (pouze na CISCO, VLAN 13, `147.32.11.0/24`)
  - WiFiFJFI (všechny AP, web autentizace, VLAN 15, NAT)
- V případě potřeby (konference, . . .) lze zprovoznit další SSID
- Účty v AD (hosté), každá síť vlastní heslo (Eduroam politika)
- Infomace o konfiguraci AP na NMS wiki
- Rozmístění AP v Břehovce, do kdy?
- Požadavky na další pokrytí?



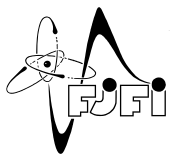
Využití privátních IP rozsahů

- Přerozděleno kvůli routování / firewallů
- 172.16.0.0/16 (fakulta), 192.168.0.0/16 (soukromé)
  - Wiki o využití IP na FJFI
  - Poznamenat sem využívání dalších rozsahů
- Routované nebo bridgované mezi budovami FJFI přes VPN (zvážit pohodlí *x* odolnost pří výpadku (gateway) *x* chování při L2 broadcast storm)
  - Spojovačky, OSPF, ...
  - Management (secure, unsecure)
  - Servery — VLAN 9
  - "Inteligentní" zařízení (tiskárny, ...)
- Lokální sítě v budově
  - default (neregistrované, blokované+smazané)
  - Eduroam (blokované+smazané) — VLAN 13
  - WiFiFJFI (blokované+smazané) — VLAN 15



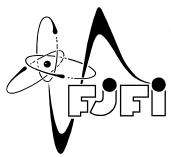
Využití privátních IP rozsahů

- Přerozděleno kvůli routování / firewallů
- `172.16.0.0/16` (fakulta), `192.168.0.0/16` (soukromé)
  - Wiki o využití IP na FJFI
  - Poznamenat sem využívání dalších rozsahů
- Routované nebo bridgované mezi budovami FJFI přes VPN (zvážit pohodlí *x* odolnost pří výpadku (gateway) *x* chování při L2 broadcast storm)
  - Spojovačky, OSPF, ...
  - Management (secure, unsecure)
  - Servery — VLAN 9
  - "Inteligentní" zařízení (tiskárny, ...)
- Lokální sítě v budově
  - default (neregistrované, blokované+smazané)
  - Eduroam (blokované+smazané) — VLAN 13
  - WiFiFJFI (blokované+smazané) — VLAN 15



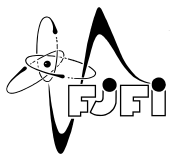
Využití privátních IP rozsahů

- Přerozděleno kvůli routování / firewallů
- `172.16.0.0/16` (fakulta), `192.168.0.0/16` (soukromé)
  - Wiki o využití IP na FJFI
  - Poznamenat sem využívání dalších rozsahů
- Routované nebo bridgované mezi budovami FJFI přes VPN (zvážit pohodlí *x* odolnost pří výpadku (gateway) *x* chování při L2 broadcast storm)
  - Spojovačky, OSPF, ...
  - Management (secure, unsecure)
  - Servery — VLAN 9
  - "Inteligentní" zařízení (tiskárny, ...)
- Lokální sítě v budově
  - default (neregistrované, blokované+smazané)
  - Eduroam (blokované+smazané) — VLAN 13
  - WiFiFJFI (blokované+smazané) — VLAN 15



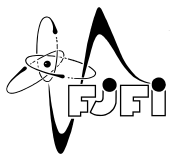
Využití privátních IP rozsahů

- Přerozděleno kvůli routování / firewallů
- `172.16.0.0/16` (fakulta), `192.168.0.0/16` (soukromé)
  - Wiki o využití IP na FJFI
  - Poznamenat sem využívání dalších rozsahů
- Routované nebo bridgované mezi budovami FJFI přes VPN (zvážit pohodlí *x* odolnost pří výpadku (gateway) *x* chování při L2 broadcast storm)
  - Spojovačky, OSPF, ...
  - Management (secure, unsecure)
  - Servery — VLAN 9
  - "Inteligentní" zařízení (tiskárny, ...)
- Lokální sítě v budově
  - default (neregistrované, blokované+smazané)
  - Eduroam (blokované+smazané) — VLAN 13
  - WiFiFJFI (blokované+smazané) — VLAN 15



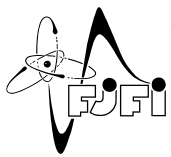
Motivace

- Možnost dohledat problematické stroje
  - Stížnosti abuse (`abuse@cvut.cz`)
  - ČVUT IDS (většinou zavirované, hacklé stroje)
  - Konflikty IP, DHCP, ...
  - Využití adres
- Využití pro lokální konfigurace (DHCP)
- Aktuální stav (problémy) + historie výskytu stanic
- Více informací pro efektivní řešení problémů na síti



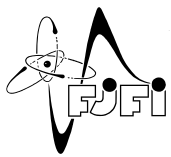
Motivace

- Možnost dohledat problematické stroje
  - Stížnosti abuse (`abuse@cvut.cz`)
  - ČVUT IDS (většinou zavirované, hacklé stroje)
  - Konflikty IP, DHCP, ...
  - Využití adres
- Využití pro lokální konfigurace (DHCP)
- Aktuální stav (problémy) + historie výskytu stanic
- Více informací pro efektivní řešení problémů na síti



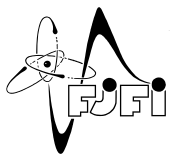
Motivace

- Možnost dohledat problematické stroje
  - Stížnosti abuse (`abuse@cvut.cz`)
  - ČVUT IDS (většinou zavirované, hacklé stroje)
  - Konflikty IP, DHCP, ...
  - Využití adres
- Využití pro lokální konfigurace (DHCP)
- Aktuální stav (problémy) + historie výskytu stanic
- Více informací pro efektivní řešení problémů na síti



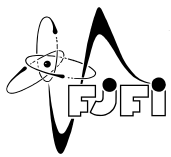
Motivace

- Možnost dohledat problematické stroje
  - Stížnosti abuse (`abuse@cvut.cz`)
  - ČVUT IDS (většinou zavirované, hacklé stroje)
  - Konflikty IP, DHCP, ...
  - Využití adres
- Využití pro lokální konfigurace (DHCP)
- Aktuální stav (problémy) + historie výskytu stanic
- Více informací pro efektivní řešení problémů na síti



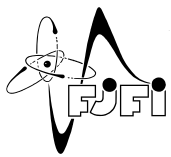
Princip fungování registrací

- Detailní popis na NMS wiki
- Pouze pro ethernet (wireless — automaticky ⇒ VLAN)
- IPv4, IPv6 (pouze blokování)
- Přidělování různých adres od DHCP
  - Neregistrovaná (blokovaná / smazaná) zařízení privátní IP
  - Brána na lokálním NAT stroji (lze clusterovat)
  - Přístup na vybrané stránky bez registrace, z ostatních přesměrování na registrační formulář (tiskárny, . . . — ručně)
  - NAT povolen okamžitě po registraci, příště již veřejná IP
  - Automatický (okamžitý) update DHCP konfigurace
  - Blokovaná / smazaná zařízení nutné řešit se správcem
  - (Ne)potřebné registrační údaje?
- Další možnosti zabezpečení
  - Povolit na CISCO pouze adresy přidělené od DHCP (VLAN)
  - Blokování podle MAC na portech switchů
  - Autentizace LAN zařízení přes RADIUS (“nelze”)



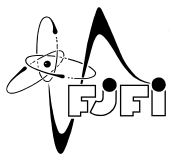
Princip fungování registrací

- Detailní popis na NMS wiki
- Pouze pro ethernet (wireless — automaticky ⇒ VLAN)
- IPv4, IPv6 (pouze blokování)
- Přidělování různých adres od DHCP
  - Neregistrovaná (blokovaná / smazaná) zařízení privátní IP
  - Brána na lokálním NAT stroji (lze clusterovat)
  - Přístup na vybrané stránky bez registrace, z ostatních přesměrování na registrační formulář (tiskárny, . . . — ručně)
  - NAT povolen okamžitě po registraci, příště již veřejná IP
  - Automatický (okamžitý) update DHCP konfigurace
  - Blokovaná / smazaná zařízení nutné řešit se správcem
  - (Ne)potřebné registrační údaje?
- Další možnosti zabezpečení
  - Povolit na CISCO pouze adresy přidělené od DHCP (VLAN)
  - Blokování podle MAC na portech switchů
  - Autentizace LAN zařízení přes RADIUS (“nelze”)



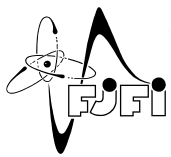
Princip fungování registrací

- Detailní popis na NMS wiki
- Pouze pro ethernet (wireless — automaticky ⇒ VLAN)
- IPv4, IPv6 (pouze blokování)
- Přidělování různých adres od DHCP
  - Neregistrovaná (blokovaná / smazaná) zařízení privátní IP
  - Brána na lokálním NAT stroji (lze clusterovat)
  - Přístup na vybrané stránky bez registrace, z ostatních přesměrování na registrační formulář (tiskárny, . . . — ručně)
  - NAT povolen okamžitě po registraci, příště již veřejná IP
  - Automatický (okamžitý) update DHCP konfigurace
  - Blokovaná / smazaná zařízení nutné řešit se správcem
  - (Ne)potřebné registrační údaje?
- Další možnosti zabezpečení
  - Povolit na CISCO pouze adresy přidělené od DHCP (VLAN)
  - Blokování podle MAC na portech switchů
  - Autentizace LAN zařízení přes RADIUS (“nelze”)



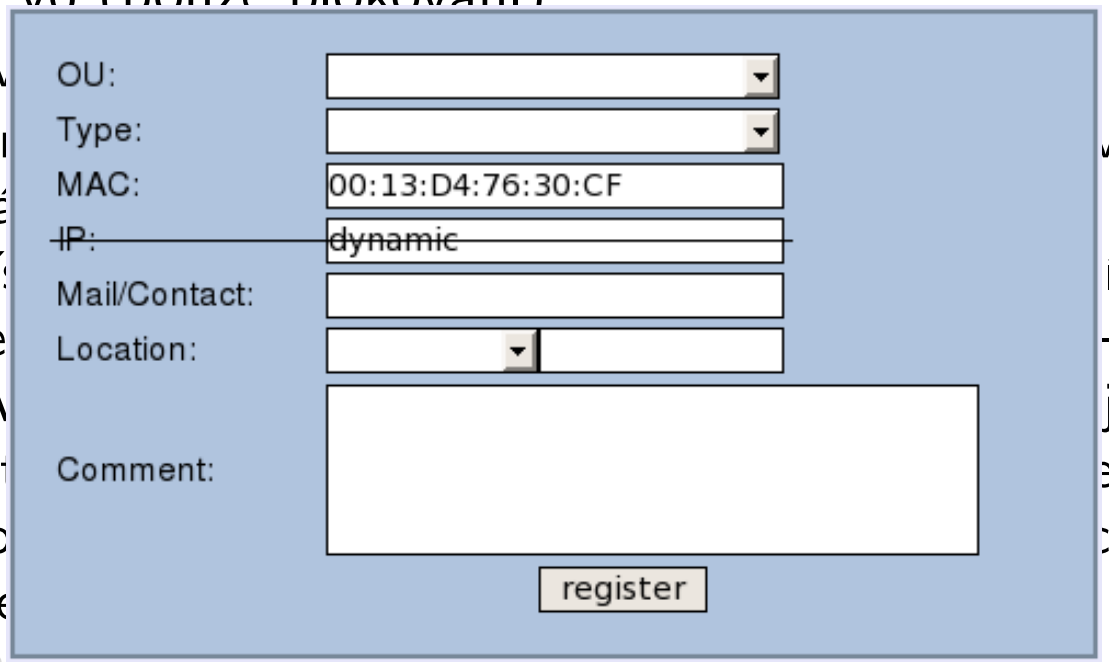
Princip fungování registrací

- Detailní popis na NMS wiki
- Pouze pro ethernet (wireless — automaticky ⇒ VLAN)
- IPv4, IPv6 (pouze blokování)
- Přidělování různých adres od DHCP
  - Neregistrovaná (blokovaná / smazaná) zařízení privátní IP
  - Brána na lokálním NAT stroji (lze clusterovat)
  - Přístup na vybrané stránky bez registrace, z ostatních přesměrování na registrační formulář (tiskárny, . . . — ručně)
  - NAT povolen okamžitě po registraci, příště již veřejná IP
  - Automatický (okamžitý) update DHCP konfigurace
  - Blokovaná / smazaná zařízení nutné řešit se správcem
  - (Ne)potřebné registrační údaje?
- Další možnosti zabezpečení
  - Povolit na CISCO pouze adresy přidělené od DHCP (VLAN)
  - Blokování podle MAC na portech switchů
  - Autentizace LAN zařízení přes RADIUS (“nelze”)



Princip fungování registrací

- Detailní popis na NMS wiki
- Pouze pro ethernet (wireless — automaticky ⇒ VLAN)
- IPv4, IPv6 (pouze blokování)
- Přidělov
  - Ne
  - Brá
  - Pří
    pře
  - NA
  - Au
  - Blo
  - (Ne



vátní IP

ích

— ručně)

jná IP

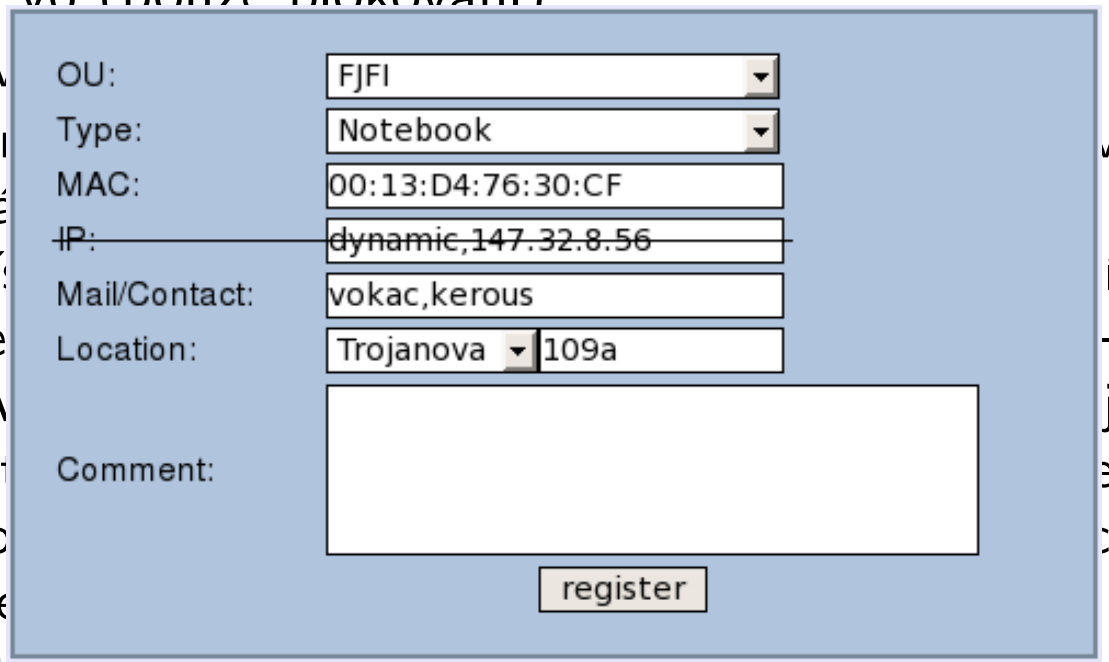
e

cem

- Další možnosti zabezpečení
  - Povolit na CISCO pouze adresy přidělené od DHCP (VLAN)
  - Blokování podle MAC na portech switchů
  - Autentizace LAN zařízení přes RADIUS (“nelze”)

Princip fungování registrací

- Detailní popis na NMS wiki
- Pouze pro ethernet (wireless — automaticky ⇒ VLAN)
- IPv4, IPv6 (pouze blokování)
- Přidělov
  - Ne
  - Brá
  - Pří
    pře
  - NA
  - Au
  - Blo
  - (Ne



vátní IP

ích

— ručně)

jná IP

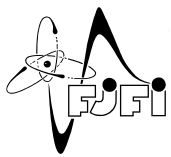
e

cem

- Další možnosti zabezpečení
  - Povolit na CISCO pouze adresy přidělené od DHCP (VLAN)
  - Blokování podle MAC na portech switchů
  - Autentizace LAN zařízení přes RADIUS (“nelze”)

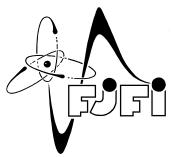
Princip fungování registrací

- Detailní popis na NMS wiki
- Pouze pro ethernet (wireless — automaticky ⇒ VLAN)
- IPv4, IPv6 (pouze blokování)
- Přidělování různých adres od DHCP
  - Neregistrovaná (blokovaná / smazaná) zařízení privátní IP
  - Brána na lokálním NAT stroji (lze clusterovat)
  - Přístup na vybrané stránky bez registrace, z ostatních přesměrování na registrační formulář (tiskárny, . . . — ručně)
  - NAT povolen okamžitě po registraci, příště již veřejná IP
  - Automatický (okamžitý) update DHCP konfigurace
  - Blokovaná / smazaná zařízení nutné řešit se správcem
  - (Ne)potřebné registrační údaje?
- Další možnosti zabezpečení
  - Povolit na CISCO pouze adresy přidělené od DHCP (VLAN)
  - Blokování podle MAC na portech switchů
  - Autentizace LAN zařízení přes RADIUS (“nelze”)



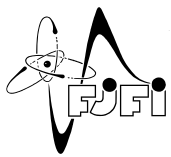
Informace o zařízení

- OU, typ, (evidenční číslo), heslo, umístění (budova, místnost), status (trusted, untrusted, blocked, deleted), poznámka
- Správci, vlastníci, . . . $(0 - \infty$, různá práva)
- Síťová rozhraní
  - MAC, Switch/port, poznámka
  - Adresa(y) pro každé rozhraní (dynamic, IP, IPv6)
- Vyhledávání zařízení v databázi
- Detekce konfliktních IP a MAC adres
- Generování grafu sítě
- Odkazy na ipstat, konfiguraci DNS, nastavení switchů, . . .



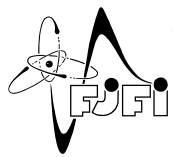
Informace o zařízení

- OU, typ, (evidenční číslo), heslo, umístění (budova, místnost), status (trusted, untrusted, blocked, deleted), poznámka
- Správci, vlastníci, ... $(0 - \infty$, různá práva)
- Síťová rozhraní
  - MAC, Switch/port, poznámka
  - Adresa(y) pro každé rozhraní (dynamic, IP, IPv6)
- Vyhledávání zařízení v databázi
- Detekce konfliktních IP a MAC adres
- Generování grafu sítě
- Odkazy na ipstat, konfiguraci DNS, nastavení switchů, ...



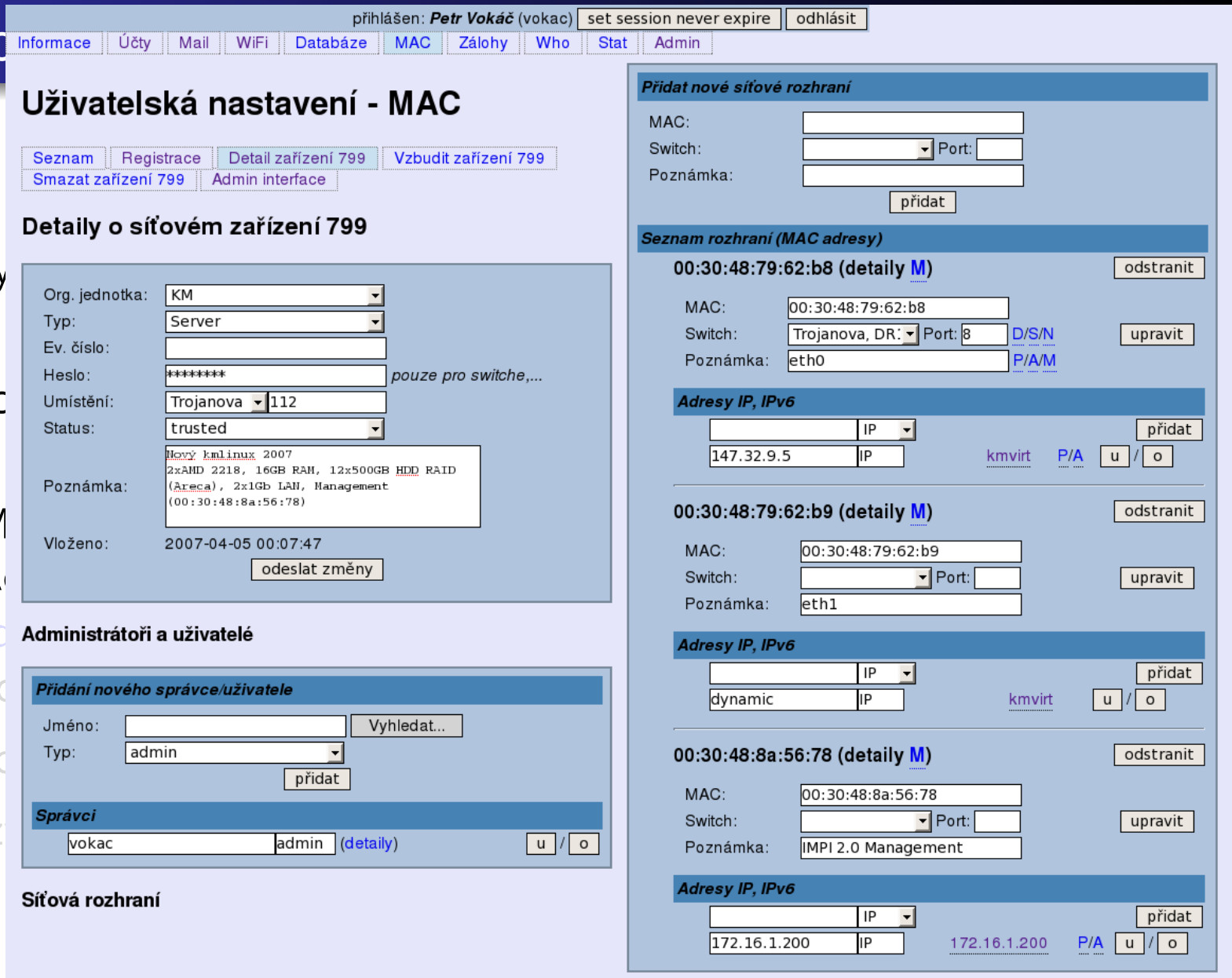
Informace o zařízení

- OU, typ, (evidenční číslo), heslo, umístění (budova, místnost), status (trusted, untrusted, blocked, deleted), poznámka
- Správci, vlastníci, ... $(0 - \infty$, různá práva)
- Síťová rozhraní
  - MAC, Switch/port, poznámka
  - Adresa(y) pro každé rozhraní (dynamic, IP, IPv6)
- Vyhledávání zařízení v databázi
- Detekce konfliktních IP a MAC adres
- Generování grafu sítě
- Odkazy na ipstat, konfiguraci DNS, nastavení switchů, ...



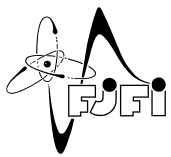
Informace o

- OU, ty
  status
- Správc
- Síťová
  - M
  - A
- Vyhled
- Deteko
- Generc
- Odkaz



Informace o zařízení

- OU, typ, (evidenční číslo), heslo, umístění (budova, místnost), status (trusted, untrusted, blocked, deleted), poznámka
- Správci, vlastníci, ... $(0 - \infty$, různá práva)
- Síťová rozhraní
  - MAC, Switch/port, poznámka
  - Adresa(y) pro každé rozhraní (dynamic, IP, IPv6)
- Vyhledávání zařízení v databázi
- Detekce konfliktních IP a MAC adres
- Generování grafu sítě
- Odkazy na ipstat, konfiguraci DNS, nastavení switchů, ...

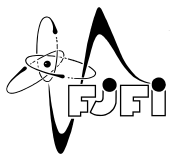


Informace o zařízení

- OU, typ … místnost), status (… mka
- Správci,
- Síťová r
  - MA
  - Adr
- Vyhledá
- Detekce
- Generov
- Odkazy na ipstat, konfiguraci DNS, nastavení switchů, . . .

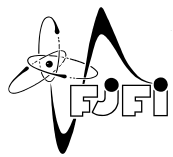
Informace o zařízení

- OU, typ, (evidenční číslo), heslo, umístění (budova, místnost), status (trusted, untrusted, blocked, deleted), poznámka
- Správci, vlastníci, ... $(0 - \infty$, různá práva)
- Síťová rozhraní
  - MAC, Switch/port, poznámka
  - Adresa(y) pro každé rozhraní (dynamic, IP, IPv6)
- Vyhledávání zařízení v databázi
- Detekce konfliktních IP a MAC adres
- Generování grafu sítě
- Odkazy na ipstat, konfiguraci DNS, nastavení switchů, ...



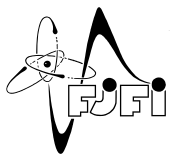
Informace o zařízení

- OU, typ, (evidenční číslo), heslo, umístění (budova, místnost), status (trusted, untrusted, blocked, deleted), poznámka
- Správci, vlastníci, ... $(0 - \infty$, různá práva)
- Síťová rozhraní
  - MAC, Switch/port, poznámka
  - Adresa(y) pro každé rozhraní (dynamic, IP, IPv6)
- Vyhledávání zařízení v databázi
- Detekce konfliktních IP a MAC adres
- Generování grafu sítě
- Odkazy na ipstat, konfiguraci DNS, nastavení switchů, ...



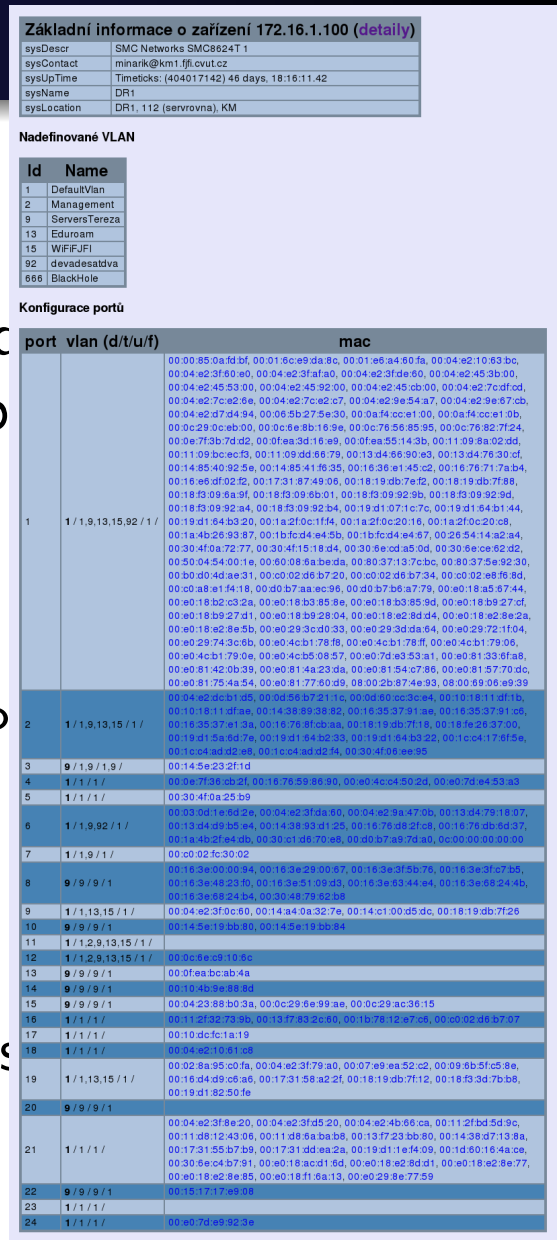
Informace o zařízení

- OU, typ, (evidenční číslo), heslo, umístění (budova, místnost), status (trusted, untrusted, blocked, deleted), poznámka
- Správci, vlastníci, ... $(0 - \infty$, různá práva)
- Síťová rozhraní
  - MAC, Switch/port, poznámka
  - Adresa(y) pro každé rozhraní (dynamic, IP, IPv6)
- Vyhledávání zařízení v databázi
- Detekce konfliktních IP a MAC adres
- Generování grafu sítě
- Odkazy na ipstat, konfiguraci DNS, nastavení switchů, ...



Informace o zařízení

- OU, typ, (evidenční číslo), heslo, umístění (buc
  status (trusted, untrusted, blocked, deleted), p
- Správci, vlastníci, . . . ($0 - \infty$, různá práva)
- Síťová rozhraní
  - MAC, Switch/port, poznámka
  - Adresa(y) pro každé rozhraní (dynamic, IP, IP
- Vyhledávání zařízení v databázi
- Detekce konfliktních IP a MAC adres
- Generování grafu sítě
- Odkazy na ipstat, konfiguraci DNS, nastavení s



Základní informace o zařízení 172.16.1.100 (detaily)

sysDescr	SMC Networks SMC8624T 1
sysContact	minarik@km1.fjfi.cvut.cz
sysUpTime	Timeticks: (404017142) 46 days, 18:16:11.42
sysName	DR1
sysLocation	DR1, 112 (servrovna), KM

Nadefinované VLAN

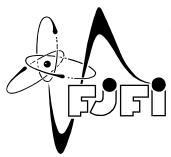
Id	Name
1	DefaultVlan
2	Management
9	ServersTereza
13	Eduroam
15	WiFiFJFI
92	devadesatdva
666	BlackHole

Konfigurace portů

port	vlan (d/t/u/f)	mac
1	**1** / 1,9,13,15,92 / 1 /	00:00:85:0a:fd:bf, 00:01:6c:e9:da:8c, 00:01:e6:a4:60:fa, 00:04:e2:10:63:bc, 00:04:e2:3f:60:e0, 00:04:e2:3f:af:a0, 00:04:e2:3f:de:60, 00:04:e2:45:3b:00, 00:04:e2:45:53:00, 00:04:e2:45:92:00, 00:04:e2:45:cb:00, 00:04:e2:7c:df:cd, 00:04:e2:7c:e2:6e, 00:04:e2:7c:e2:c7, 00:04:e2:9e:54:a7, 00:04:e2:9e:67:cb, 00:04:e2:d7:d4:94, 00:06:5b:27:5e:30, 00:0a:f4:cc:e1:00, 00:0a:f4:cc:e1:0b, 00:0c:29:0c:eb:00, 00:0c:6e:8b:16:9e, 00:0c:76:56:85:95, 00:0c:76:82:7f:24, 00:0e:7f:3b:7d:d2, 00:0f:ea:3d:16:e9, 00:0f:ea:55:14:3b, 00:11:09:8a:02:dd, 00:11:09:bc:ec:f3, 00:11:09:dd:66:79, 00:13:d4:66:90:e3, 00:13:d4:76:30:cf, 00:14:85:40:92:5e, 00:14:85:41:f6:35, 00:16:36:e1:45:c2, 00:16:76:71:7a:b4, 00:16:e6:df:02:f2, 00:17:31:87:49:06, 00:18:19:db:7e:f2, 00:18:19:db:7f:88, 00:18:f3:09:8a:9f, 00:18:f3:09:8b:01, 00:18:f3:09:92:9b, 00:18:f3:09:92:9d, 00:18:f3:09:92:a4, 00:18:f3:09:92:b4, 00:19:d1:07:1c:7c, 00:19:d1:64:b1:44, 00:19:d1:64:b3:20, 00:1a:2f:0c:1f:f4, 00:1a:2f:0c:20:16, 00:1a:2f:0c:20:c8, 00:1a:4b:26:93:87, 00:1b:fc:d4:e4:5b, 00:1b:fc:d4:e4:67, 00:26:54:14:a2:a4, 00:30:4f:0a:72:77, 00:30:4f:15:18:d4, 00:30:6e:cd:a5:0d, 00:30:6e:ce:62:d2, 00:50:04:54:00:1e, 00:60:08:6a:be:da, 00:80:37:13:7c:bc, 00:80:37:5e:92:30, 00:b0:d0:4d:ae:31, 00:c0:02:d6:b7:20, 00:c0:02:d6:b7:34, 00:c0:02:e8:f6:8d, 00:c0:a8:e1:f4:18, 00:d0:b7:aa:ec:96, 00:d0:b7:b6:a7:79, 00:e0:18:a5:67:44, 00:e0:18:b2:c3:2a, 00:e0:18:b3:85:8e, 00:e0:18:b3:85:9d, 00:e0:18:b9:27:cf, 00:e0:18:b9:27:d1, 00:e0:18:b9:28:04, 00:e0:18:e2:8d:d4, 00:e0:18:e2:8e:2a, 00:e0:18:e2:8e:5b, 00:e0:29:3c:d0:33, 00:e0:29:3d:da:64, 00:e0:29:72:1f:04, 00:e0:29:74:3c:6b, 00:e0:4c:b1:78:f8, 00:e0:4c:b1:78:ff, 00:e0:4c:b1:79:06, 00:e0:4c:b1:79:0e, 00:e0:4c:b5:08:57, 00:e0:7d:e3:53:a1, 00:e0:81:33:6f:a8, 00:e0:81:42:0b:39, 00:e0:81:4a:23:da, 00:e0:81:54:c7:86, 00:e0:81:57:70:dc, 00:e0:81:75:4a:54, 00:e0:81:77:60:d9, 08:00:2b:87:4e:93, 08:00:69:06:e9:39
2	**1** / 1,9,13,15 / 1 /	00:04:e2:dc:b1:d5, 00:0d:56:b7:21:1c, 00:0d:60:cc:3c:e4, 00:10:18:11:df:1b, 00:10:18:11:df:ae, 00:14:38:89:38:82, 00:16:35:37:91:ae, 00:16:35:37:91:c6, 00:16:35:37:e1:3a, 00:16:76:8f:cb:aa, 00:18:19:db:7f:18, 00:18:fe:26:37:00, 00:19:d1:5a:6d:7e, 00:19:d1:64:b2:33, 00:19:d1:64:b3:22, 00:1c:c4:17:6f:5e, 00:1c:c4:ad:d2:e8, 00:1c:c4:ad:d2:f4, 00:30:4f:06:ee:95
3	**9** / 1,9 / 1,9 /	00:14:5e:23:2f:1d
4	**1** / 1 / 1 /	00:0e:7f:36:cb:2f, 00:16:76:59:86:90, 00:e0:4c:c4:50:2d, 00:e0:7d:e4:53:a3
5	**1** / 1 / 1 /	00:30:4f:0a:25:b9
6	**1** / 1,9,92 / 1 /	00:03:0d:1e:6d:2e, 00:04:e2:3f:da:60, 00:04:e2:9a:47:0b, 00:13:d4:79:18:07, 00:13:d4:d9:b5:e4, 00:14:38:93:d1:25, 00:16:76:d8:2f:c8, 00:16:76:db:6d:37, 00:1a:4b:2f:e4:db, 00:30:c1:d6:70:e8, 00:d0:b7:a9:7d:a0, 0c:00:00:00:00:00
7	**1** / 1,9 / 1 /	00:c0:02:fc:30:02
8	**9** / 9 / 9 / 1	00:16:3e:00:00:94, 00:16:3e:29:00:67, 00:16:3e:3f:5b:76, 00:16:3e:3f:c7:b5, 00:16:3e:48:23:f0, 00:16:3e:51:09:d3, 00:16:3e:63:44:e4, 00:16:3e:68:24:4b, 00:16:3e:68:24:b4, 00:30:48:79:62:b8
9	**1** / 1,13,15 / 1 /	00:04:e2:3f:0c:60, 00:14:a4:0a:32:7e, 00:14:c1:00:d5:dc, 00:18:19:db:7f:26
10	**9** / 9 / 9 / 1	00:14:5e:19:bb:80, 00:14:5e:19:bb:84
11	**1** / 1,2,9,13,15 / 1 /	
12	**1** / 1,2,9,13,15 / 1 /	00:0c:6e:c9:10:6c
13	**9** / 9 / 9 / 1	00:0f:ea:bc:ab:4a
14	**9** / 9 / 9 / 1	00:10:4b:9e:88:8d
15	**9** / 9 / 9 / 1	00:04:23:88:b0:3a, 00:0c:29:6e:99:ae, 00:0c:29:ac:36:15
16	**1** / 1 / 1 /	00:11:2f:32:73:9b, 00:13:f7:83:2c:60, 00:1b:78:12:e7:c6, 00:c0:02:d6:b7:07
17	**1** / 1 / 1 /	00:10:dc:fc:1a:19
18	**1** / 1 / 1 /	00:04:e2:10:61:c8
19	**1** / 1,13,15 / 1 /	00:02:8a:95:c0:fa, 00:04:e2:3f:79:a0, 00:07:e9:ea:52:c2, 00:09:6b:5f:c5:8e, 00:16:d4:d9:c6:a6, 00:17:31:58:a2:2f, 00:18:19:db:7f:12, 00:18:f3:3d:7b:b8, 00:19:d1:82:50:fe
20	**9** / 9 / 9 / 1	
21	**1** / 1 / 1 /	00:04:e2:3f:8e:20, 00:04:e2:3f:d5:20, 00:04:e2:4b:66:ca, 00:11:2f:bd:5d:9c, 00:11:d8:12:43:06, 00:11:d8:6a:ba:b8, 00:13:f7:23:bb:80, 00:14:38:d7:13:8a, 00:17:31:55:b7:b9, 00:17:31:dd:ea:2a, 00:19:d1:1e:f4:09, 00:1d:60:16:4a:ce, 00:30:6e:c4:b7:91, 00:e0:18:ac:d1:6d, 00:e0:18:e2:8d:d1, 00:e0:18:e2:8e:77, 00:e0:18:e2:8e:85, 00:e0:18:f1:6a:13, 00:e0:29:8e:77:59
22	**9** / 9 / 9 / 1	00:15:17:17:e9:08
23	**1** / 1 / 1 /	
24	**1** / 1 / 1 /	00:e0:7d:e9:32:3e

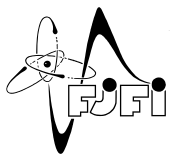
ARP monitoring daemon (Arpmon)

- Monitorování výskytu stanic (IP) na síti, detaily na NMS wiki
  - Historie výskytu zařízení na síti
  - Neregistrovaná zařízení
  - Špatné registrace (IP adresa)
  - Konflikty IP — není 100% (jeden vlastník, rezervace IP)
  - Neschválené DHCP servery
- L2 resp. L3 broadcast ⇒ poslouchá v každém subnetu
- Reporty
  - Rozesílány mailem na správce subnetu, admina zařízení
  - Obsahují info a odkazy (ipstat, registrace, . . .)
  - Lze definovat, komu mají chodit dané typy reportů — jaké?
  - Je možné individuálně umlčet libovolné konkrétní reporty



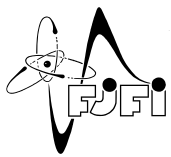
ARP monitoring daemon (Arpmon)

- Monitorování výskytu stanic (IP) na síti, detaily na NMS wiki
  - Historie výskytu zařízení na síti
  - Neregistrovaná zařízení
  - Špatné registrace (IP adresa)
  - Konflikty IP — není 100% (jeden vlastník, rezervace IP)
  - Neschválené DHCP servery
- L2 resp. L3 broadcast $\Rightarrow$ poslouchá v každém subnetu
- Reporty
  - Rozesílány mailem na správce subnetu, admina zařízení
  - Obsahují info a odkazy (ipstat, registrace, ...)
  - Lze definovat, komu mají chodit dané typy reportů — jaké?
  - Je možné individuálně umlčet libovolné konkrétní reporty



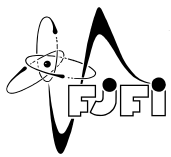
ARP monitoring daemon (Arpmon)

- Monitorování výskytu stanic (IP) na síti, detaily na NMS wiki
  - Historie výskytu zařízení na síti
  - Neregistrovaná zařízení
  - Špatné registrace (IP adresa)
  - Konflikty IP — není 100% (jeden vlastník, rezervace IP)
  - Neschválené DHCP servery
- L2 resp. L3 broadcast $\Rightarrow$ poslouchá v každém subnetu
- Reporty
  - Rozesílány mailem na správce subnetu, admina zařízení
  - Obsahují info a odkazy (ipstat, registrace, ...)
  - Lze definovat, komu mají chodit dané typy reportů — jaké?
  - Je možné individuálně umlčet libovolné konkrétní reporty



Postup při řešení stížností

- Má na starosti správce budovy (P.S., M.M., O.K., P.B.)
- V nornálních případech kontaktovat uživatele adresu uvedenou při registraci
  - Jak reagovat na různé typy stížností?
  - Požadovat replay? Jak dlouho čekat?
  - Zablokovat nebo počkat na další stížnost?
  - Jak si v tom udržet přehled?
- V urgentních případech zablokovat (jak? switch x DHCP)
- Řešení CESNETích ticketů vyžadujících replay na NMS wiki



Postup při řešení stížností

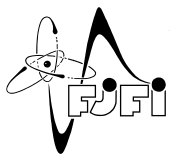
- Má na starosti správce budovy (P.S., M.M., O.K., P.B.)
- V nornálních případech kontaktovat uživatele adresu uvedenou při registraci
  - Jak reagovat na různé typy stížností?
  - Požadovat replay? Jak dlouho čekat?
  - Zablokovat nebo počkat na další stížnost?
  - Jak si v tom udržet přehled?
- V urgentních případech zablokovat (jak? switch x DHCP)
- Řešení CESNETích ticketů vyžadujících replay na NMS wiki

Postup při řešení stížností

- Má na starosti správce budovy (P.S., M.M., O.K., P.B.)
- V nornálních případech kontaktovat uživatele adresu uvedenou při registraci
  - Jak reagovat na různé typy stížností?
  - Požadovat replay? Jak dlouho čekat?
  - Zablokovat nebo počkat na další stížnost?
  - Jak si v tom udržet přehled?
- V urgentních případech zablokovat (jak? switch x DHCP)
- Řešení CESNETích ticketů vyžadujících replay na NMS wiki

Postup při řešení stížností

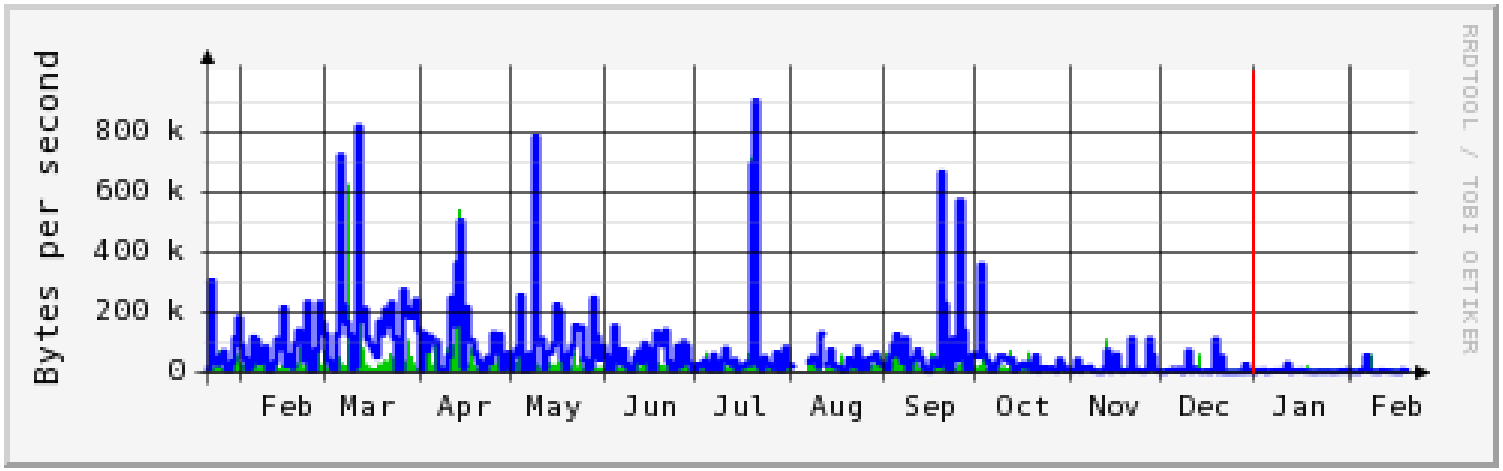
- Má na starosti správce budovy (P.S., M.M., O.K., P.B.)
- V nornálních případech kontaktovat uživatele adresu uvedenou při registraci
  - Jak reagovat na různé typy stížností?
  - Požadovat replay? Jak dlouho čekat?
  - Zablokovat nebo počkat na další stížnost?
  - Jak si v tom udržet přehled?
- V urgentních případech zablokovat (jak? switch x DHCP)
- Řešení CESNETích ticketů vyžadujících replay na NMS wiki



Random notes I

- Trója, Břehovka — dohodnout termíny
  - Konec provozu `tjn`? Převodka? Využití fileserverů (net, I/O, ...)? Info mail uživatelům (data, mail, web)?
  - Iméno Windows v Tróji (troja ⇒ rekonfigurace Novellu)

`Yearly' Graph (1 Day Average) - NET - tjn.fjfi.cvut.cz

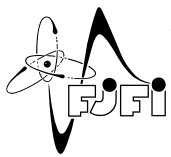


Max In: 787.3 kB/s (0.6%) Average In: 29.2 kB/s (0.0%) Current In: 4334.2 B/s (0.0%)
Max Out: 904.2 kB/s (0.7%) Average Out: 63.9 kB/s (0.1%) Current Out: 5816.9 B/s (0.0%)

- M
- (Ne)používané skupiny resp. používat ty "oficiální"
- Perfomance — 700 lokálně zbytek frw. (stu 3/4, emp 1/5)
- Preferovat — jmeno.prijmeni@fjfi, username@fjfi, ...

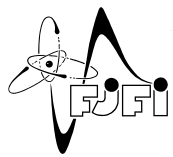
Random notes I

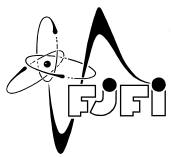
- Trója, Břehovka — dohodnout termíny
  - Konec provozu `tjn`? Převodka? Využití fileserverů (net, I/O, ...)? Info mail uživatelům (data, mail, web)?
  - Jméno Windows v Tróji (`troja` ⇒ rekonfigurace Novellu)
  - Registrace MAC (jak DHCP v Tróji), kdy spustit?
  - Zapojení a přístup na switche/AP (Břehovka, Trója)
  - Využití IP rozsahů (Břehovka, Trója), dokumentace sítě
- Mail
  - Usermap — vymlátit @km1, @troja, @br, @kmat? Zaškrtit IP.
  - Hromadné maily — throtling?
  - Bounces pro forwardované maily (problém se spamy — rbl)
  - Mailing list *x* distribuční seznam na Exchange
  - Konfigurace na NMS (způsob aplikace forwardu na mailgw)
  - Automatický přesun spamu do "Junk folder" na Exchange?
  - (Ne)používané skupiny resp. používat ty "oficiální"
  - Perfomance — 700 lokálně zbytek frw. (stu 3/4, emp 1/5)
  - Preferovat — `jmeno.prijmeni@fjfi`, `username@fjfi`, ...



Random notes I

- Trója, Břehovka — dohodnout termíny
  - Konec provozu `tjn`? Převodka? Využití fileserverů (net, I/O, ...)? Info mail uživatelům (data, mail, web)?
  - Jméno Windows v Tróji (`troja` ⇒ rekonfigurace Novellu)
  - Registrace MAC (jak DHCP v Tróji), kdy spustit?
  - Zapojení a přístup na switche/AP (Břehovka, Trója)
  - Využití IP rozsahů (Břehovka, Trója), dokumentace sítě
- Mail
  - Usermap — vymlátit @km1, @troja, @br, @kmat? Zaškrtit IP.
  - Hromadné maily — throtling?
  - Bounces pro forwardované maily (problém se spamy — rbl)
  - Mailing list *x* distribuční seznam na Exchange
  - Konfigurace na NMS (způsob aplikace forwardu na mailgw)
  - Automatický přesun spamu do "Junk folder" na Exchange?
  - (Ne)používané skupiny resp. používat ty "oficiální"
  - Perfomance — 700 lokálně zbytek frw. (stu 3/4, emp 1/5)
  - Preferovat — `jmeno.prijmeni@fjfi`, `username@fjfi`, ...



Random notes II

- Informace a dokumentace
  - Jak udržet platné údaje v Usermapu (telefon, místnost, . . .)
  - Platný mail na všechny studenty? (při zápisu? průkaz?)
  - Revize dokumentů “pro prváky” (web, nástěnky, studijní, . . .), datum vydání a verzování
- rrn
  - Rozmístění AP v Břehovce
  - Backup (`trarch`, `tjnarch`), rozdělení domény na sites, podivné účty jako např. děkan, . . .
  - Fakultní Windows Terminal Server, VPN Server, . . .
  - Zabezpečení zásuvek na veřejně přístupných místech? 802.1x?
  - “Inteligentní” zařízení na přivátní síť nebo za firewall
  - Přístup k domovským adresářům (vědí správci?)
  - Uživatelské www stránky zakládat individuálně (rozhraní na NMS), individuální URL?
  - ČVUT Identity Management — získat info
  - Single Point of Failure