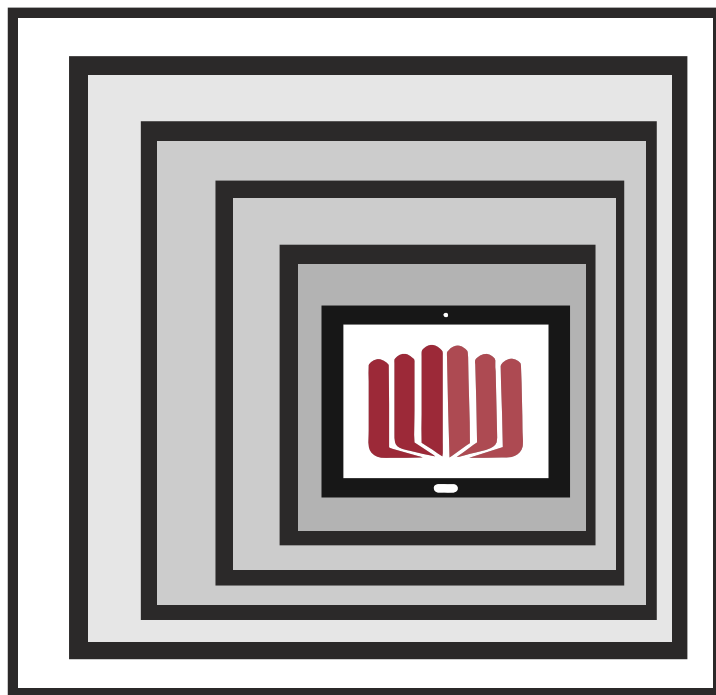
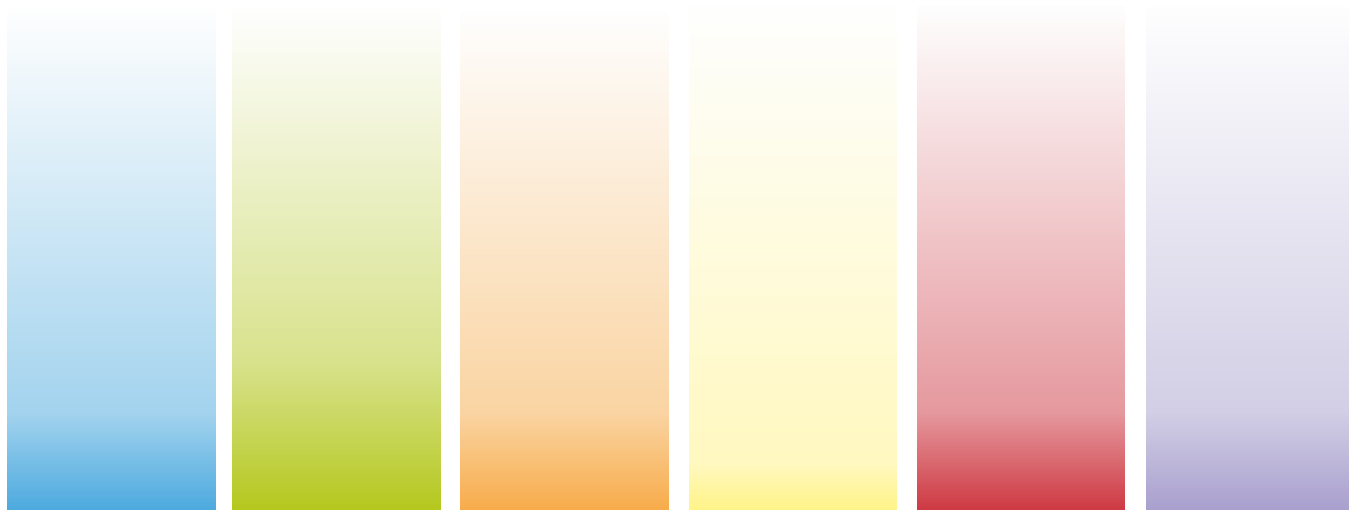


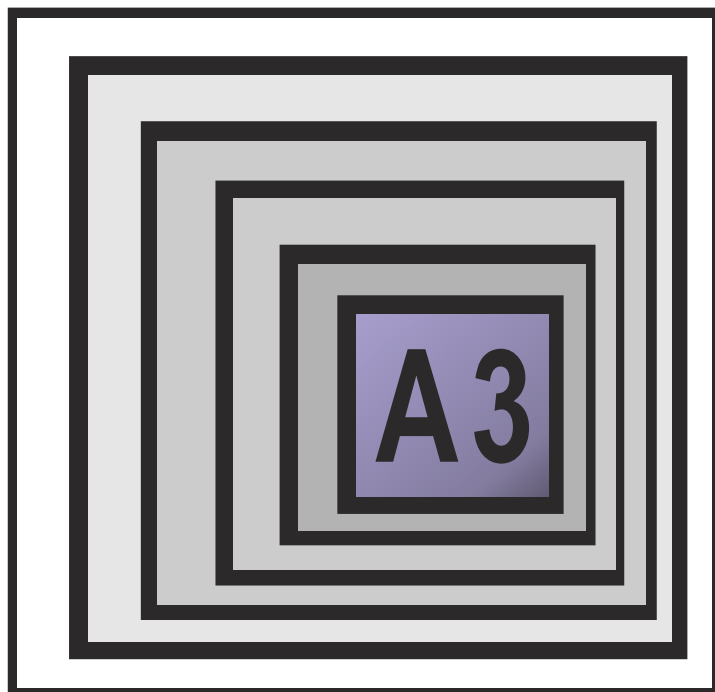
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ



Kantor Ideál

ZÁKLADY SPRÁVY SÍTÍ A ŠKOLNÍ INFRASTRUKTURY





ZÁKLADY SPRÁVY SÍTÍ A ŠKOLNÍ INFRASTRUKTURY

OBSAH

Základy správy sítí a školní infrastruktury.	3
Fyzická kabeláž.	3
Fyzická topologie	4
Logické rozdělení VLAN v typické školní síti	4
Inteligentní switche a jejich nastavení	5
Centrální počítač	8
Pravidla pro centrální počítač a/nebo firewall	9
Přístup z vnějšku	11
Centrální správa bezdrátové sítě s více AP	16
Školní DHCP server	21
Školní DNS server.	24
Bootserver	25
Klonování disků/diskových oddílů po síti	30
Systémy sledování sítě.	30
Analogová a VOIP telefonie.	37
Kamerové systémy	38
Centrální správa uživatelů, skupin a oprávnění pomocí Active Directory .	38
Interakce Active Directory s Office365 nebo s Google Apps	45
Centrální správa tiskáren a kopírek	47
Správa menších databází	51
Centrální správa antiviru	55
Virtualizace serverů	56
Databáze pro vedení školní agendy	63

Základy správy sítí a školní infrastruktury

Fyzická kabeláž

Fyzická kabeláž se nejčastěji realizuje z UTP (Unshielded Twisted Pair, nestíněná kroucená dvojlinka) kategorie 5e či 6, délka segmentu do 100 metrů. Kategorie 5e hraničně zvládá i 1Gbps (1000BaseT), ale je nutno brát ohled na kvalitu a délku kabeláže, pro gigabit je lepší mít kat. 6 (ten pracuje na 200 MHz, oproti 100MHzové kat. 5e).

Stínění (STP kabel) až na velmi ojedinělé případy rušení není nutný.

V kabelu je 8 žil (4 samostatně kroucené páry), skládáme-li je do konektoru (RJ-45), je nutné dodržet schéma T568B (čteno z ploché strany, tak aby nám „zobáček nezavazela při čtení“): O/2, O, Z/2, M, M/2, Z, H/2, H. (O=oranžová, Z=zelená, M=modrá, H=hnědá, značka /2 znamená polobarevný polobílý).



Zdroj obr.: http://cs.wikipedia.org/wiki/RJ-45#mediaviewer/File:RJ45_standardni_zapojeni.gif

Teoreticky, zapojujeme-li proti sobě dva počítače se starší síťovou kartou (nikoliv jeden PC do switchu), je nutné místo rovného kabelu vyrobit tzv. překřížený, aby byly na jedné straně prohozeny oranžové a zelené kabely, tedy Z/2, Z, O/2, M, M/2, O, H/2, H. Karty novější než 3 roky už AutoNegotiation (pod zkratkou MDI-X) umějí.

Informace při 100Mbps proudí pouze po O/2, O, Z/2, Z kabelech => v případě, kdy je to opravdu, ale opravdu nezbytné, lze zbylé žíly „ukrást“ pro další linku – například telefon nebo opět data (vše ovšem běží výrazně pomaleji a „bez záruky“). Viz obr. „profi rozdělovátka“ níže.

Pro srovnání: Dle normy má telefonní konektor RJ-11 pouze čtyři žíly, z čehož se pro telefon využívají prostřední modré dvě – proto jsou u RJ-45 prázdné, aby do RJ-45 zásuvky šlo zastrčit telefonní RJ-11 zástrčku a spojit tak prostřední čtyři linky.



Obr.: Vlevo standardní RJ45 zástrčka, vpravo „profi rozdělovátka“, které z osmi žil udělá 2x4 žíly.

Zdroje obr.: http://cs.wikipedia.org/wiki/Ethernet#P.C5.99.C3.ADm.C3.BD_a_k.C5.99.C3.AD.C5.BEen.C3.BD_kabel, http://www.tsbohemia.cz/solarix-rozdvojka-pocitac-pocitac-2-x-rj45-utp-t-mod-3-u5_d125182.html

Obyčejné krimpovací kleště lze koupit do 500 Kč a není až tak těžké se naučit krimpovat (=připevňovat konektor RJ-45 na kabel UTP).

Fyzická topologie

Obvyklá topologie je stromová či hvězdicová. Ideální stav je jeden centrální switch, do nějž se zapojí servery+další switche, které pak vedou k uživatelům. (Pravidlo: Nikdy ne víc než tři switche pod sebou: centrální, rozdělovací, v kabinetě.)

Při zapojování více budov do jedné LAN lze použít optický kabel, „tenký“ v budovách či „tlustý“ v exteriéru. Optický kabel je jednosměrný, proto stavíme fyzickou topologii kruh (dvouprvkový kruh = dva kabely mezi dvěma stanovišti; víceprvkový kruh = jeden kabel po obvodu kruhu, světlo proudí jedním směrem, např. jen po směru hodinových ručiček).

Logické rozdělení VLAN v typické školní síti

Proč dělit síť do VLAN?

I přes fyzickou kabeláž vedenou do společných switchů lze síť logicky rozdělit do několika částí, tzv. VLANů: pro informatické učebny, pro ostatní učebny, pro wifi, pro kabinety, pro sekretariát, pro servery, pro management sítě, pro vnější přístupy do sítě.

Každému VLANu můžeme měnit chování: Poběží v něm multicast vysílání (=vysílání z jednoho zdroje po celém VLANu pro všechny stanice)? Uvidí se jednotlivé stroje mezi sebou? Dostanou se na Internet? Omezíme jim rychlost přístupu k Internetu? Dostanou se do ostatních VLANů, případně do kterých?

Propojení VLANů mezi sebou ideálně řeší jeden centrální počítač – viz samostatná kapitola o něm níže. Ten funguje i jako brána (gateway, gw), kudy se stanice ze své virtuální lokální sítě dostanou ven do ostatních virtuálních lokálních sítí, případně do Internetu.

Příklad rozdělení sítě do VLANů

VLAN	IP adresy	netmask	gw	popis
100	172.20.0.0	255.255.255.0	172.20.0.254	SERVERY_EXT
101	172.20.1.0	255.255.255.0	172.20.1.254	SERVERY_INT
102	172.20.2.0	255.255.255.0	172.20.2.254	TISKARNY
103	172.20.3.0	255.255.255.0	172.20.3.254	MANAGEMENT
104	172.20.4.0	255.255.255.0	172.20.4.254	KABINETY
110	172.20.10.0	255.255.255.0	172.20.10.254	OST_UCEBNY
111	172.20.11.0	255.255.255.0	172.20.11.254	INF1
112	172.20.12.0	255.255.255.0	172.20.12.254	INF2
113	172.20.13.0	255.255.255.0	172.20.13.254	INF3
114	172.20.14.0	255.255.255.0	172.20.14.254	INF4
115	172.20.15.0	255.255.255.0	172.20.15.254	INF-FYZIKA
200	192.168.0.30–192.168.7.250	255.255.248.0	192.168.7.254	WIFI_UCITELE
208	192.168.8.30–192.168.15.250	255.255.248.0	192.168.15.254	WIFI_HOST
216	192.168.16.30–192.168.23.250	255.255.248.0	192.168.23.254	WIFI_ZACI

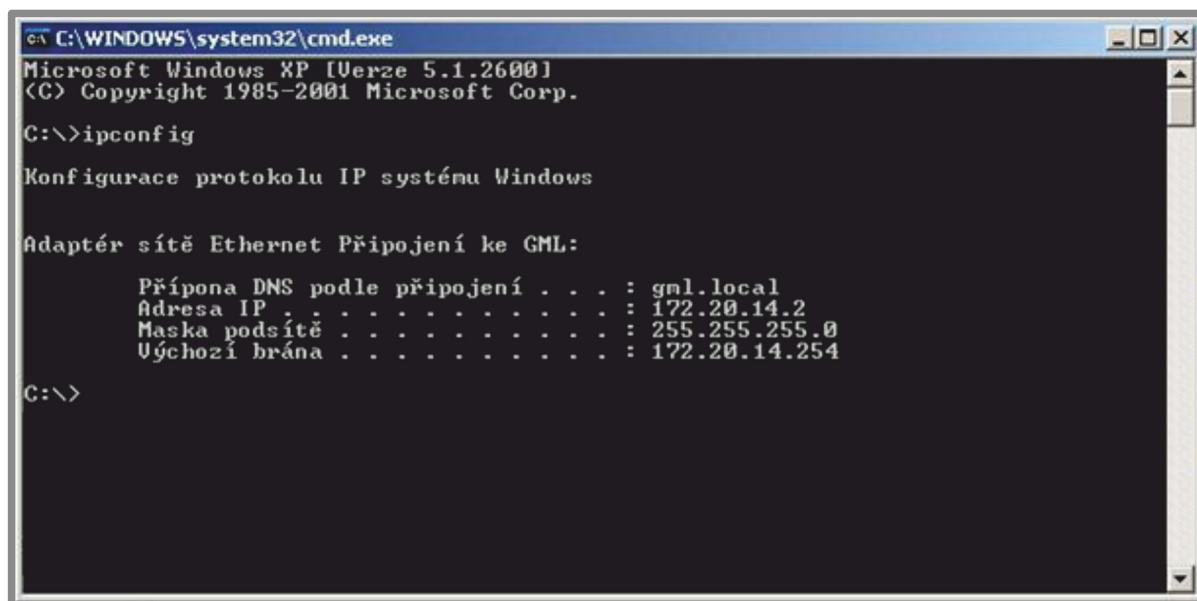
Komentář:

Rozdělení VLANů koresponduje s IP adresami, dobře se člověku pamatuje, že stroje ve VLAN114 mají IP adresy 172.20.14.xxx.

(Pozn.: Používáme v pevné síti poměrně neobvyklé volné IP adresy, v praxi častější jsou adresy typu: 192.168.xxx.xxx než 172.16–23.xxx.xxx či než 10.xxx.xxx.xxx.)

- VLAN100 slouží pro přístup zvenku k serverům (je tak zajištěna bezpečnost – potenciální útočník přicházející z Internetu se nedostane mimo VLAN100), například pro webový server,
- databázový server, obědový server, rozhraní pro identifikaci uživatelů, VPN, ...
- VLAN101 jsou interní servery
- VLAN102 jsou tiskárny, též kopírky, kamerový systém, ... prostě samostatná zařízení stojící někde „na chodbě“
- VLAN103 je management sítě, tedy přístup ke konfiguraci switchů, z důvodu bezpečnosti je samostatný a povolen jen cca 3 stanicím
- VLAN104 jsou všechny kabinety a též sekretariát. (Chcete-li, lze mít kabinety a sekretariát i v oddělených VLANech, záleží na osobních preferencích.)
- VLAN110 jsou odborné učebny (zeměpis, matematika, ...), u nichž je předpoklad, že je budou obsluhovat jak učitelé, tak studenti
- VLAN111–115 jsou informatické učebny (studenti sedící u počítačů + jeden učitel)
- VLAN200, VLAN208 a VLAN216 jsou wifi sítě, ke každé se chováme jinak (multicasty, viditelnost jednotlivých stanic, přístup k Internetu a jeho rychlost, přístup do ostatních VLANů)

Konfigurace IP-adres stanic ve VLAN114 může být tedy například:



```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Verze 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ipconfig

Konfigurace protokolu IP systému Windows

Adaptér sítě Ethernet Připojení ke GML:

    Přípona DNS podle připojení . . . : gml.local
    Adresa IP . . . . . : 172.20.14.2
    Maska podsítě . . . . . : 255.255.255.0
    Výchozí brána . . . . . : 172.20.14.254

C:\>
  
```

Obr.: Druhá studentská stanice v učebně Inf4.

Inteligentní switche a jejich nastavení

Pro rozdělení do VLAN je nutné mít tzv. inteligentní (též smart) switche – takové, u nichž je psaná podpora VLAN a které umožňují management (obvykle přístup formou webových stránek, ale lepší je je konfigurovat pomocí ssh konzole či pomocí přímého propojení RS232 kabelem).

Zavedené jsou značky Cisco (nejlepší), též MikroTik, případně Linksys, naopak ostatní značky (Netgear, D-Link, Zyxel, TP-link) jsou méně robustní, méně výkonné, mají menší výdrž a hůř se konfiguruje.

Small Business
cisco SF 200E-24 24-Port 10/100 Smart Switch

Getting Started
 ▶ Status and Statistics
 Administration
 System Settings
 Management Interface
IPv4 Interface
 IPv6 Interface
 IPv6 Neighbors
 User Accounts
 Management Services
 Idle Session Timeout
 Login Sessions
 Login History
 ▶ Time Settings
 ▶ System Log
 ▶ File Management
 Reboot
 Ping
 Control Packet Forwarding
 ▶ Diagnostics
 Discovery - Bonjour

IPv4 Interface

Management VLAN: 103 ▼

Member Ports: e10

IP Address Type:
☐ DHCP
☐ Bootp
☒ Static

IP Address: 172.20.3.41 (xxx.xxx.xxx.xxx)

Mask:
☒ Network Mask 255.255.255.0 (xxx.xxx.xxx.xxx)
☐ Prefix Length 24 (Range: 0-32, Default: 24)

Default Gateway:
☒ User Defined 172.20.3.254 (xxx.xxx.xxx.xxx)
☐ None

Operational Default Gateway: 172.20.3.254

Renew DHCP ☐

Apply Cancel

Obr.: Novější Cisco switch – nastavení IP-adresy a VLANy, po níž poběží management

Small Business
cisco SF 200E-24 24-Port 10/100 Smart Switch

admin Language English Logout About Help

Getting Started
 ▶ Status and Statistics
 Administration
 Port Management
 Port Settings
 Link Aggregation
 Green Ethernet
VLAN Management
 Create VLAN
 Interface Settings
 Port To VLAN
Port VLAN Membership
 Default VLAN Settings
 ▶ Voice and Media
 ▶ Spanning Tree
 ▶ MAC Address Tables
 ▶ Multicast
 ▶ IP Configuration
 Security
 RADIUS
 Password Strength
 Management Access Profile Rule
 Authentication Methods
 Storm Control
 Port Security
 SSH Key Management
 ▶ 802.1X
 ▶ Quality of Service
 ▶ SNMP

Interface	Mode	PVID	Operational VLAN Membership
☐ e1	Trunk	1	1U,100T,101T,102T,103T,104T,110T...
☐ e2	Access	104	104U
☐ e3	Access	104	104U
☐ e4	Access	104	104U
☐ e5	Access	110	110U
☐ e6	Access	102	102U
☐ e7	Access	1	1U
☐ e8	Access	1	1U
☐ e9	Access	1	1U
☒ e10	Access	103	103U
☐ e11	Access	1	1U
☐ e12	Access	1	1U
☐ e13	Access	1	1U
☐ e14	Access	1	1U
☐ e15	Access	1	1U
☐ e16	Access	1	1U
☐ e17	Access	1	1U
☐ e18	Access	104	104U
☐ e19	Access	1	1U
☐ e20	Access	1	1U
☐ e21	Access	1	1U
☐ e22	Access	1	1U
☐ e23	Access	1	1U
☐ e24	Access	1	1U
☐ g1	Trunk	1	1U
☐ g2	Trunk	1	1U

Edit... Detail...

Page

Obr.: Novější Cisco switch – jeden z možných pohledů na porty a jejich přiřazení VLANům


```
switch-i.gml.local - PuTTY
login as: admin
admin@switch-1's password:

(switch-1) #?

boot                Marks the given image as active for subsequent
                    re-boots.
clear                Reset configuration to factory defaults.
configure            Enter into Global Config Mode.
copy                Uploads or Downloads file.
debug               Configure debug flags.
delete              Deletes given image or config file
help                Display help for various special keys.
ip                  Configure IP parameters.
logout              Exit this session. Any unsaved changes are lost.
md5sum              Compute md5sum
network              Configuration for inband connectivity.
password            Change an existing user's password.
ping                Send ICMP echo packets to a specified IP address.
quit                Exit this session. Any unsaved changes are lost.
reload              Reset the switch.
renew                To renew IP Address
reset                Reset the switch to factory default.
show                Display Switch Options and Settings.
sshcon              Configure SSH connection parameters.
telnet              Telnet to a remote host.
telnetcon           Configure telnet connection parameters.
--More-- or (q)uit
vlan                Type 'vlan database' to enter into VLAN mode.
write               Save the current configuration to NVRAM.

(switch-1) #
```

Obr.: Novější Cisco switch – přístup pomocí ssh – píšeme příkazy

```
switch-a.gml.local - PuTTY

Switch Main Menu
=====
1. System Configuration Menu
2. Port Status
3. Port Configuration
4. System Mode (Layer 2 / Layer 3)
5. Help
0. Logout

ArrowKey/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back
```

Obr.: Starší Linksys switch (cca 10 let) – přístup pomocí ssh – vybíráme v menu (lze stisknout CTRL+Z a přihlásit se do příkazové textové konzole)

LINKSYS
A Division of Cisco Systems, Inc.

24-port 10/100/1000 Gigabit Switch SW2024

VLAN Management Setup Port Management VLAN Management Statistics ACL Security QoS Spanning Tree Multicast SNMP Admins Logout

Current VLAN: Port Setting: Ports to VLAN: VLAN to Ports: Setup

Port Setting

Previous 1 2 3 Next

Port	Mode	Acceptable Frame Type	PVID	Ingress Filtering	LAG
g1	Trunk	AdmB AS	25	1	
g2	Access	AdmB AS	25	101	
g3	Access	AdmB AS	25	101	
g4	Access	AdmB AS	25	101	
g5	Access	AdmB AS	25	101	
g6	Access	AdmB AS	25	101	
g7	Access	AdmB AS	25	101	
g8	Access	AdmB AS	25	101	
g9	Trunk	AdmB AS	25	1	
g10	Trunk	AdmB AS	25	1	
g11	Access	AdmB AS	25	1	
g12	Access	AdmB AS	25	1	

VLAN Port Setting

The VLAN Port Setting screen provides information for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the VLAN Port Setting screen. All untagged packets arriving to the device are tagged by the port PVID.

The VLAN Port Setting screen contains the following fields:

- **Unit No.** — Indicates the starting member being managed.
- **Port** — The port number included in the VLAN.
- **Mode** — Indicates the port mode. Possible values are:
 - **General** — The port belongs to a single untagged VLAN. When a port is in Access mode, the packet types which are accepted on the port (packet type) cannot be designated. It is also not possible to untag packets. Ingress filtering on an access port.
 - **Trunk** — The port belongs to VLANs in which all ports are tagged (except for an optional single native VLAN).

Obr.: Starší Linksys switch (cca 10 let) – jeden z možných pohledů na porty a jejich přiřazení VLANům (korektně běží pouze ve starších verzích Internet Exploreru)

Uložíte-li konfiguraci rozumného switche do textového souboru, bude v něm čistý text – ten lze opatrně upravit a nahrát do dalšího switche (máme-li víc stejných modelů):

```
!Current Configuration:
!
!System Description "8-Port Gigabit PoE Smart Switch"
!System Software Version "1.0.6.2"
!System Up Time "7 days 23 hrs 35 mins 52 secs"
!Additional Packages FASTPATH QOS
!Current SNTP Synchronized Time: Not Synchronized
!
network protocol none
network parms 172.20.3.54 255.255.255.0 172.20.3.254
vlan database
vlan 102-104,110,200,208,216
vlan name 102 "TISKARNY"
vlan name 103 "Management"
vlan name 104 "KABINETY"
vlan name 110 "OST UCEBNY"
vlan name 200 "WIFI UCITELE"
vlan name 208 "WIFI-HOST"
vlan name 216 "WIFI_ZACI"
exit
configure
username "cisco" password b0a...zkraceno...822 encrypted override-complexity-check
authentication dot1x none
spanning-tree configuration name "EC-E1-A9-C9-BA-E5"
!
interface g1
switchport trunk allowed vlan add 102-104,110,200,208,216
exit
interface g2
switchport mode access
switchport access vlan 104
exit
interface g3
switchport trunk allowed vlan add 103,200,208,216
exit
interface g4
switchport mode access
switchport access vlan 110
exit
interface g5
switchport mode access
switchport access vlan 110
exit
interface g6
switchport mode access
switchport access vlan 103
exit
interface g7
switchport mode access
switchport access vlan 102
exit
interface g8
switchport mode access
switchport access vlan 102
exit
exit
network mgmt_vlan 103
```

Centrální počítač

Logickou komunikaci v síti řídí centrální počítač/switch (nejlépe linux, ale může být i Windows) s virtuálními síťovými kartami zapojenými do všech VLANů, který pro provoz mezi VLANy stanovuje pravidla. Funguje též jako default gateway, tedy brána, přes níž se dostanou jednotlivé počítače „ven ze své sítě“.

Například, chce-li student ze stanice 172.20.14.2 oslovit stanici 172.20.4.56, jde jeho požadavek na default gateway 172.20.14.254, která mu případně toto oslovení zakáže: Proč by měl student z učebny (VLAN114) oslovovat počítač v kabinetě (VLAN104)?

Například, chce-li student ze stanice 172.20.14.2 oslovit stanici 77.75.76.3 (server Seznam.cz), jde jeho požadavek na default gateway 172.20.14.254, která jej pošle na firewall, ten si vyrobí permanentní spojení a pošle jej ven...

Firewall

Firewall lze mít jako samostatný počítač (nejlépe opět linux), který jednak brání útokům z Internetu a druhak překládá adresy (funguje jako tzv. NAT). V podmínkách běžné školy lze i firewall a centrální počítač sloučit do jednoho, který bude rozhodovat i o provozu uvnitř školy i o provozu dovnitř/ven ze školy.

Pravidla pro centrální počítač a/nebo firewall

V linuxovém centrálním počítači i firewallu lze pravidla chování nastavit pomocí iptables – je vhodné na to mít speciální skript či více skriptů. Příklad výpisu části (úvodu) iptables:

```
#iptables -L
Chain INPUT (policy DROP)
target      prot opt source                               destination                                limit: avg 5/sec burst 1
ACCEPT      icmp -- anywhere                               anywhere
ACCEPT      tcp  -- safeq.gml.local                       anywhere                                tcp dpt:smtp
ACCEPT      tcp  -- 172.20.1.97                           anywhere                                tcp dpt:smtp
ACCEPT      tcp  -- 172.20.2.23                           anywhere                                tcp dpt:smtp
ACCEPT      tcp  -- 172.20.2.16                           anywhere                                tcp dpt:smtp
ACCEPT      tcp  -- 172.20.2.25                           anywhere                                tcp dpt:smtp
ACCEPT      tcp  -- 172.20.4.50                           anywhere                                tcp dpt:smtp
ACCEPT      tcp  -- k268-kancelar.gml.local               anywhere                                tcp dpt:smtp
ACCEPT      tcp  -- pc-sekretariat.gml.local              anywhere                                tcp dpt:smtp
ACCEPT      tcp  -- 271-kovac                             anywhere                                tcp dpt:smtp
ACCEPT      tcp  -- k272-havranova.gml.local              anywhere                                tcp dpt:smtp
ACCEPT      tcp  -- knihovnice.gml.local                  anywhere                                tcp dpt:smtp
DROP        tcp  -- anywhere                               anywhere                                tcp dpt:smtp
ACCEPT      tcp  -- ip4-83-240-30-125.cust.nbox.cz        www.gml.cz                             tcp spts:1024:65535 dpt:ssh
ACCEPT      tcp  -- gw.omega.cz                           www.gml.cz                             tcp spts:1024:65535 dpt:ssh
ACCEPT      tcp  -- 83.136.206.64/28                       www.gml.cz                             tcp spts:1024:65535 dpt:ssh
ACCEPT      tcp  -- 213-194-204-89-static.vivo.cz         www.gml.cz                             tcp spts:1024:65535 dpt:ssh
ACCEPT      tcp  -- ip4-46-39-170-36.cust.nbox.cz         www.gml.cz                             tcp spts:1024:65535 dpt:ssh
ACCEPT      tcp  -- 89-24-240-231.i4g.tmcz.cz             www.gml.cz                             tcp spts:1024:65535 dpt:ssh
ACCEPT      tcp  -- anywhere                               www.gml.cz                             tcp spts:1024:65535 dpt:openvpn
ACCEPT      udp  -- anywhere                               www.gml.cz                             udp spts:1024:65535 dpt:openvpn
ACCEPT      all  -- anywhere                               www.gml.cz                             state RELATED,ESTABLISHED
ACCEPT      tcp  -- 213.29.26.1.dial-up.cz                172.20.1.97                             tcp dpt:5900 state
NEW,RELATED,ESTABLISHED
ACCEPT      tcp  -- 83.136.206.64/28                       bobanek.gml.local                       tcp dpt:5900 state
NEW,RELATED,ESTABLISHED
ACCEPT      tcp  -- 213-194-204-89-static.vivo.cz          bobanek.gml.local                       tcp dpt:5900 state
NEW,RELATED,ESTABLISHED
ACCEPT      tcp  -- ip4-46-39-170-36.cust.nbox.cz          bobanek.gml.local                       tcp dpt:5900 state
NEW,RELATED,ESTABLISHED
LOG         all  -- anywhere                               anywhere                                LOG level info prefix
"INPUT_DENY:"
DROP        all  -- anywhere                               anywhere
```

Stručný komentář: **První řádek** povoluje PING jenom pětkrát za sekundu (zbytek zahodí) – v běžném síťovém provozu to nevadí a útočník, který by nás chtěl zahltit velkými či častými ping-požadavky má smůlu.

Další řádky obsahují ACCEPT pro konkrétní vyjmenované stanice, které smějí kamkoliv posílat SMTP požadavky, tedy odchozí poštu. **Ostatní stanice mají DROP** (=zákaz, paket se zahodí), poštu přes SMTP (port :25) posílat nemohou – obrana proti spamu...

Další řádky povolují přístup na vnější rozhraní pomocí **ssh (jen odněkud)** a pomocí **openvpn (odevšad)**.

Další řádek říká, že je-li spojení už navázáno (typicky: iniciováno zevnitř školy ven), smí se nadále používat i v opačném směru (typicky zvenku dovnitř).

Další dva řádky se týkají povolení přenosu z některých stanic dovnitř na počítač 172.20.1.97 či bobanek.gml.local na port 5900 (což je vzdálená plocha, VNC server).

Poslední dva řádky: všechno, co dosud nebylo povoleno, zaloguj v levelu info s prefixem „INPUT_DENY:“ a následně DROPni.

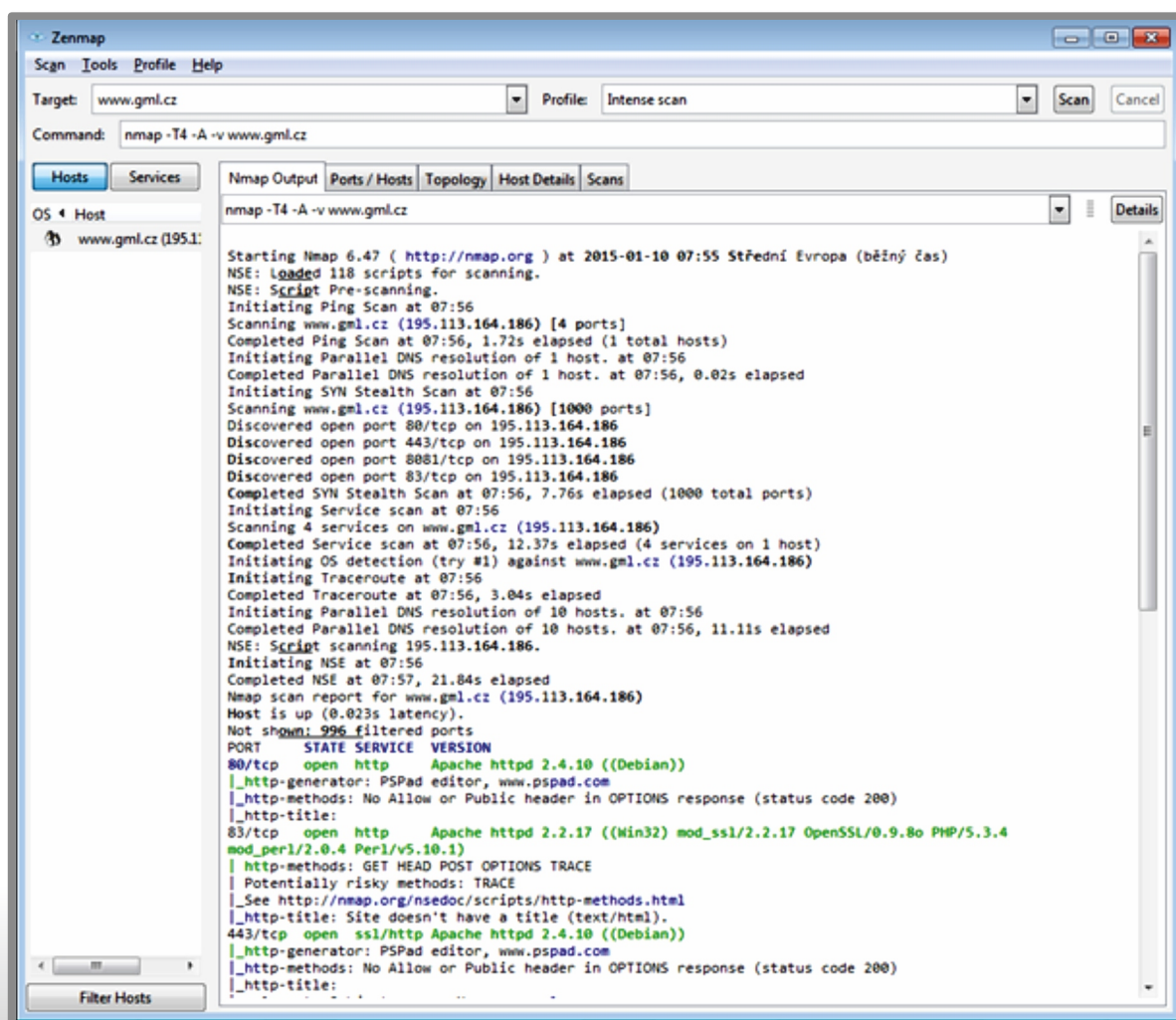
Ve skutečnosti bývá povolovací/zakazovací tabulka podstatně složitější, vždy je třeba postupovat ve dvou krocích:

- Nejprve povolit vstup (udělit výjimku ve firewallu) – některé výjimky budou jen pro konkrétní stanice, jiné lze činit paušálně, např. „všichni zevnitř školy na firewall standardně mohou“ či „všichni z vnějšku mohou přistoupit na port :8081“, atp.
- Poté povolit forward (vyrobit propojení mezi jednou a druhou stanicí) – typicky „kdo přistoupí na port :8081, bude jeho požadavek přeposlán na stanici 172.20.1.122, a to na její port :80“.

Nastavení iptables lze ukládat a načítat (pomocí příkazů iptables-save a iptables-restore), je tedy možné mít víc nastavení a měnit je podle potřeby (na přestávku, na hodinu, ráno, odpoledne, o víkendu).

Budete-li speciální skript (tvořící iptables pravidla) stavět sami, lze se na Internetu inspirovat již hotovými: <http://svn.cacert.org/CACert/SystemAdministration/backup/root/firewall.sh>, <http://web.suffieldacademy.org/ils/netadmin/docs/software/iptables/dist/etc/network/if-up.d/firewall-init>. Existují i linuxové grafické „klikací“ nástroje, ale moc bych jim nevěřil a jejich práci zkontroloval.

Celý firewall/centrální počítač je třeba jednou za čas testovat – např. skenováním portů – pod linuxem program nmap, pro Windows používám grafický Zenmap (<http://nmap.org/zenmap/>):

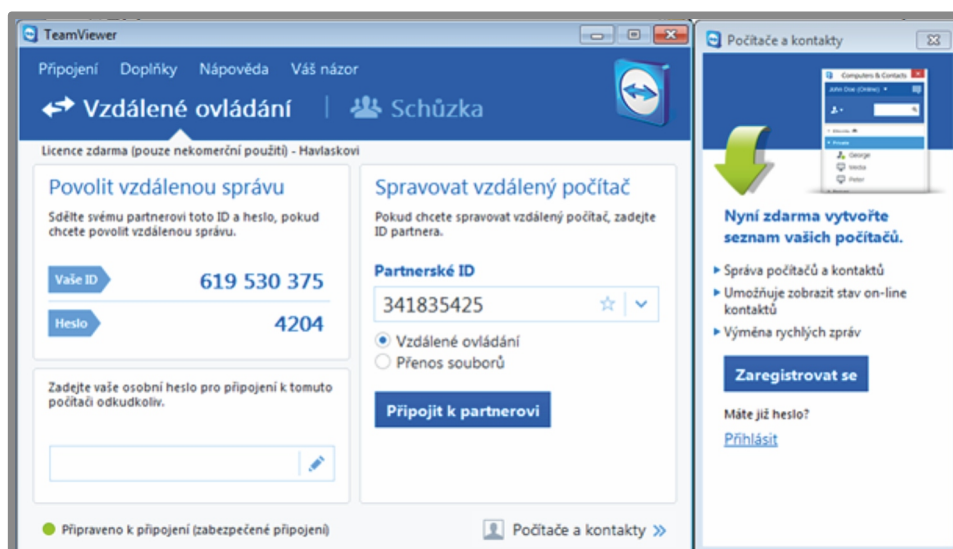
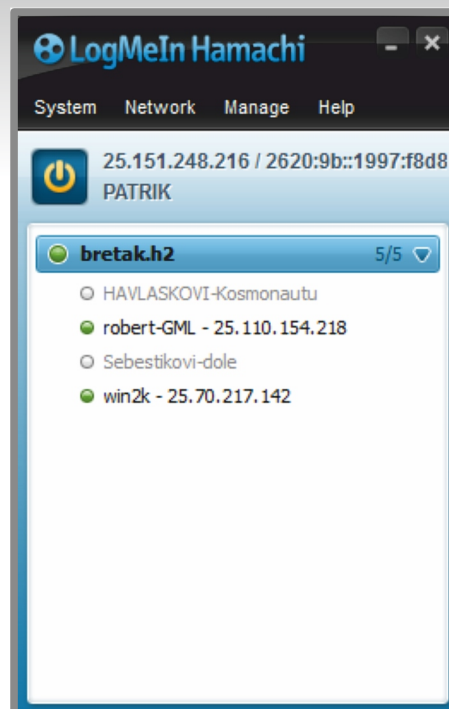


Přístup z vnějšku

Možnosti přístupu z vnějšku na jednu konkrétní stanici:

1. pomocí softwaru třetí strany:

- a. Hamachi: vyrobí virtuální síť, pomalé, nebezpečné, obě stanice jsou klienti serveru hamachi.cc, ale lze provozovat cokoliv jako na běžné síti (vyrobí se virtuální síťový adaptér, získá vlastní virtuální IP adresa, ...). Free verze omezena 5 stanicemi. Lze provozovat i pod linuxem, ale linuxový klient je dosti nešťastný.
- b. TeamViewer (pro Windows i linux): i zde jsou obě stanice klienti serveru Teamviewer.com, lze provozovat jen vzdálenou plochu či přenos souborů. Poměrně bezpečné, používají i komerční firmy (na základě licence mají speciálního klienta a management přístupových práv). Lze nainstalovat i jako službu běžící hned po startu systému na pozadí.



Přímou konkurencí programu TeamViewer jsou programy Comodo Unite a Gbridge, oba též velmi kvalitní.

2. pomocí „díry ve firewallu“ a serveru vzdálené plochy: Kontaktujeme-li z vnějšku firewall na konkrétním portu (lze omezit i zdrojovou IP, která kontaktuje, je to pak bezpečnější), přesměruje nás na konkrétní stanici a její konkrétní port.

- a. VNC server pro Windows (existuje ale i pro linux), například UltraVNC Server či TightVNC Server či RealVNC Server.

Typicky vpn.gml.cz:5555 -> 172.20.4.21:5900 (zvenku oslovíme firewall na portu :5555, dovnitř se dostaneme na stanici 172.20.4.21, port :5900, na kterém poslouchá VNC server. Obrázek konfigurace UltraVNC Serveru (povšimněte si možné autentifikace pomocí MS Domain, tedy Active Directory):

UltraVNC Server Property Page

Incoming Connections

☒ Accept Socket Connections

Display Number or Ports to use:

☐ Display N° 0

☐ Ports Main: 5900 ☒ Auto

Http: 5800

☒ Enable JavaViewer (Http Connect)

☐ Allow Loopback Connections

☐ LoopbackOnly

When Last Client Disconnects

☒ Do Nothing

☐ Lock Workstation (W2K)

☐ Logoff Workstation

Query on incoming connection

☐ Display Query Window

Timeout: 10 seconds

Default action: ☒ Refuse ☐ Accept

Keyboard & Mouse

☐ Disable Viewers inputs

☐ Disable Local inputs

☐ Alternate keyboard method

Multi viewer connections

☒ Disconnect all existing connections

☐ Keep existing connections

☐ Refuse the new connection

☐ Refuse all new connection

Authentication

VNC Password:

View-Only Password:

☐ Require MS Logon (User/Pass./Domain)

☐ New MS Logon (supports multiple domains)

Configure MS Logon Groups

File Transfer

☒ Enable ☒ User impersonation (for Service only)

DSM Plugin

☐ Use : Config.

Misc.

☒ Remove Aero (Vista)

☒ Remove Wallpaper for Viewers

☒ Enable Blank Monitor on Viewer Request

☒ Disable Only Inputs on Blanking Request

☐ DisableTrayIcon

☐ Forbid the user to close down WinVNC

Default Server Screen Scale: 1 / 1

Logging

☐ Log debug infos to the WinVNC.log file

Path: C:\Program Files\UltraVNC

OK Apply Cancel

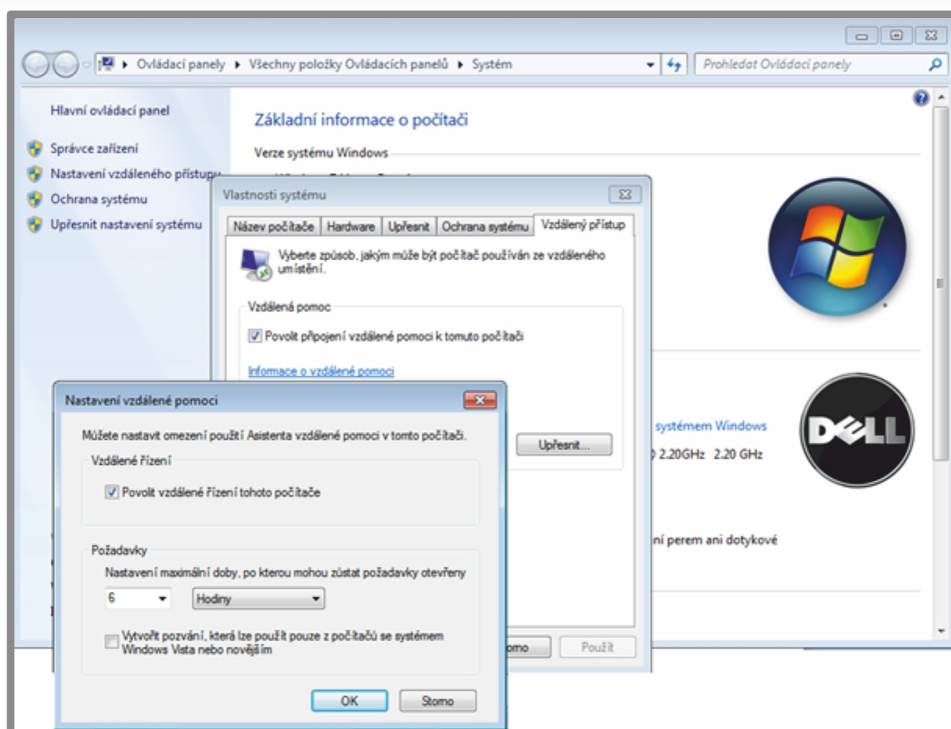
b.. XWindows

(linuxová vzdálená plocha, komplikovaní klienti jsou i pro Windows).

Typicky vpn.gml.cz:6666 -> 172.20.4.21:6001 (port :6000 je standardní pro XWindowsí první displej, port :6001 pro XWindowsí druhý displej, atd.)

Konfigurace XWindows spojení pod linuxem je bez problémů, pod Windows není vůbec jednoduchá – narazíte na problém, že vlastně na vašem klientském počítači potřebujete XWinServer, aby mu aplikace mohly posílat grafická data do okna zpět. Takový XWinServer pro Windows je docela „bumbrlíček“, náročný zejména na RAM. Vybírejte jej mezi XMin (http://sourceforge.net/projects/xming/) a Cygwin (http://x.cygwin.com/).

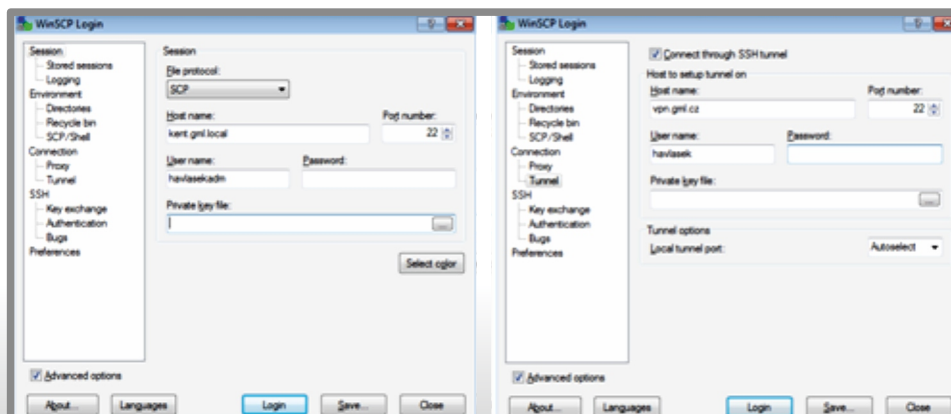
- c. RDP server (windowsí Vzdálená plocha) – server je přímo uvnitř systému libovolných Windows (WinXP SP3 a novějších).
Typicky vpn.gml.cz:3333 -> 172.20.4.21:3389 (port :3389 je standardní pro RDP).
Lze ji zapnout přes Ovládací panely-System-Nastavení vzdáleného přístupu:



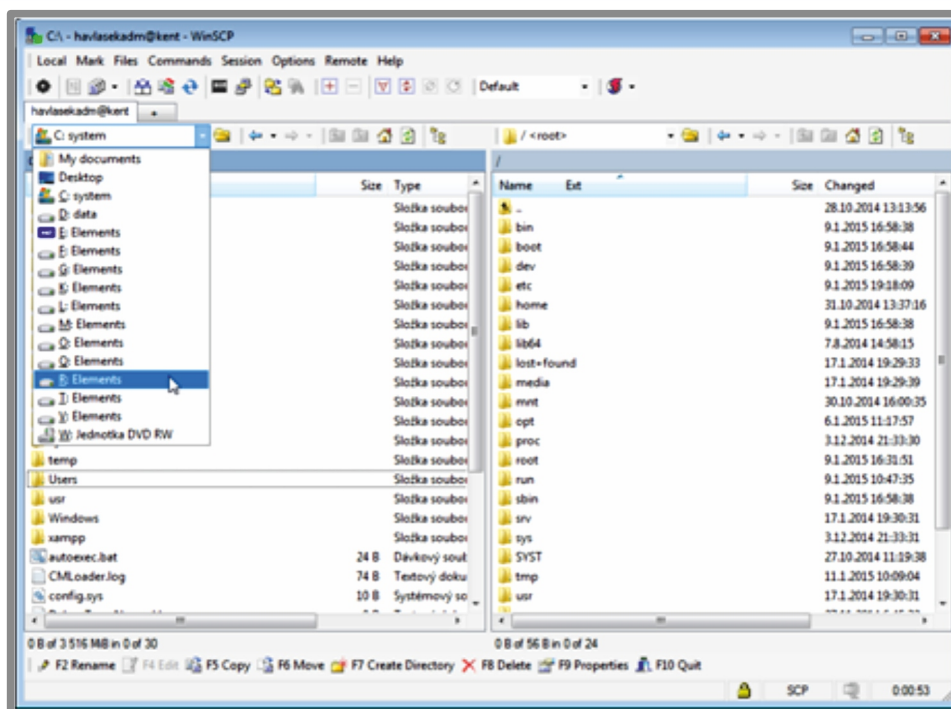
Rovněž klient je součástí všech verzí Windows, stačí spustit Start-Spustit: mstsc.exe. Umožňuje vzdálenou plochu, přenášení souborů, sdílení disků, tisk na vzdálených tiskárnách.

Běží šifrovaně a je bezpečný. Funguje pouze pod Windows.

3. Pomocí ssh tunelu přes firewall – je-li na zmiňované konkrétní stanici nainstalovaný SSH server (v linuxu nativně, jako ssh server pro Windows doporučuji MobaSSH <http://mobassh.mobatek.net/>, pro nekomerční použití je zdarma a umí toho docela dost).
 - a. Lze se nejprve pomocí ssh přihlásit zvenku na firewall (máme-li toto přihlášení povolené) a pak pomocí ssh z firewallu přihlásit na konkrétní stanici. Program WinSCP (<http://winscp.net/>) umožňuje při zatržení „Advanced options“ možnost zadání tunnellingu přes firewall:



Takto nastavené spojení jde nejprve na vpn.gml.cz, kde se přihlásí uživatelem havlasek (na heslo se zeptá) a poté z něj na kent.gml.local, kde se přihlásí jako havlasekadm (na heslo se též zeptá). Po ustanovení spojení máme k dispozici v jednom okně místní disky a v druhém okně vzdálené disky:

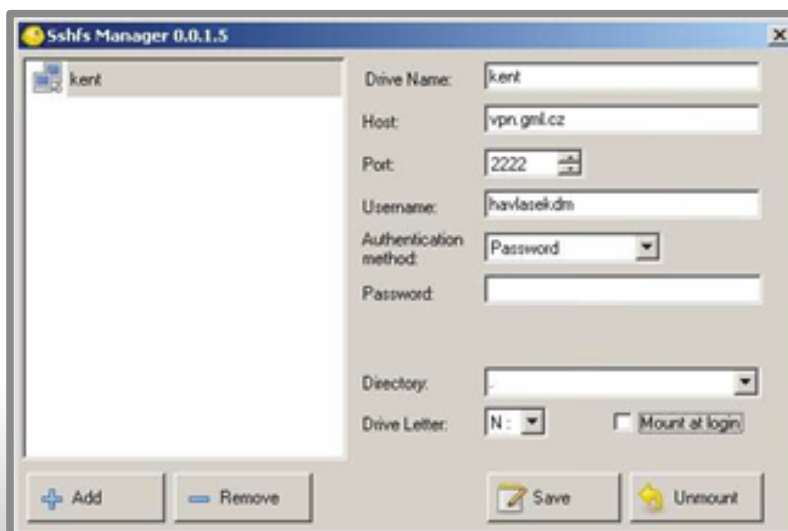


Opensource program WinSCP je bezpečný, přistupuje k souborům velmi inteligentně a je prakticky jediný svého druhu. (Respektive, určitě jediný, který umožňuje tunnelling nastavit přímo uvnitř programu.)

- b. Pomocí „díry ve firewallu“, která přeposílá požadavky na ssh server lokálního počítače, typicky vpn.gml.cz:2222 -> 172.20.4.21:22 (port :22 je standardní pro ssh).

Programů pro přístup pomocí ssh k souborům je celá řada, budete-li chtít namapovat vzdálený ssh server jako „lokální disk“

(podobně jako „Připojit síťovou jednotku“), doporučuji program Winsshfs (<https://code.google.com/p/win-sshfs/>), jeho konfigurace je velmi jednoduchá:

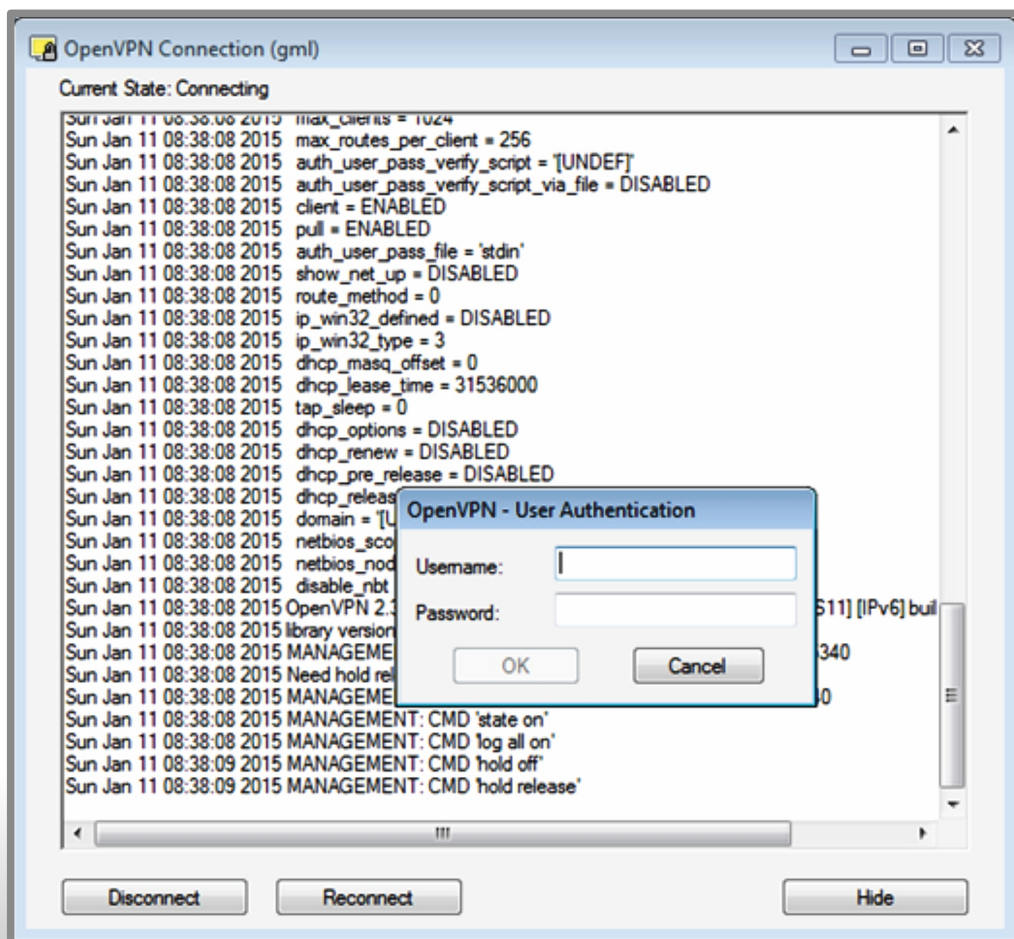


DriveName je pouze název profilu, zatrhnout můžete i „Mount at login“ (v případě nevyplněného hesla se při startu programu zeptá). Jakou autentifikační metodu lze použít buď heslo, nebo privátní certifikát. Tento program doporučuji pro neprofesionály (např. kantory, ale i studenty) pro přístup k ssh diskům, typicky např. na jejich linuxový web.

4. Pomocí VPN tunelu.

Poznámka: Nehovoříme o „anonymním prohlížení Internetu“, jak je u některých uživatelů VPN chápáno (ve smyslu: připojím se k nějakému americkému/britskému/... anonymizačnímu serveru a ten skryje moji IP-adresu za svoji IP-adresu a dovolí mi prohlížet obsah přístupný jen pro tuto zemi). Naopak hovoříme o VPN tunellingu, tedy můj počítač vně školy na jedné straně, VPN server uvnitř školy na straně druhé. Principiálně lze použít jeden z těchto protokolů:

- PPTP protokol – nejméně bezpečný, ovšem nejrozšířenější. Býval v minulosti hojně využíván pro připojení modemu k serveru poskytovatele Internetu. Všechny běžné operační systémy umějí nastavit PPTP server, návod pro Windows třeba zde:
<http://pcworld.cz/internet/jak-a-proc-nastavit-vpn-jeste-dnes-2-dil-45777>
- L2TP a IPsec protokol jsou bezpečnější, ovšem s lehce komplik. nastavením.
- SSL protokol je nejbezpečnější, systém veřejného+privátního klíče. Využívá jej i program OpenVPN (<http://openvpn.net/>, GPL licence), který je de facto standardem pro profesionální přístup dovnitř sítě. Spojit lze s libovolným autentifikačním serverem (ve školních podmínkách obvykle pomocí LDAP s Active Directory). Obr. běžného klienta:



Při VPN tunellingu se vyrobí vlastní virtuální síťové rozhraní a možné jsou všechny služby (kompletní síťová komunikace).

5. Pomocí WebDAV serveru: Běžný http server (windowsí i linuxový) lze skriptem doplnit o WebDAV server – ten umožňuje obousměrnou výměnu souborů přes http (resp. lépe přes https) protokol. Klientem jsou samy Windows, WebDAV lze připojit jako disk. Klientem jsou i internetové prohlížeče a též Microsoft Office, které k WebDAVu umějí přímo přistupovat.
2. Pomocí speciálního webového rozhraní, doporučím Owncloud (<http://owncloud.org/>), usazení není až tak jednoduché) nebo Pydio (dříve AjaXplorer, <https://pydio.io/>).

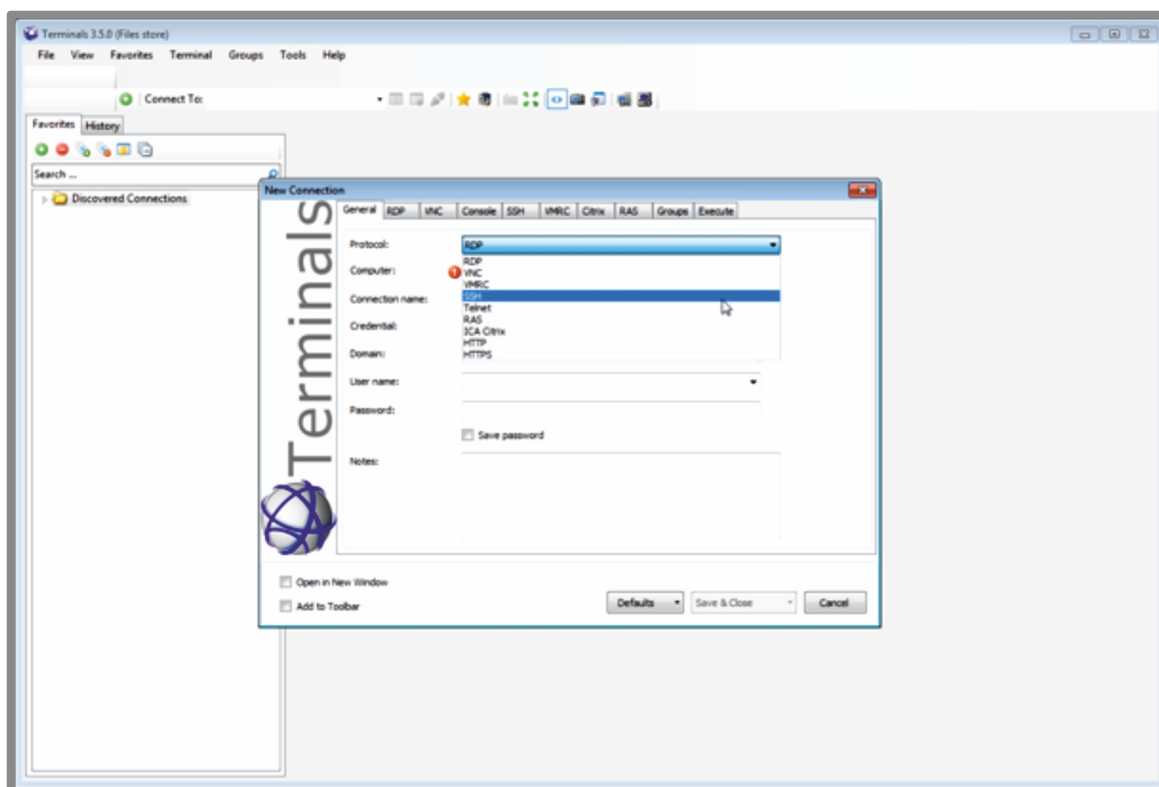
U prvních čtyř zmiňovaných přístupů zvnějšku na jednu konkrétní stanici platí: Pustí-li nás tato stanice dál do sítě (překládá-li naše požadavky vlastním NATem do místní sítě), znamená to pro nás možnost oslovit z domu libovolný počítač v místní síti.

U varianty přístupu 2a jsem se u UltraVNC Serveru setkal s programem UltraVNC Repeater (<http://www.uvnc.com/downloads/repeater.html>), který jako NAT částečně funguje.

Obousměrnou komunikaci (že by někdo zevnitř školy oslovil můj počítač) umějí varianty 1a, 2a, 3a, 3b, 4a, 4b, 4c.

Existuje celá řada programů sdružujících různé vzdálené přístupové protokoly (RDP, VNC, ssh či VMRC pro připojení k virtuálním plochám – viz kapitoly níže). XWin „neumí“ žádný z nich. Doporučím opensource program Terminals (<http://terminals.codeplex.com/>), mRemoteNG (<http://www.mremoteng.org/>) či Remote Desktop Manager (<http://remotedesktopmanager.com/>, free či placená verze).

Screenshot programu Terminals:



Centrální správa bezdrátové sítě s více AP

AccessPointy lze spravovat buď odděleně (každý nastaven samostatně) nebo centrálně (pomocí tzv. wifi controlleru). Nejlépe zpracovanou síťovou infrastrukturu má jednoznačně firma Cisco, s jejich Cisco APčky a Cisco Wireless LAN Controllerem.

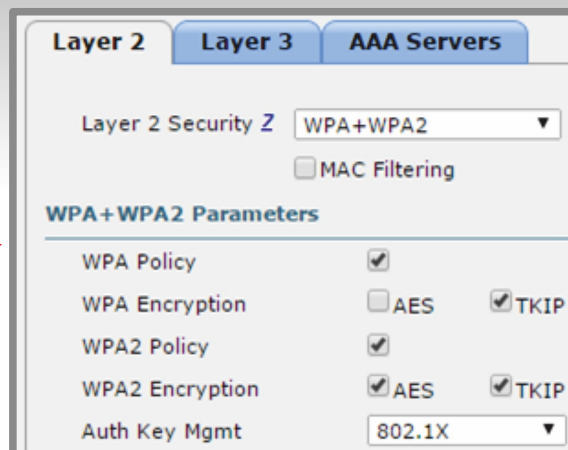
Autentifikace

Autentifikovat uživatele můžeme na úrovni Layer 2 pomocí statického WEP („obyčejné heslo“, žádné zvláštní krytování), WPA či WPA2 (i tuto autentifikaci lze lehce prolomit, jde o heslo s výměnou klíčů, se šifrováním AES či TKIP): →

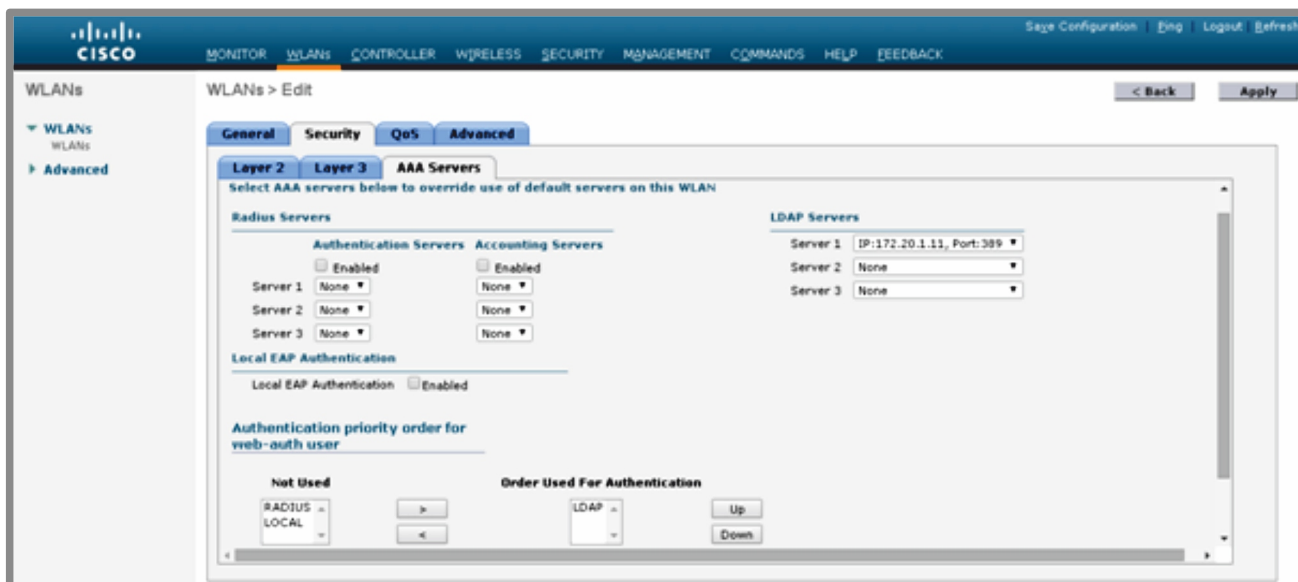
Nejbezpečnější z výše uváděných metod je kombinace WPA2+AES či WPA2+TKIP s užíváním filtrování MAC adres jednotlivých klientů. Správcovat ale MAC adresy je u větší školy prakticky nadlidský výkon.

Chytřejší Access Pointy a též všechny Controllery umožňují autentifikaci protokolem 802.1X:

Notebook požádá APčko, APčko je zapojeno do Controlleru, v něm je nastavena autentifikace pomocí 802.11X na RADIUS serveru nebo na LDAP serveru a ten si uživatele ověří dle svého nastavení.



Obr.: Kousek obrazovky z Cisco WLAN Controlleru



Obr.: RADIUS vypnut, LDAP server zapnut, dole nastaveno pořadí, že se identifikujeme jen přes LDAP.

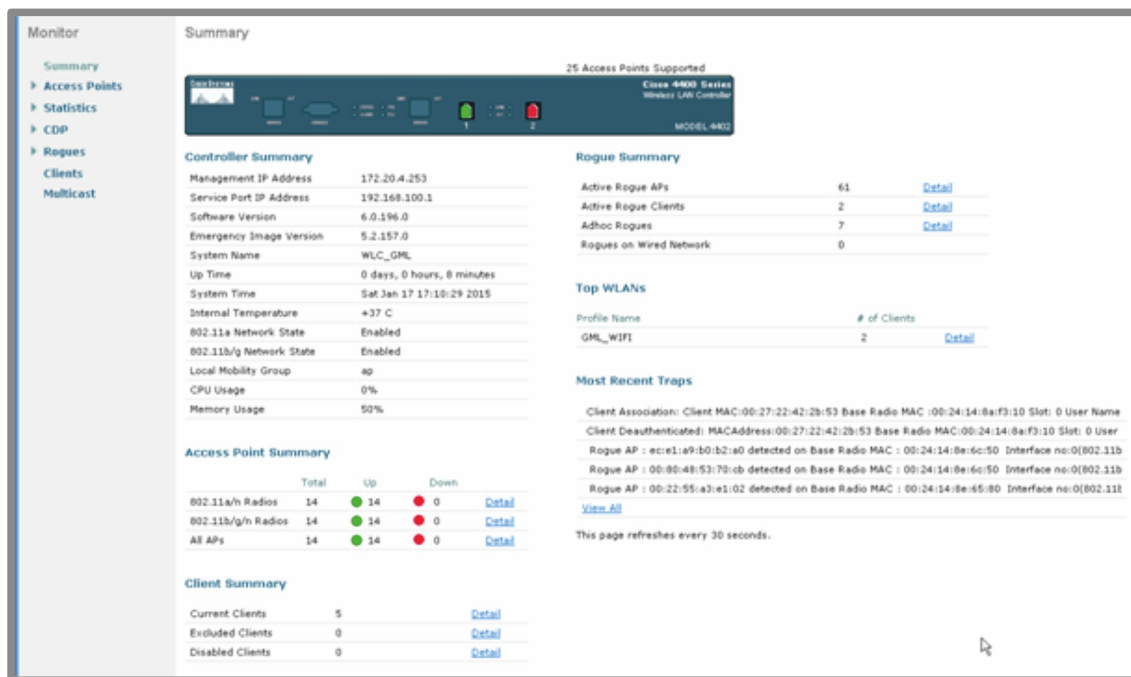
Nejpoužívanější model: uživatel se bez hesla připojí k „omezené“ WIFI, která veškeré http požadavky (běžný provoz internetového prohlížeče) směřuje nikoliv na požadované stránky, ale na autentifikační lokální stránku – teprve po jejím správném vyplnění (ověření přes LDAP či RADIUS) se uživatel dostane ven na požadované stránky. Nepříjemná na tomto modelu je nutnost spustit internetový prohlížeč (pokud se uživatel připojuje k wifi například jen za účelem stažení pošty POP3 protokolem, nedostane se nikam a stejně musí pustit internetový prohlížeč...)

Ve školních podmínkách běží LDAP či RADIUS server rovnou na PDC (primárním řadiči domény, čili serveru, jenž má na starosti autentifikaci uživatelů v Active Directory). Ovšem nemusí to tak být vždy, například celorepubliková wifi síť EduROAM, jíž se účastní většina VŠ zapojených do Cesnetu, umožňuje kdekoli v republice přihlášení na základě loginu+hesla z jiné části republiky. Tamní RADIUS server rozhodne, do působnosti kterého jiného RADIUS serveru uživatel patří a pošle mu žádost o ověření. Prakticky, jste-li jako škola členem EduROAM sítě, přihlásíte se kdekoli v republice svým domácím účtem.

Logování pomocí trap-serveru

Rozhodneme-li se netrápit uživatele přihlašování vlastními účty a ponecháme-li jednotné heslo na wifi pro celou školu, je třeba poctivě zaznamenávat, kdo (která MAC adresa), kdy a kam se připojil.

Controller samozřejmě může vyrábět vlastní textový log někde na svém disku. Profesionálnější je ale nechat si všechny události posílat do logovacího serveru pomocí aktivní části SNMP protokolu.



Obr.: Čerstvě nastartovaný controller, připojeno 14 AP. Vpravo vidíme záznam logu s tzv. trapy (událostmi, které spadly do „pasti“ – filtru toho, co se má logovat). Aktuálně jsou v záznamu tři „cizácké“ AP, které ruší ty naše a Deautentifikace a posléze Asociace jednoho klienta.

SNMP trapy umí posílat poměrně hodně zařízení (nejen wifi controller, ale i tiskárny, počítače, kamery, třeba při detekci pohybu, atp.).

Je dobré si na nějakém linuxu postavit trap-server, který trapy odchyťává a třídí (vyrábí si z nich logy). Trap-server je jednoduchý démon, který sedí na UDP portu 161 a volá skript v libovolném programovacím jazyce, jenž čte ze standardního vstupu zjištěné trapy, filtruje je a ukládá do logů dle libosti. Příklad obslužného skriptu psaného v shellu (vybral jsem jen řádky týkající se trapů z wifi controlleru):

```
#!/bin/sh

logfile="/var/log/wifi-trap-log"

read host
# byva <UNKNOWN>
read ip
# IP adresa zarizeni, co trap posila
read oid uptime uptime
# uptime zarizeni, co trap posila
read oid trap trap
# nazev trapy podle MIB

vars=

if [ "$trap" = "AIRESpace-Wireless-MIB::bsnDot11StationAssociate" ]; then
    read oid_apmac apmac;
    # MAC adresa zarizeni, co trap posila
    read oid_APIfSlot APIfSlot;
    # netuSim, co to je
    read oid_pcmac pcmac;
```

```

# MAC adresa notebooku, co se prave asocioval
pcmac2=`echo , $pcmac: | sed "s/:(.\\):/:0\\1:/g" | sed "s/,\\(.\\):/:0\\1:/g" | head -c18
| tail -c17`
# nahrazení jednociferných číslic dvojcifernými (typu 0:18:1:f9:4c:72 nahradí za
00:18:01:f9:4c:72)
read oid_userip userip;
# napřed není určena DHCP serverem (je 0.0.0.0), při přechodu z jednoho AP na jiný
(pohyb po budově) tu je
read oid_apname apname;
# jméno APčka, na kterém se asocioval (např. AP_01)
read oid_StationUserName StationUserName;
# jméno uživatele, v případě, že se přihlasoval k AP (to my nemáme => je prázdné)
echo "ASSOC " `date` $pcmac2 $apname $userip >> $logfile
fi

if [ "$trap" = "AIRESpace-WIRELESS-MIB::bsnDot11StationDeauthenticate" ]; then
read oid_apmac apmac;
# MAC adresa zařízení, co trap posílá
read oid_APIfSlot APIfSlot;
# netuším, co to je
read oid_reason reason;
# důvod deasociace (v případě odpojení notebooku ze strany uživatele bývá
"unspecified")
read oid_pcmac pcmac;
# MAC adresa notebooku, co se prave deasocioval
pcmac2=`echo , $pcmac: | sed "s/:(.\\):/:0\\1:/g" | sed "s/,\\(.\\):/:0\\1:/g" | head -c18
| tail -c17`
# nahrazení jednociferných číslic dvojcifernými (typu 0:18:1:f9:4c:72 nahradí za
00:18:01:f9:4c:72)
read oid_userip userip;
# vždy tu je
read oid_apname apname;
# jméno APčka, na kterém se deasocioval (např. AP_01)
read oid_StationUserName StationUserName;
# jméno uživatele, v případě, že se přihlasoval k AP (to my nemáme => je prázdné)
echo "DEAUTH " `date` $pcmac2 $apname $userip >> $logfile
fi

if [ "$trap" = "SNMPv2-SMI::enterprises.9.9.599.0.4" ]; then
# Tohle je MIB pro Authenticate, akorát ho nemám v externím souboru, takže se
nepíše "hezky", ale "skaredě" :-))
read oid_pcmac pcmac;
# MAC adresa notebooku, co se prave autentifikoval
pcmac2=`echo $pcmac | head -c18 | tail -c17 | sed "s/ /:/g" | sed 's/\\(.*)\\L\\1/g`
# update MAC adresy (orezáni mezer okolo, nahrazení mezer mezi za :, změna velkých
písmen na malá
read oid_apname apname;
# jméno APčka, na kterém se deasocioval (např. AP_01)
read oid_apmac apmac;
# MAC adresa zařízení, co trap posílá
read oid_APIfSlot APIfSlot;
# netuším, co to je
read oid_userip userip;
# vždy tu je
read oid_StationUserName StationUserName;
# jméno uživatele, v případě, že se přihlasoval k AP (to my nemáme => je prázdné)
read oid_sit sit;
# jméno site, ke které se autentifikoval (zde "GML WIFI")
echo "AUTH " `date` $pcmac2 $apname $userip >> $logfile
fi

```

Tento skript vyrábí log typu:

```

ASSOC Sat Jan 17 14:36:20 CET 2015 00:27:22:42:2b:53 "AP_13" 192.168.16.15
AUTH Sat Jan 17 14:36:20 CET 2015 00:27:22:42:2b:53 "AP_13" 192.168.16.15
ASSOC Sat Jan 17 14:36:43 CET 2015 00:27:22:42:2b:53 "AP_13" 192.168.16.15
AUTH Sat Jan 17 14:36:46 CET 2015 00:27:22:42:2b:53 "AP_13" 192.168.16.15
ASSOC Sat Jan 17 15:03:01 CET 2015 00:27:22:42:2b:53 "AP_13" 0.0.0.0
ASSOC Sat Jan 17 15:03:03 CET 2015 00:27:22:42:2b:53 "AP_13" 0.0.0.0
DEAUTH Sat Jan 17 15:05:23 CET 2015 00:27:22:42:2b:53 "AP_13" 0.0.0.0
ASSOC Sat Jan 17 15:05:23 CET 2015 00:27:22:42:2b:53 "AP_13" 0.0.0.0
ASSOC Sat Jan 17 15:07:03 CET 2015 8c:77:16:72:44:7c "AP_06" 0.0.0.0
AUTH Sat Jan 17 15:07:08 CET 2015 8c:77:16:72:44:7c "AP_06" 192.168.16.90
DEAUTH Sat Jan 17 15:07:43 CET 2015 00:27:22:42:2b:53 "AP_13" 0.0.0.0
ASSOC Sat Jan 17 15:07:43 CET 2015 00:27:22:42:2b:53 "AP_13" 0.0.0.0

```

Lze tedy dohledat, kdo se kdy do wifi sítě autentifikoval, jakou IP-adresu přitom dostal, ke kterému AP se asocioval a kdy se odpojil (buď odešel k jinému AP nebo zmizel z dosahu wifi).

Řízení AP a přehled o nich

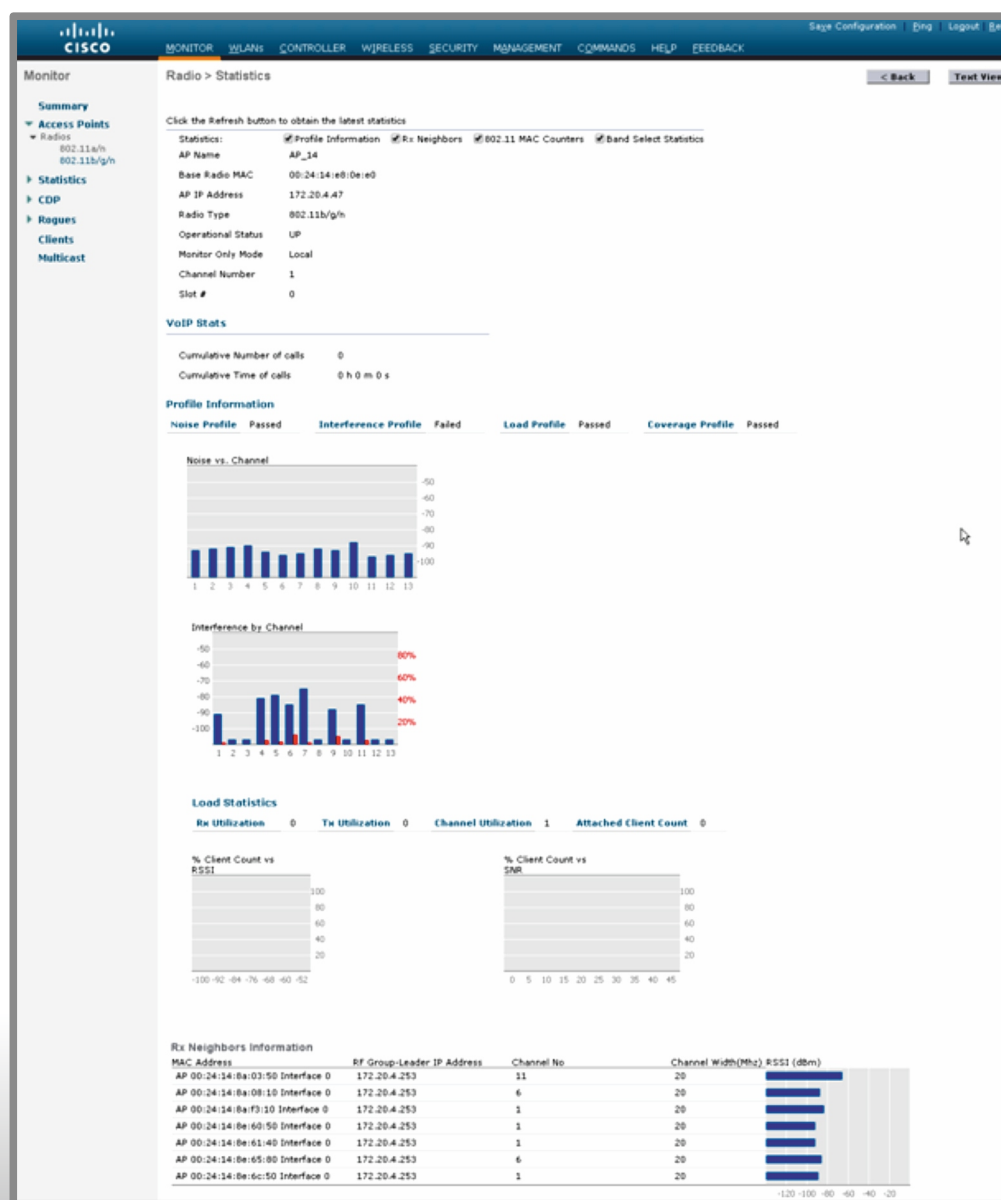
Připojíme-li AP do controlleru, tento si sám řídí výkon jednotlivých AP a frekvence (wifi kanály), na nichž jednotlivé AP běží, aby nekonkurovaly samy sobě ani našim sousedům.

Po kliknutí vlevo v menu na Access Points – Radios a volbě 802.11a/n či 802.11b/g/n vidíme seznam AP s jejich aktuálními kanály:

AP Name	Radio Slot#	Base Radio MAC	Operational Status	Load Profile	Noise Profile	Interference Profile	Coverage Profile
AP_14	0	00:24:14:e8:0e:e0	UP	Passed	Passed	Failed	Passed
AP_07	0	00:24:14:8e:60:b0	UP	Passed	Passed	Passed	Passed
AP_02	0	00:24:14:8e:65:00	UP	Passed	Passed	Passed	Passed
AP_13	0	00:24:14:8a:f3:10	UP	Passed	Passed	Passed	Passed
AP_12	0	00:24:14:8e:61:40	UP	Passed	Passed	Passed	Passed
AP_11	0	00:24:14:8e:65:00	UP	Passed	Passed	Failed	Passed
AP_01	0	00:24:14:8e:60:90	UP	Passed	Passed	Passed	Passed
AP_04	0	00:24:14:8e:60:50	UP	Passed	Passed	Passed	Passed
AP_08	0	00:24:14:8e:5a:80	UP	Passed	Passed	Passed	Passed
AP_10	0	00:24:14:8a:03:50	UP	Passed	Passed	Passed	Passed
AP_03	0	00:24:14:8e:66:b0	UP	Passed	Passed	Passed	Passed
AP_09	0	00:24:14:8e:5b:20	UP	Passed	Passed	Passed	Passed
AP_06	0	00:24:14:8a:08:10	UP	Passed	Passed	Passed	Passed
AP_05	0	00:24:14:8e:6c:50	UP	Passed	Passed	Failed	Passed

Kanály volí controller tak, aby si APčka nekonkurovaly – zde se mu to patrně daří, neboť všechny AP mají Power Level 1 (netřeba jejich výkon upravovat).

Kliknutím na Detail u jednotlivého AP pak získáme o něm všehrájkající přehled:



Controlleru lze nastavit opravdu velmi mnoho věcí. Spíše než grafické webové rozhraní by měli správci preferovat textovou konzoli (přístup pomocí ssh či sériové linky).

Školní DHCP server

DHCP server (=server, který připojenému stroji přidělí IP-adresu na základě jeho MAC adresy) je v dnešní době nutností a všichni správci sítě jej nakonfigurovaný mají. Lze jej postavit na libovolném linuxu i na Windows Serveru.

Pro linux bohatě postačí démon dhcpd s jednoduchou konfigurací (souborem /etc/dhcpd):

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#   see 'man 5 dhcpd.conf'
#
authoritative;
log-facility local6;

option domain-name "gml.loc";
option domain-name-servers 172.20.1.254;
        default-lease-time 604800;

## Subnet pro kabinety
subnet 172.20.4.0 netmask 255.255.255.0 {
    range 172.20.4.220 172.20.4.245;
    option routers 172.20.4.254;
    allow booting;
    allow bootp;
    option dhcp-max-message-size 2048;
    do-forward-updates on;
    ddns-updates on;
    use-host-decl-names on;
    ddns-update-style interim;
    next-server 172.20.4.3;
    option tftp-server-name "172.20.4.3";
    get-lease-hostnames true;
    filename "pxelinux.0";
}

## Subnet pro ostatni ucebny
(...)

host K215-FJ-MUS-FER {
    fixed-address 172.20.4.131; hardware ethernet 00:13:d4:06:a9:8e;
}
host K223-FJ-KIR-ARN {
    fixed-address 172.20.4.132; hardware ethernet 00:24:1d:28:f5:be;
}
host K225-JAKUBKOVA {
    fixed-address 172.20.4.133; hardware ethernet 00:24:1d:28:f6:13;
}
(...)
```

Stručný komentář:

Přidělujeme stanicím doménové jméno **gml.loc**. Říkáme jim, že DNS server (server překládající doménová jména typu **www.seznam.cz** na IP -adresy typu **77.75.76.3**), na nějž se mohou obracet, je **172.20.1.254**. Default lease time je čas, po který jednotlivým stanicím IP -adresu propůjčujeme (po tomto čase relaci mezi MAC - adresou a IP - adresou server zapomene a přidělí znovu, buď stejnou nebo jinou). **604 800 sekund** je 7 dní, tedy přesně týden.

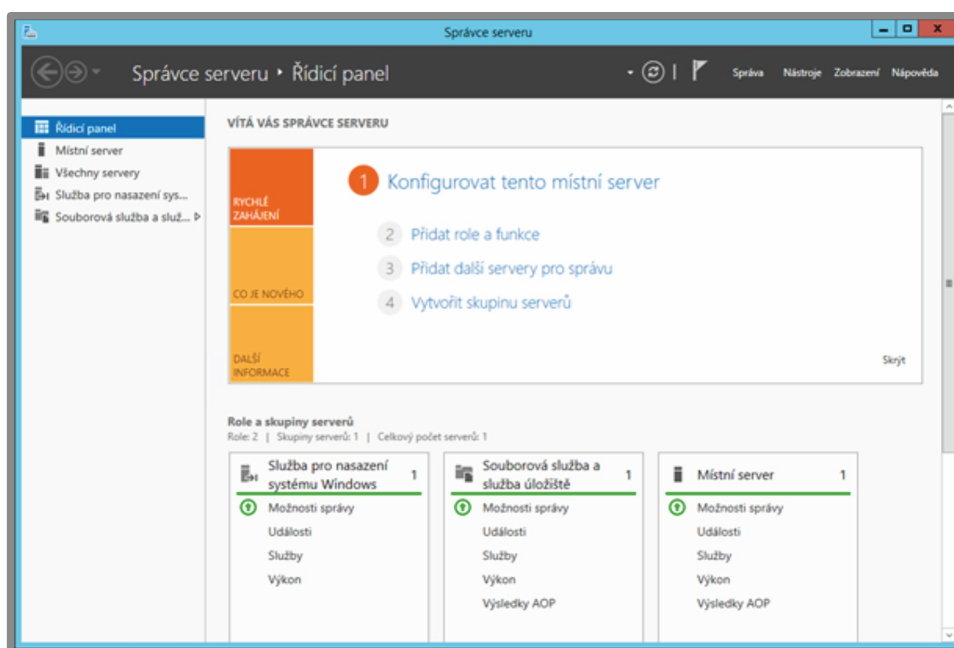
V konkrétním subnetu **172.20.4.0** s maskou **255.255.255.0** (tedy s rozsahem **172.20.4.0 až 172.20.4.254**) poskytujeme neznámým novým stanicím adresy **od 172.20.4.220 do 172.20.4.245** (tedy docela málo, všechny známé stanice jsou přidělovány **dle svých MAC adres podle pravidel uvedených na spodních červených řádcích**).

Fialová oblast v daném subnetu umožňuje bootování ze sítě pomocí PXE protokolu (viz samostatná kapitola o několik stran níže, hned za DNS serverem). Nastavení říká, že oslovíme bootovací server **172.20.4.3** a data stahujeme (pomocí FTP protokolu) rovněž z **172.20.4.3**, konkrétně si klient při startu sítě stáhne soubor **pxelinux.0** a poté mu předá řízení.

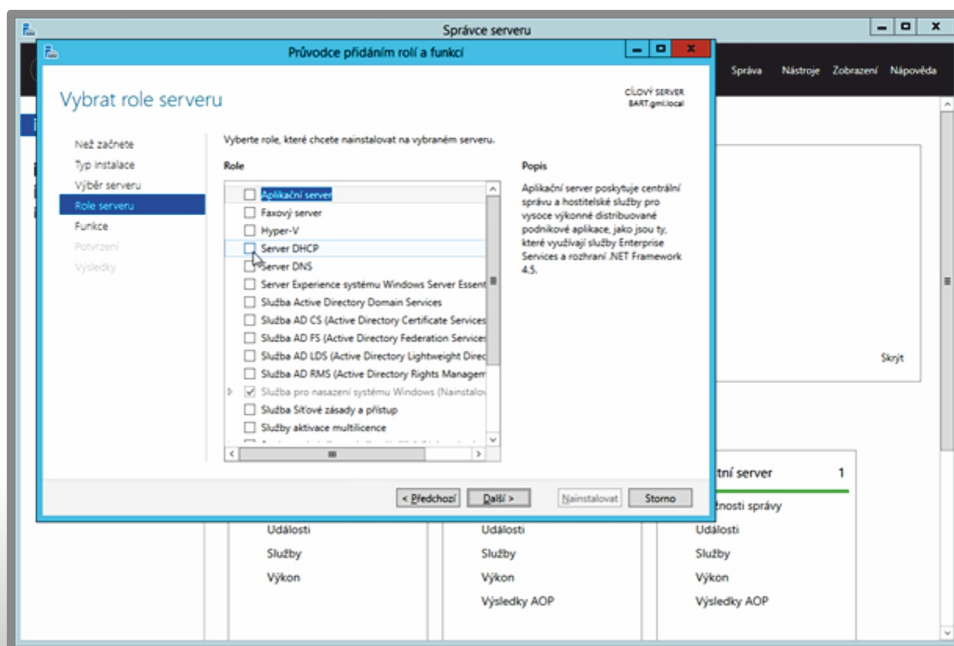
V případě DHCP serveru provozovaného pod Windows lze používat přímo DHCP server uvnitř operačního systému (povolíme-li službu Sdílení internetu, spustí se automaticky). Vhodnější je mít na DHCP server speciální program, z běžně používaných jmenujme DHCP Server for Windows (<http://www.dhcpserver.de/>), Open DHCP Server (<http://dhcpserver.sourceforge.net/>).

Pro domácí použití vřele doporučuji TFTP Server, který, ač maličký, free a opensource, umí roli DHCP serveru, DNS serveru, TFTP serveru (viz kapitola o bootování ze sítě přes PXE) a prý i SNMP server (zachytávat trapy z aktivní části SNMP protokolu, nezkoušel jsem). TFTP server nemusíte instalovat, jednoduše si stáhnete .zip, rozbalíte, povolíte ve firewallu, spustíte a jede. Ideální též pro nošení s sebou na flashdisku.

Nejobtustnější možností provozu pod Windows je spuštění speciální role DHCP serveru ve Windows Serveru. Na Windows Serveru 2012 se tak děje ve Správci Serveru:

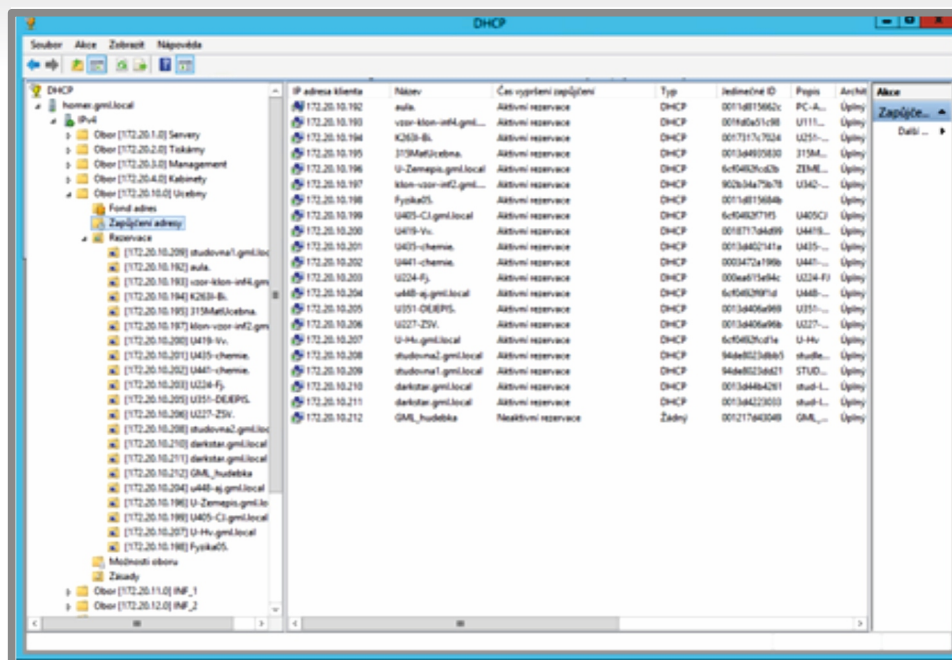


Zvolíte Přidat role a funkce, průvodcem se doklikáte až k samotnému přidání:



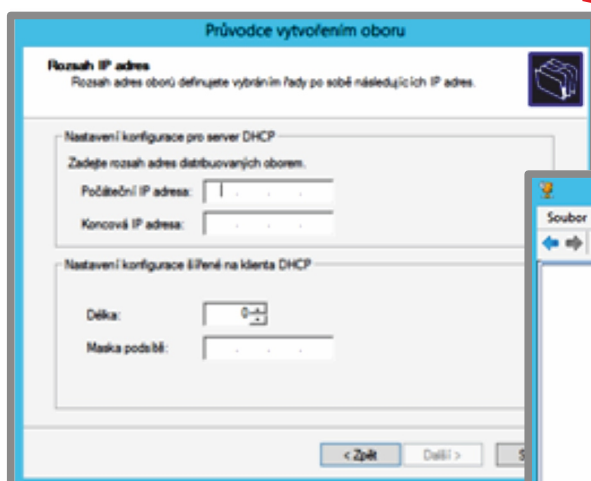
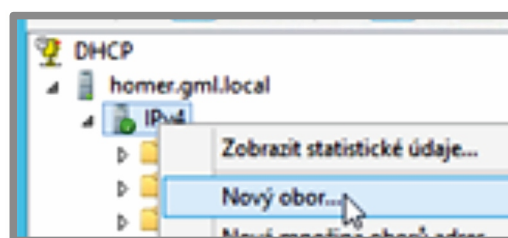
Konfigurace DHCP serveru pod Windows

DHCP server běžící na Windows Serveru konfiguruje pomocí konzole:

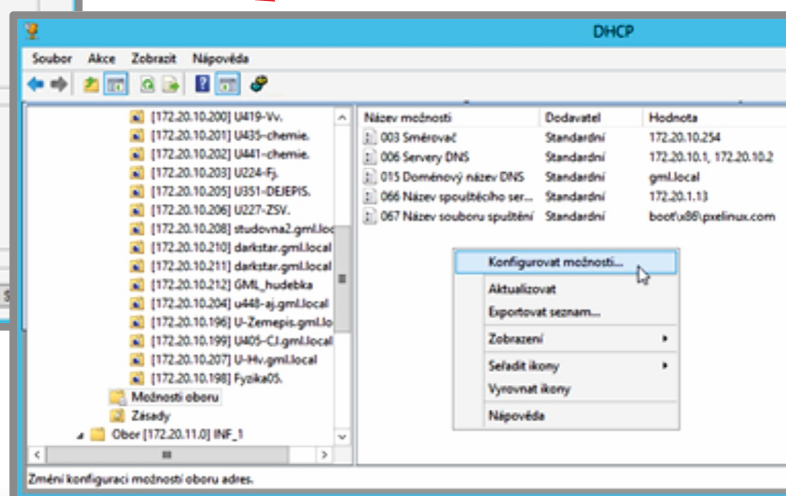


V ní vyrobíme jednotlivé obory
(odpovídající logické struktuře VLANů):

Každému oboru pak v průvodci zadáme
rozsah přidělovaných adres a masku podsítě:

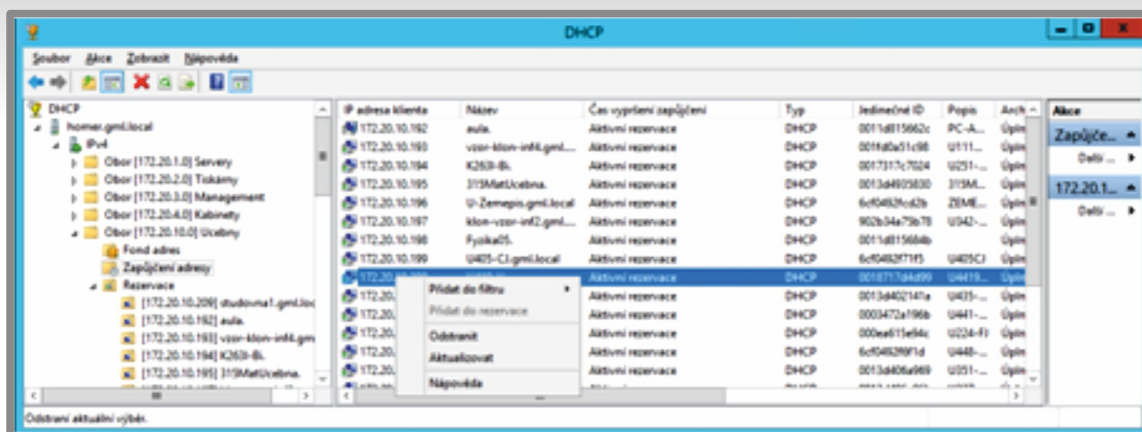


případně nějaké rozsahy adres vyloučíme. Mož-
nosti pro obor můžeme nastavit buď rovnou
v průvodci nebo posléze v konzoli hotového
oboru:



Na obr. vpravo jsou Mož-
nosti oboru 172.20.10.xxx. Vidí-
me, že brána (směrovač, default
gateway, přes ni se dostaneme ven ze sítě) je nastavena na 172.20.10.254, servery DNS
(viz následující kapitola) na 172.20.10.1 a 172.20.10.2, doménový název obdrží počítač
gml.local a kdyby chtěl startovat po síti, požádal by stanici 172.20.1.13 (řekl by si jí o soubor
boot\x86\pxelinux.com, který by si stáhnul a předal mu řízení).

Seznam aktuálně půjčených adres najdeme u oboru v záložce Zapůjčení adresy:

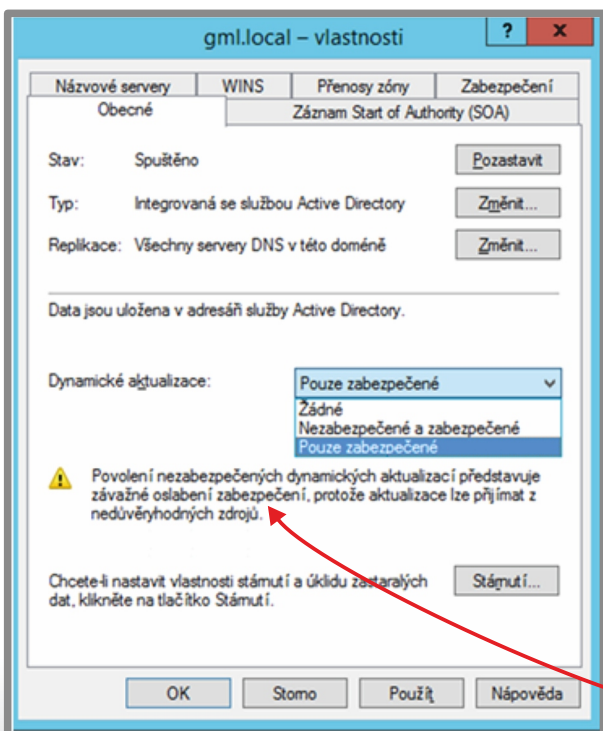


Vidíme zde IP-adresu, název počítače (ten, který má stanice uveden v Ovládacích panelech-Systém je silnější a je vhodné nechat si jím přepsat i ten v DHCP serveru) i MAC adresu.

Stanici lze v kontextovém menu přidat do Rezervací (pokud by tam ještě nebyla), a od toho okamžiku bude získávat adresu stále stejnou, tuto. Naopak, do Rezervací nebudeme přidávat „hosty“, kteří jsou v síti jen na chvíli.

Školní DNS server

Rovněž školní DNS server (=server, který dotazy na doménová jména typu www.seznam.cz překládá na IP-adresy typu 77.75.76.3) je v dnešní době nutností. Respektive, teoreticky se lze spolehnout na DNS server providera, ale pak by všechny lokální počítače nebylo možné oslovovat DNS jménem, ale pouze IP-adresou..

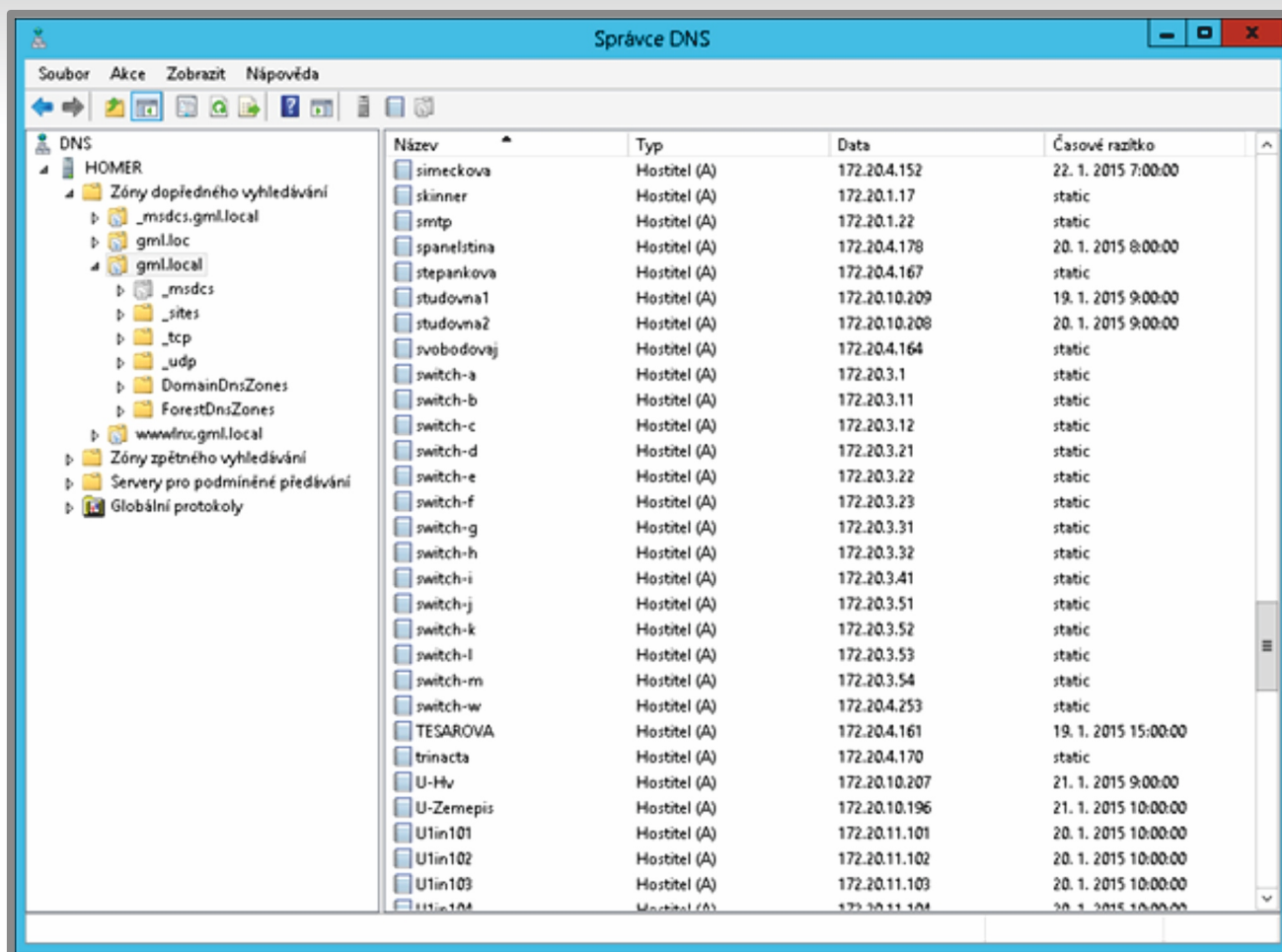


Mezi DNS serverem, Active Directory a DHCP serverem je dobré nastavit „spolupráci“: *Co DHCP server přidělí a Active Directory ověří, že do ní patří, to DNS server zaindexuje a začne pojmenovávat.*

Případá Vám ověření přes AD zbytečné? Ano, může fungovat i spolupráce: *Co DHCP server přidělí, to DNS server zaindexuje a začne pojmenovávat.* Ale je krajně nebezpečné ji provozovat. Vyhodí-li někdo v aule pojistky a přijde-li s vlastním počítačem pojmenovaným Aula, DHCP server mu adresu přidělí, DNS přeindexuje původní záznam a všichni budou s počítačem aula.gml.local komunikovat, aniž by tušili, že mluví s někým jiným... I windowsí server před touto „slepou důvěryhodností“ varuje:

Obrázek pochází z DNS konzole (dialogové okno vznikne kliknutím Vlastnosti v kontextovém menu nějaké Zóny dopředného vyhledávání). DNS konzole na windows

serveru standardně vypadá takto:



Název	Typ	Data	Časové razítko
simeckova	Hostitel (A)	172.20.4.152	22. 1. 2015 7:00:00
skinner	Hostitel (A)	172.20.1.17	static
smtp	Hostitel (A)	172.20.1.22	static
spanelstina	Hostitel (A)	172.20.4.178	20. 1. 2015 8:00:00
stepankova	Hostitel (A)	172.20.4.167	static
studovna1	Hostitel (A)	172.20.10.209	19. 1. 2015 9:00:00
studovna2	Hostitel (A)	172.20.10.208	20. 1. 2015 9:00:00
svobodovaj	Hostitel (A)	172.20.4.164	static
switch-a	Hostitel (A)	172.20.3.1	static
switch-b	Hostitel (A)	172.20.3.11	static
switch-c	Hostitel (A)	172.20.3.12	static
switch-d	Hostitel (A)	172.20.3.21	static
switch-e	Hostitel (A)	172.20.3.22	static
switch-f	Hostitel (A)	172.20.3.23	static
switch-g	Hostitel (A)	172.20.3.31	static
switch-h	Hostitel (A)	172.20.3.32	static
switch-i	Hostitel (A)	172.20.3.41	static
switch-j	Hostitel (A)	172.20.3.51	static
switch-k	Hostitel (A)	172.20.3.52	static
switch-l	Hostitel (A)	172.20.3.53	static
switch-m	Hostitel (A)	172.20.3.54	static
switch-w	Hostitel (A)	172.20.4.253	static
TESAROVA	Hostitel (A)	172.20.4.161	19. 1. 2015 15:00:00
trinacta	Hostitel (A)	172.20.4.170	static
U-Hiv	Hostitel (A)	172.20.10.207	21. 1. 2015 9:00:00
U-Zemepis	Hostitel (A)	172.20.10.196	21. 1. 2015 10:00:00
U1in101	Hostitel (A)	172.20.11.101	20. 1. 2015 10:00:00
U1in102	Hostitel (A)	172.20.11.102	20. 1. 2015 10:00:00
U1in103	Hostitel (A)	172.20.11.103	20. 1. 2015 10:00:00
U1in104	Hostitel (A)	172.20.11.104	20. 1. 2015 10:00:00

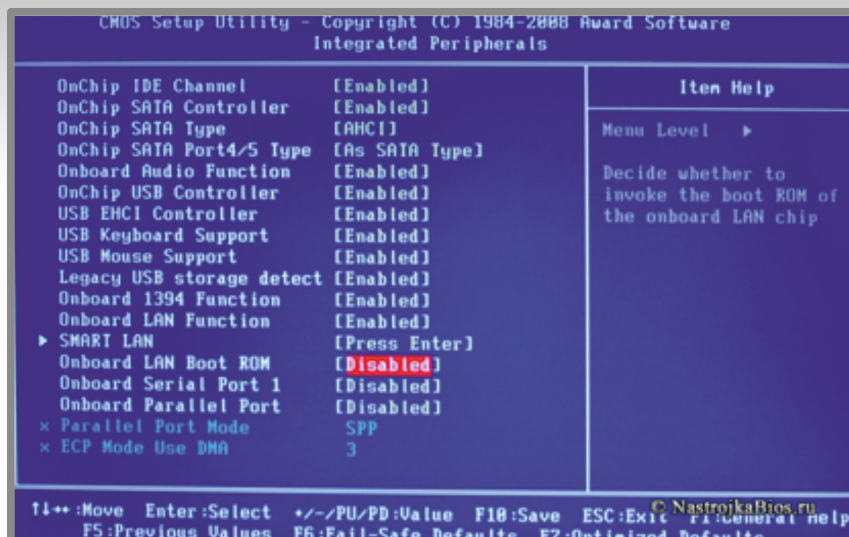
V Zónách dopředného vyhledávání vidíme přehlednou tabulku se vztahem mezi DNS jménem a IP-adresou. Ve sloupci Časové razítko jde buď o dynamicky přidělenou adresu od DHCP serveru (vidíme, kdy byla naposledy obnovena) nebo o „static“, kterýžto záznam vyrobil ručně administrátor, je statický a nikdy nebude změněn – statický záznam používáme u zařízení se statickými adresami (typicky u switchů, u nichž při startu není vhodné DHCP o adresu žádat) a též u počítačů, u nichž sedí víc kantorů (jeden a tentýž PC má dle svého jména dynamickou adresu anglictina.gml.local a statickou adresu trinacta.gml.local, vlk.gml.local a mikesova.gml.local).

Je dobré, aby aplikační servery mají alternativní statickou adresu pojmenovanou podle své funkce (smtp.gml.local, avg.gml.local, www.gml.local, safeq.gml.local, tisk.gml.local, ...), budeme-li DNS adresu poctivě používat ve všech konfiguracích, je pak velmi jednoduché aplikační server přehodit na jiný fyzický server (jiné železo, jiný virtuální počítač), například při upgradu nebo při nečekaném hardwarovém problému.

Boot server

Boot server je počítač, který startující stanici po síti pomocí technologie PXE pošle celý operační systém, stanice si jej zavede do RAM paměti a předá mu řízení (nastartuje, aniž by potřebovala lokální disk).

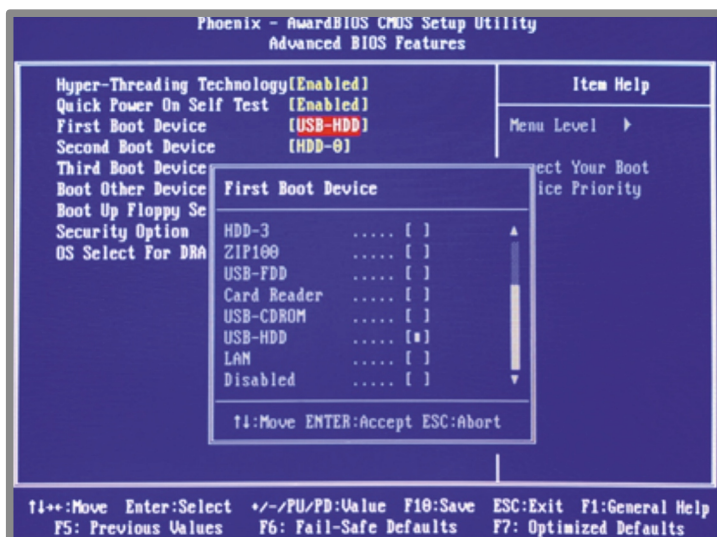
Prakticky všechny síťové karty umějí PXE zapnout, jde-li o integrovanou síťovou kartu, pak je ale v BIOSu její možnost PXE bootování obvykle vypnutá. Nastartujeme klientský počítač, pomocí DEL (či F2 či jiného tlačítka) vlezeme do BIOSu a nastavíme jej, typicky:



Obr.:

<http://www.nastrojka BIOS.ru/setevie-nastrojki/onboard-lan-boot-rom.html>,

Poté vyskočí v menu „Boot order“ nová položka, kterou je třeba dát před hard-disk, typicky:



U některých BIOSů obsahují položky „Boot order“ dvě různě znějící síťové karty (například „LAN“ a „Realtec PXE“), z nichž funguje pouze jedna (obvykle ta se složitějším názvem).

U jiných BIOSů zase zapnutí BootROM u síťové karty automaticky vynucuje primární bootování z PXE.

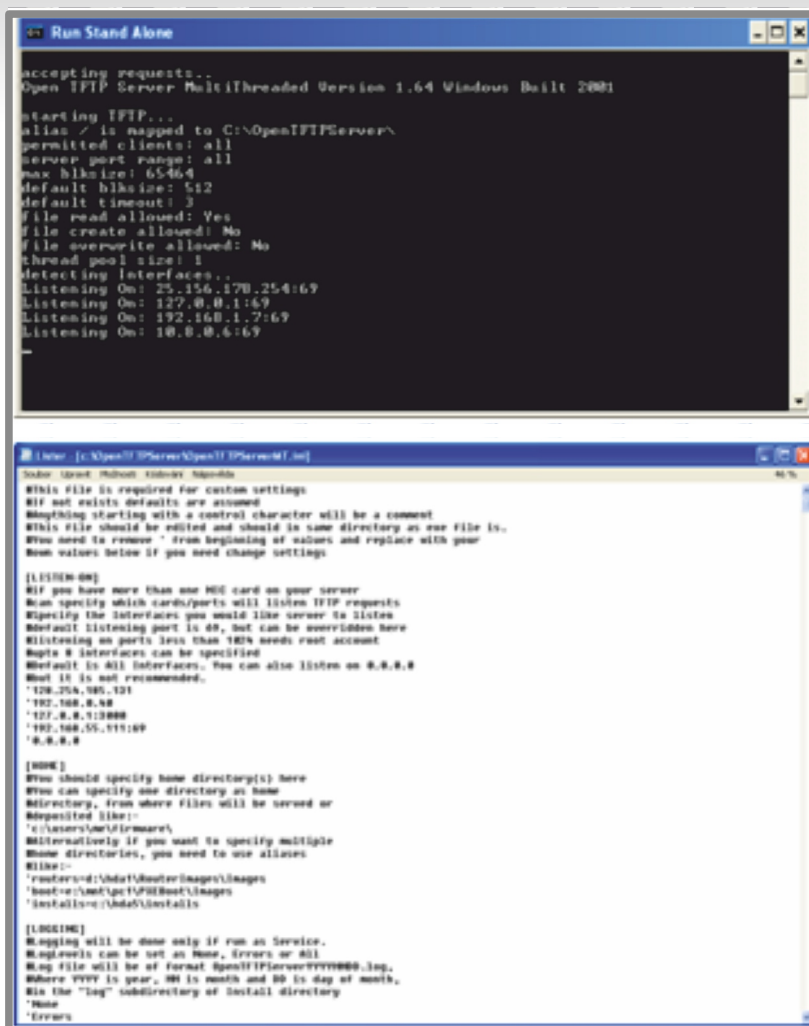
U většiny BIOSů lze nastavit možnost aktuální změny startovacího místa stisknutím F12 při startu (bez nutnosti ukládání nastavení do BIOSu), což je na jednu stranu pohodlné, na druhou stranu ovšem krajně nebezpečné – uživatel může nastartovat z vlastního CD či vlastního USB zařízení svůj vlastní operační systém a převzít kontrolu nad počítačem i daty v něm...

Boot server pod linuxem

...je v podstatě součástí balíku dhcpd, resp. je nutné ke správnému bootování ještě přiinstalovat balík tftpd. Prakticky ihned po instalaci a základním nastavení dhcpd je systém připraven poskytovat boot obrazy. Je třeba nakonfigurovat, kde který obraz leží a jak vypadá menu, jež se při startu ze sítě objeví. (Viz konfigurace o několik řádků níže.)

Boot server pod běžným windowsím PC

...stačí stáhnout instala-lačky k nějakému TFTP serveru (doporučím např. OpenTFTP, <http://sourceforge.net/projects/tftp-server/>, instaluje se Next-Next-Finish, běží jako služba či jako běžná aplikace, konfiguruje se jednoduchým textovým souborem .ini):

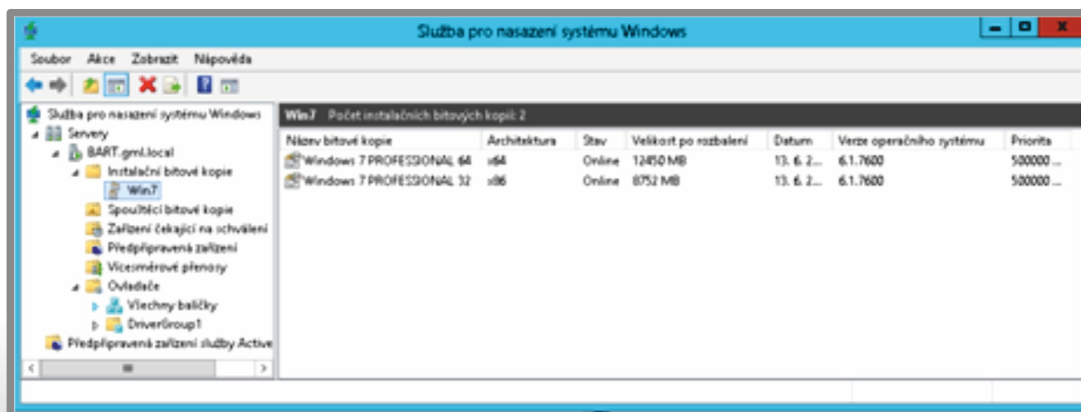


Je příjemné doma takový příruční boot server mít, často má člověk „na opravu“ počítač, který nespouští z disku. Teoreticky lze provozovat i portable verzi (např. na flashce, s sebou).

Boot server pod Windows serverem

Boot server zde figuruje pod službou WDS, Windows Deployment Services, česky Služba pro nasazení systému Windows. (Respektive, WDS toho nabízí maličko víc, umí nejen nastartovat ze sítě instalaci, ale i rozdistribuovat polopřipravené instalace windowsích stanic po síti.)

I pro WDS je na serveru jednoduchá konzole:



Zde ale nezapřeme původně linuxový původ, takže se menu a další nastavování dělá ručně.

Konfigurace boot serveru a soubory, jenž používá

Ať jde o jakýkoliv bootserver na jakékoliv platformě, potřebujeme k jeho provozu TFTP server, v jehož adresáři je nutné mít soubory:

pxelinux.0 ... binární soubor, který řídí vlastní start operačního systému (stáhne binárku s menu, řídí stisky kláves při startu)

menu.c32 či barevný **vesamenu.c32** ... binární soubor, řídí vykreslování a vlastní pohyb v menítku

soubory **default** (obvykle v adresáři pxelinux.cfg), příp. **default.001217d43049** či jen třeba **default.001217d4** (číslo udává MAC adresu či část MAC adresy) – může jich být více pro různé síťové karty či skupinu síťových karet. Bootovací menu tak teoreticky můžeme přizpůsobit stanici, která o něj žádá – jiné bude pro kantory, jiné pro učebny, jiné pro cizí počítače...

Soubor default může obsahovat odkazy do jiných textových souborů obsahujících podmenítka.

Ajak default vypadá? Například:

```
MENU TITLE Install a Tools

LABEL Ghost
  MENU LABEL Hiren - ^Norton Ghost (se siti)
  kernel memdisk
  append priority=low vga=normal initrd=/_tools/hirens/boot_ghost.ima

LABEL NetBoot
  MENU LABEL ^Hiren (mini)
  kernel memdisk
  append priority=low vga=normal initrd=/_tools/hirens/boot.ima

LABEL Hiren
  MENU LABEL H^iren
  kernel memdisk
  append priority=low vga=normal initrd=/_tools/hirens/boot_full.ima

LABEL Puppylinux
  MENU LABEL ^Puppy Linux 5.2.5
  kernel /_Linux/x86/puppy/puppy-linux-vmlinuz
  append initrd=/_Linux/x86/puppy/puppy-linux-newinitrd.gz

LABEL stresslinux
  MENU LABEL ^Stresslinux x86-64 0.7.177
  KERNEL /_Linux/x86/stresslinux/initrd-netboot-suse-11.4.x86_64-2.1.1.kernel
  APPEND initrd=image/initrd-netboot-suse-11.4.x86_64-2.1.1.gz
ramdisk_size=1101824

label GParted Live
  MENU LABEL ^GParted Live
  kernel /_tools/gparted_vmlinuz
  append initrd=/_tools/gparted_initrd.img boot=live config union=aufs
noswap noprompt vga=788
fetch=http://172.20.1.13/filesystemy/filesystem.gparted.squashfs

label RescueCD
  MENU LABEL ^Rescue CD
  kernel /_tools/rescuecd
  append initrd=/_tools/rescuecd_initram.igz
netboot=http://172.20.1.13/filesystemy/filesystem.sysrcd.dat

label KonBoot
  MENU LABEL ^Kon-Boot (hacking utility)
  kernel memdisk
  append initrd=/_tools/konFLOPPY.img

label Clonezilla Live
  MENU LABEL ^Clonezilla Live
  kernel /_tools/clonezilla_vmlinuz
  append initrd=/_tools/clonezilla_initrd.img boot=live live-config noswap
```

```
nolocal edd=on nomodeset ocs live_run="ocs-live-general"
ocs_live_extra_param="" ocs_live_keymap="" ocs_live_batch="no" ocs_lang=""
vga=788 nosplash
fetch=http://172.20.1.13/filesystem/filesystem.clonezilla.squashfs

label HDT
MENU LABEL ^Hardware Detection Tool
kernel memdisk
append initrd=/_tools/hardware-detection-tool-0.5.0.img

label AVG
menu label ^AVG Rescue CD
kernel /_tools/avg vmlinuz
append max_loop=255 vga=791 initrd=/_tools/avg_initrd.lzm init=linuxrc

label pxeknife
MENU LABEL ^PXE Knife --->
kernel vesamenu.c32
append pxeknife/pxeknife.conf

LABEL thinstation
MENU LABEL Installer for ThinStation
KERNEL /_tools/thinstation vmlinuz
APPEND initrd=/_tools/thinstation initrd splash=silent,theme:default
console=tty1 vt.global_cursor_default=0 loglevel=3 LM=3 earlyprintk=serial

LABEL Main Menu
MENU LABEL ^Back to Main Menu
KERNEL vesamenu.c32
APPEND pxelinux.cfg/default
```

Každá položka v menu musí mít k dispozici vlastní soubor s kernelem (jádro zavádějící systém), jde-li o podmenu, pak je kernelem soubor vesamenu.c32 či menu.c32, jde-li o nějaký nástroj, obvykle bývá kernel ke stažení na webu (v celém .zip balíku s PXE konfigurací).

Dále musí být k dispozici image, čili vlastní operační systém (něco jako bitová kopie bootovatelného CDčka), ten lze obvykle rovněž stáhnout z webu příslušného nástroje. Image je nejlépe mít menších rozměrů, starší TFTP servery měly limit 32 MB, dnes sice limit není, ale musí se vlézt do RAM paměti a velké image se hůř po síti tahají. Image si může administrátor vyrobit i z běžné diskety či běžného CD či .iso, osvědčil se mi program WinImage (<http://www.winimage.com/>), ten umí dokonce soubory rozbalit na disk/zabalit zpět, čili ideální pro „vrtání se uvnitř“.

Chceme-li image mít opravdu malý, aby se dobře do paměti přes PXE natáhnul, některé nástroje jej mají jen jako „další loader“ – zavedou si jádro (schopné přístupu k síti přes http) a zbytek si fetchnou z připraveného webového serveru.

Například nástroj GParted má v menu řádky:

```
label GParted Live
MENU LABEL ^GParted Live
kernel /_tools/gparted vmlinuz
append initrd=/_tools/gparted initrd.img boot=live config union=aufs noswap
noprompt vga=788 fetch=http://172.20.1.13/filesystem/filesystem.gparted.squashfs
```

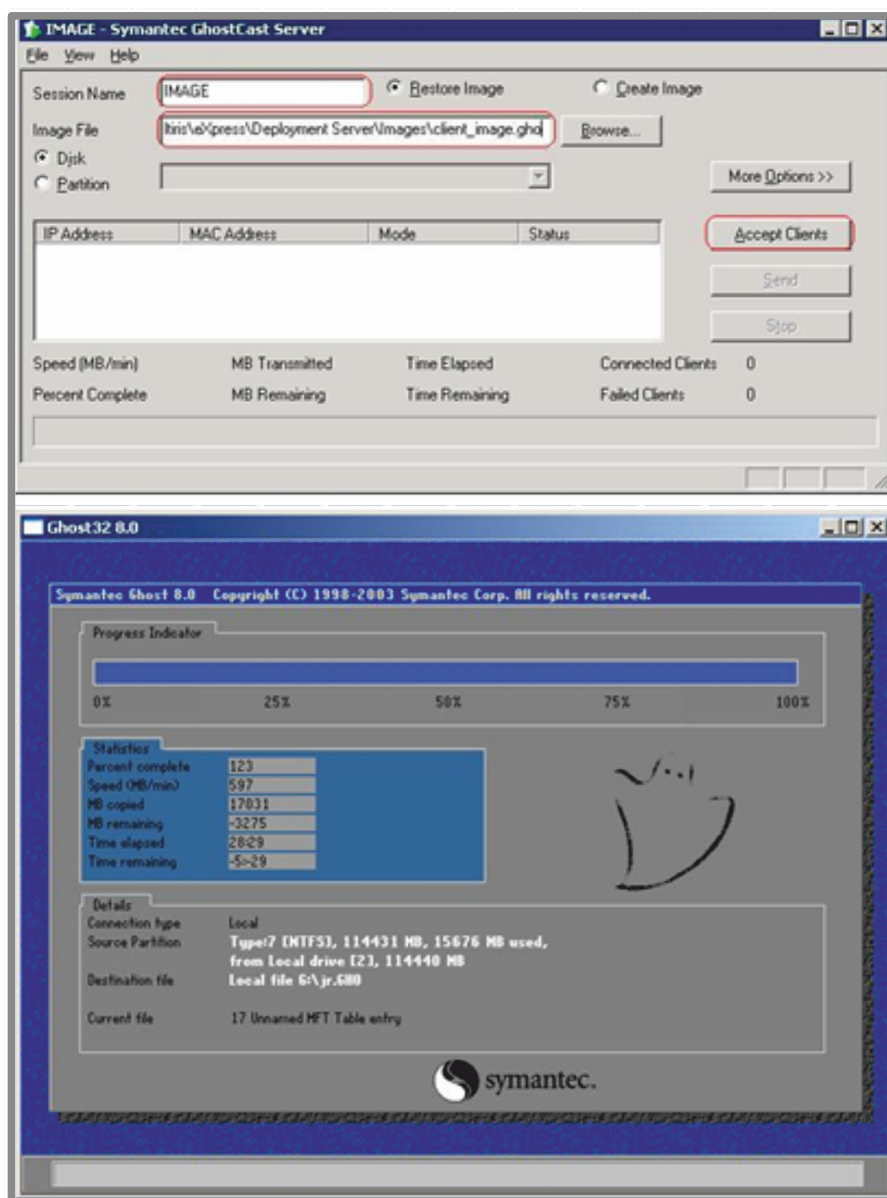
Tedy v menítku uvidíme text GParted Live (s podtrženým G), vybereme-li si jej, stáhne se kernel **/_tools/gparted_vmlinuz**, což je obvyklé jádro pro tahání linuxových operačních systémů, to stáhne image **/_tools/gparted_initrd.img**, který dostane pokyn, aby nainstaloval live, bez swapování, bez ptání, s barvičkama a fetchnul si **<http://172.20.1.13/filesystem/filesystem.gparted.squashfs>**, kde je vlastní operační systém (112 MB).

Nastavování boot serveru chce jistou zkušenost, jednotlivé PXE nástroje jsou obvykle linuxové, některé hůř dokumentované, takže práce občas probíhá metodou pokus-omyl. Ale ten výsledek stojí za to...

Klonování disků/diskových oddílů po síti

S možností startu OS po síti se otevírá i možnost klonování po síti. (Respektive, klonovat disky po síti lze i z běžně spuštěného operačního systému, například připojím-li k běžným windows či linuxu další disk třeba přes USB-SATA či USB-IDE převodník, mohu jej naklonovat v grafickém prostředí klonovacích nástrojů přímo v OS.)

Nastartujeme-li MS-DOS s podporou TCP/IP protokolu (skvěle se pro takový start hodí Hiren's Boot CD, <http://www.hirensbootcd.org/>, toto CD toho umí opravdu, opravdu hodně, stáhněte si jej!), lze poté pod MS-DOSem spustit program Norton Ghost, kterým lze klonovat stanice buď Peer-to-peer nebo připojením ke Ghostcast serveru. Ghostcast server se velmi hezky provozuje jako program pro Windows, má intuitivní rozhraní a nabízí dokonalý přehled, kdo se k němu připojil a komu jaká data unicastem/multicastem posíláme:

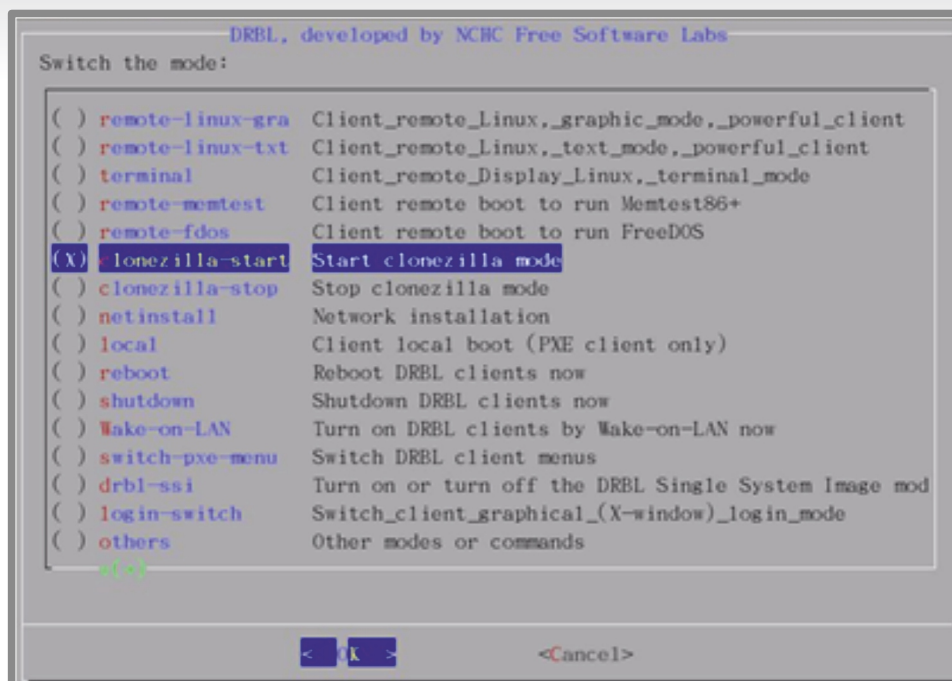


Obr.: Ghostcast server a DOSový klient, zdroje:

<http://www.symantec.com/business/support/index?page=content&id=HOWTO31153>, <http://www.symantec.com/connect/forums/customizing-ghost-consol-background-and-or-color>

Program Norton Ghost je licencovaný, rovněž Ghostcast server se musí kupovat.

Nastartujeme-li ze sítě linuxový program Clonezilla, máme k dispozici textové rozhraní, na jehož logiku si administrátor musí chvíli zvykat:



Obr.: Po startu Clonezilly, zdroj: <http://clonezilla.org/clonezilla-SE/>

Klonujeme-li multicastem, musíme mít toto všesměrové vysílání povolené v centrálním počítači pro daný VLAN. Multicastovou propustnost mezi VLANy (že by klonovací server byl v jiném VLANu než cílové stanice) lze velmi komplikovaně nastavit, prakticky je „multicastová samostatnost“ VLANů jedním z důvodů, proč si VLANy pořizujeme – aby se VLANy mezi sebou nerušily kdejakým balastem. Nejpraktičtější je, máme-li klonovací server dostupný ve většině VLANů (což lze samozřejmě na switchi nastavit).

Pro klonování existuje celá řada komerčních programů, dobrou zkušenost mám s Acronis True Image (verze Home zdarma, <http://www.acronis.cz/domacnosti-a-kancelare/produkty/true-image-home/>).

Klonování počítačů, které jsou připojené do AD, řadič domény většinou velmi špatně snáší – klon musíte z AD odebrat, tím se ale ani originál do AD nedostane, takže druhou stanici taky (na oko) odeberete, pak klonu změníte jméno a oba zase hezky připojíte... Podstatně jednodušší je mít připraveny klony jednotlivých stanic těsně před jejich vstupem do AD (nebo těsně po jejich výstupu).

Systémy sledování sítě

Na sledování toků sítě se nejlépe hodí pasivní část protokolu SNMP. „Pasivní část“ znamená, že jednotlivé síťové prvky (switche, servery, tiskárny, ...) čekají na oslovení sledovacím snmp-klientem, kterému pak poctivě odpoví velké množství informací, v jakém jsou stavu – jaká mají počítadla průtoku dat, kolik je připojených klientů, jak využívají CPU či paměť, jaký je pagecount tiskárny, ...

Aby nám síťový prvek odpovídal, musí v něm být SNMP zapnut (obvykle bývá vypnutý), nastaveno tzv. community name (obvykle bývá „public“) a režim SNMP protokolu (verze 1, verze 2c či verze 3, ta je nejsofistikovanější, umí i autentifikovat tazatele). Je též vhodné povolit SNMP odpovědi jen někomu (na základě IP-adresy).

Nejjednodušším klientem je textový snmpwalk (lze nainstalovat v linuxu jako balíček ve všech možných distribucích, stejně jako pod Windows, doporučuji pod nimi net-snmp, <http://sourceforge.net/projects/net-snmp>).

Například příkaz `snmpwalk 172.20.2.25 -v 2c -c public | head` odeslaný na kopírku Minolta bizhub C220 odpoví (zkrácená verze, `| head` vrátí jen prvních 10 řádků):

```
iso.3.6.1.2.1.1.1.0 = STRING: "KONICA MINOLTA bizhub C220"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.18334.1.1.1.2.1.57.2.2
iso.3.6.1.2.1.1.3.0 = Timeticks: (67630559) 7 days, 19:51:45.59
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = ""
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.2.1.0 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
(...)
```

Dodám ještě: `snmpwalk 172.20.2.25 -v 2c -c public | wc -l` odpoví: **1397**

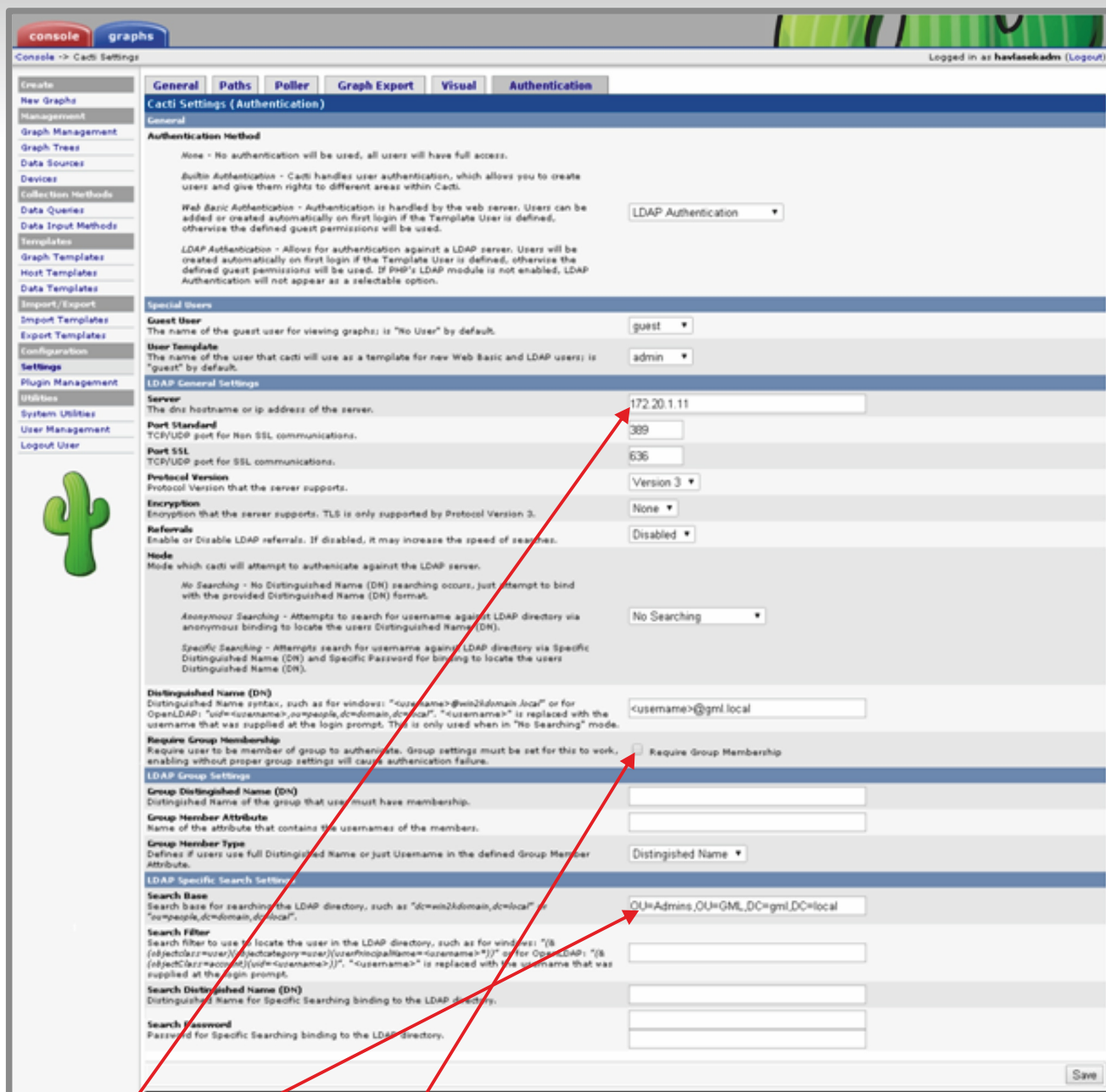
Pro nelineuxáky: Celý výpis, co kopírka odpoví, má 1397 řádků.

„Překladem“ jednotlivých `iso.3.6.1.2.1.1.1.0` čísel (dodáním významu pro strohá čísla) jsou tzv. MIB záznamy. Není ovšem až tak jednoduché je získat, špatně se googlí, rovněž mám špatnou zkušenost s komunikací s výrobcí hardware. Podstatně jednodušší je zjistit požadovaná data metodou reverzního inženýrství: vyklikám si v grafickém rozhraní pagecount kopírky, vyhledám si ve výpisu snmpwalku stejné číslo, ověřím mezi nimi korelaci.

Číst textové informace z výstupu snmpwalku není úplně ideální (nanejvýš, že by si administrátor nad nimi napsal nějaký skript s výstupem podle svého). Vhodnější je používat monitorovací systém. Doporučit mohu MRTG (<http://oss.oetiker.ch/mrtg/>, pro sledování síťového provozu), Ganglia (<http://ganglia.sourceforge.net/>, ideální pro sledování serverů), Nagios (<http://www.nagios.org/>, velmi hezký). Osobně používám Cacti (<http://www.cacti.net/>), z popísaných monitorovacích systémů mi připadá, že má největší uživatelskou základnu a podporu na vlastních diskuzních fórech.

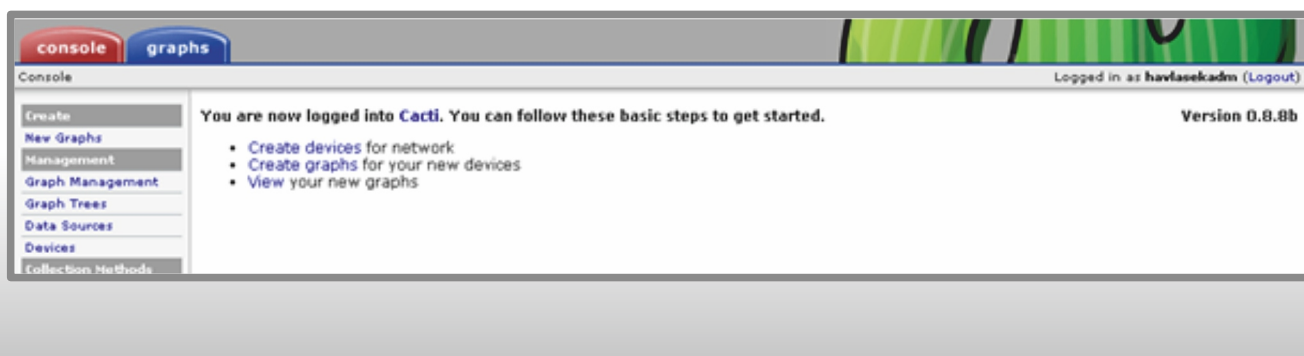
Konfigurace Cacti a nastavení síťového prvku v něm

Cacti stáhneme jako `.zip` nebo jako `.tar.gz`, rozbalíme do podadresáře nějakého webového serveru. Běží prakticky okamžitě, zvolíme pouze způsoby autentifikace uživatelů: buď necháme ověření uživatelů na lokálních cacti-účtech, nebo je ověříme webovým serverem, na němž běžíme, nebo můžeme uživatele ověřovat pomocí LDAP (tedy z AD); pro LDAP stačí nastavit: (na další stránce)



AD server, který ověřuje pokud bychom chtěli povolit přihlášení jen uživatelům z nějaké skupiny cesta v AD-struktuře, odkud se uživatelé berou (na obr. jsou bráni jen uživatelé z podpoložky Admins)

Při přihlášení vidíme v Console pouze:



Postup nastavení sledování nějakého síťového prvku sestává z několika kroků.

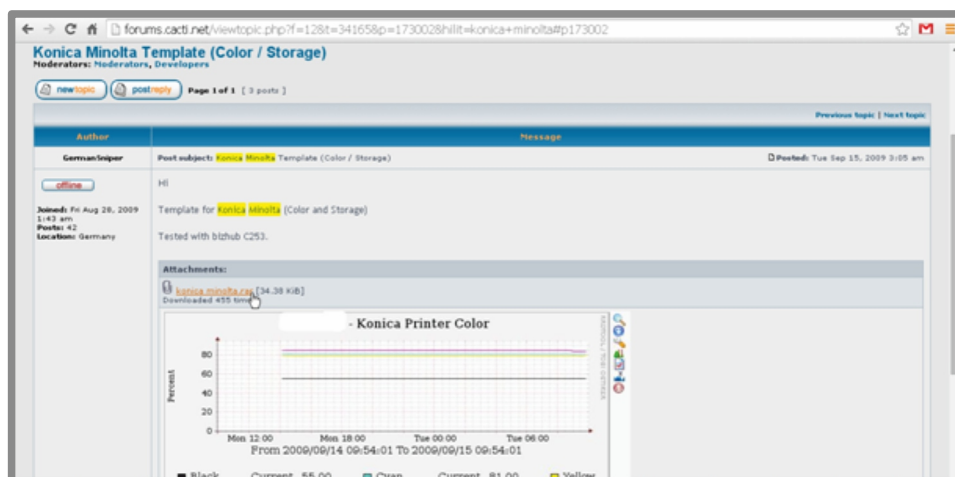
1. Nejprve importujeme template.

Jako největší problém bych viděl nutnost sehnání a import správného Template (vzoru, který nějaký nadšený pokročilý uživatel Cacti musel podle vzoru MIB vyrobit).

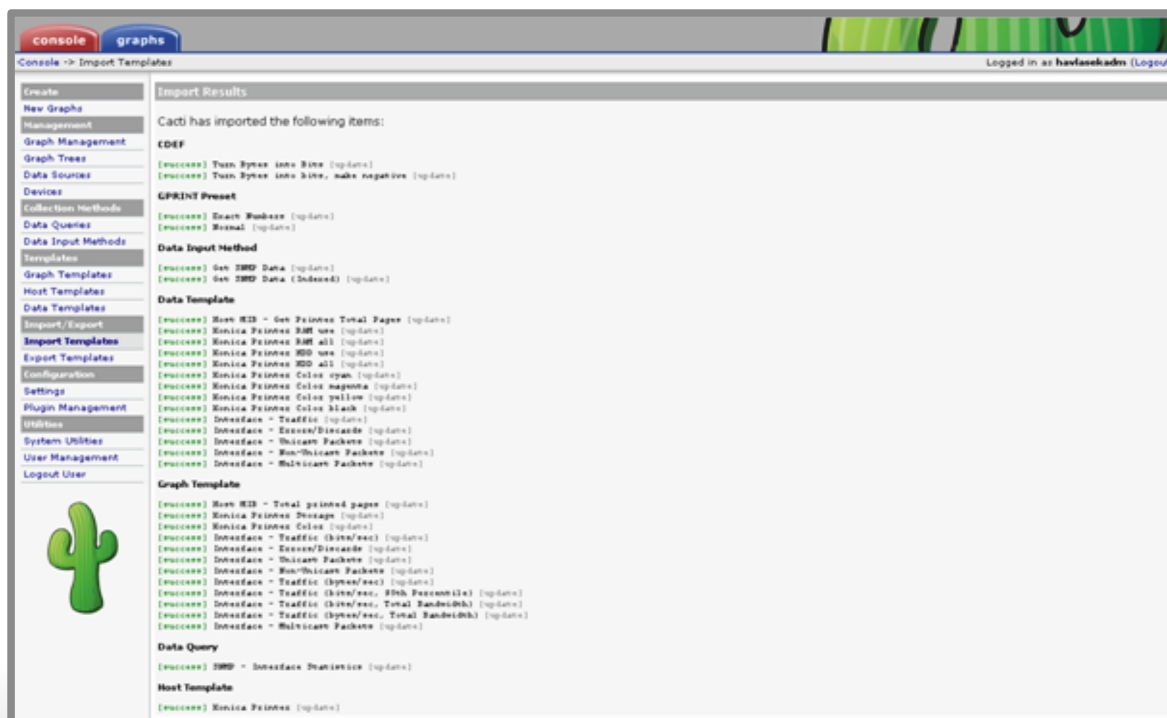
Template se dá obvykle dohledat

na oficiálním webu (<http://docs.cacti.net/templates>) nebo na Cacti-fóru

(<http://forums.cacti.net/viewforum.php?f=12&sid=c3c74f1cc590af76048839ae30b23bc7>), například pro dotaz Konica Minolta:



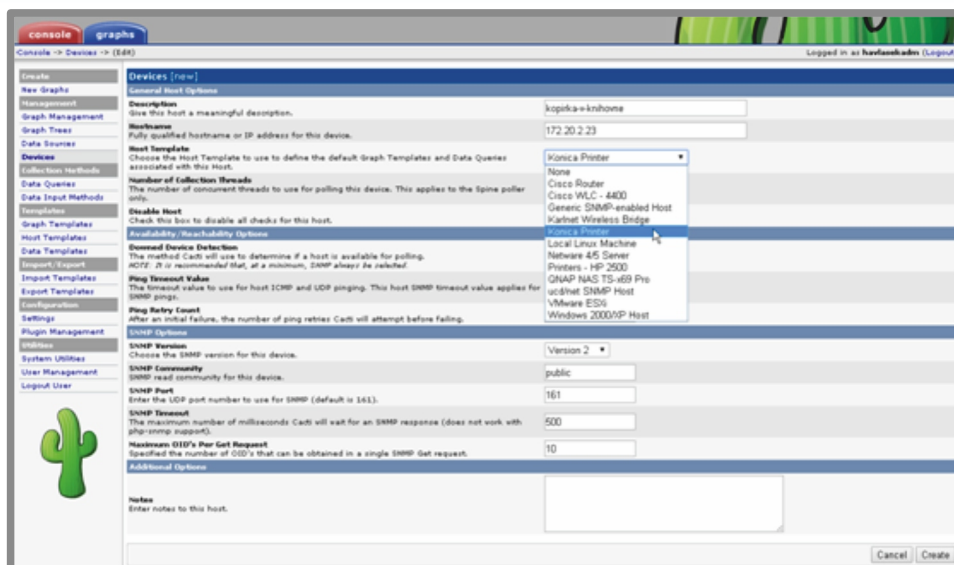
Stáhneme .rar, rozbalíme do lokálního adresáře, v menu Cacti (sloupec vlevo) zvolíme Import Templates. Některá sofistikovanější sledování je nutné podpořit uploadem skriptu (psaného v Perlu, shellu, PHP, prostě různě) zevnitř .raru do podadresáře site/scripts uvnitř webu cacti (typicky tedy /var/www/html/cacti/site/scripts). Pokud vše dopadne dobře, vidíme protokol:



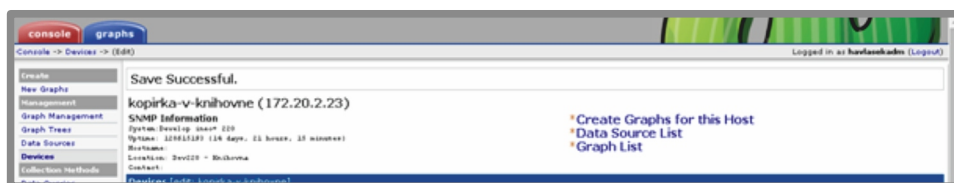
Pozn.: Na screenshotu je všude status [update], protože už jsem template pro Konica Printer v Cacti měl... ☺

2. Vyrobit Device

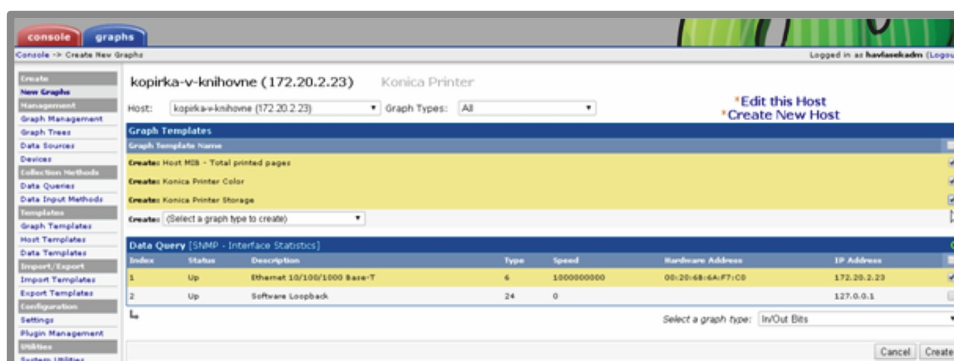
Kliknutím na Devices, vpravo nahoře na Add, do Cacti přidáme fyzické zařízení, které sledujeme. (Máme-li třeba v síti tři podobné kopírky od Minolty, provedeme přidání Device třikrát). Příklad přidání nového device:



Po přidání (kliknutím na Create vpravo dole) vidíme status:



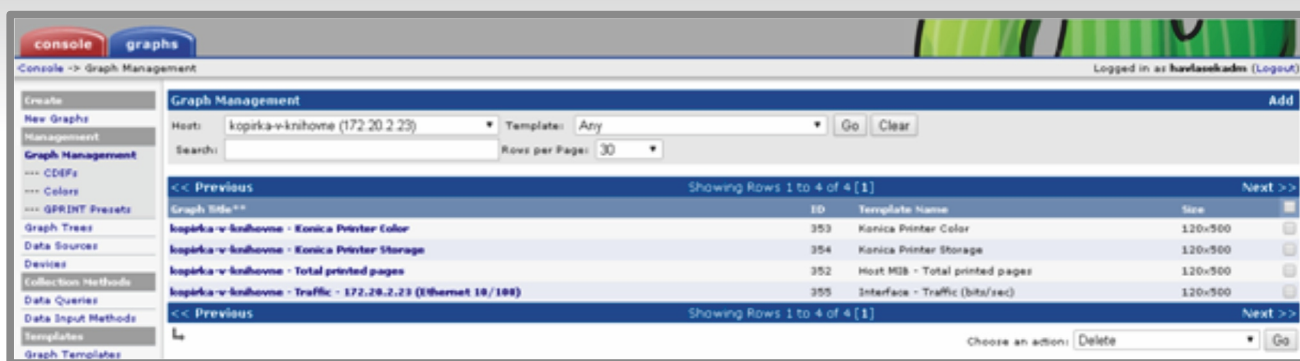
3. Správně bychom měli přidat Data Source a teprve potom vyrobit graf. Zde nás ale Cacti navádí, že nám Data Source vyrobí automaticky, podle toho, jaký graf si zvolíme. Klikneme proto rovnou na link Create Graphs for this Host, v následné stránce zvolíme grafy, které by se nám u kopírky líbily (standardně jsou připravené „Host MIB – Total printed pages“, „Konica Printer Color“ a „Konica Printer Storage“, dole též „Ethernet 10/100/1000“) – těm, co chceme, musíme vpravo zafajfkovat checkboxy:



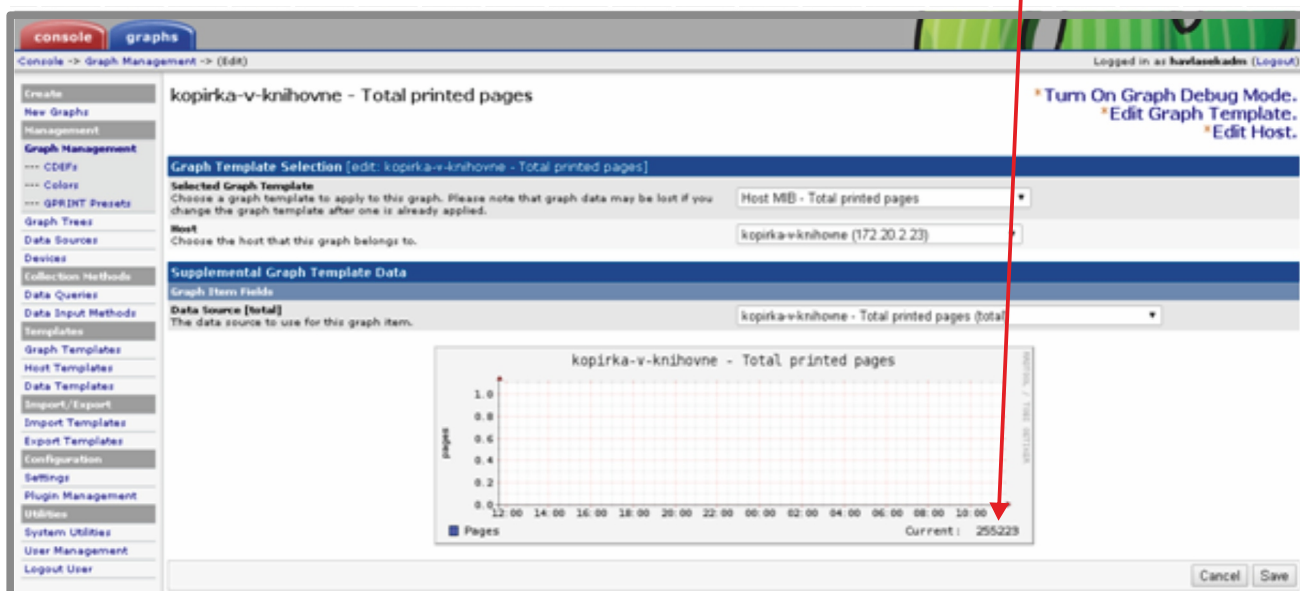
Po kliknutí na Create:



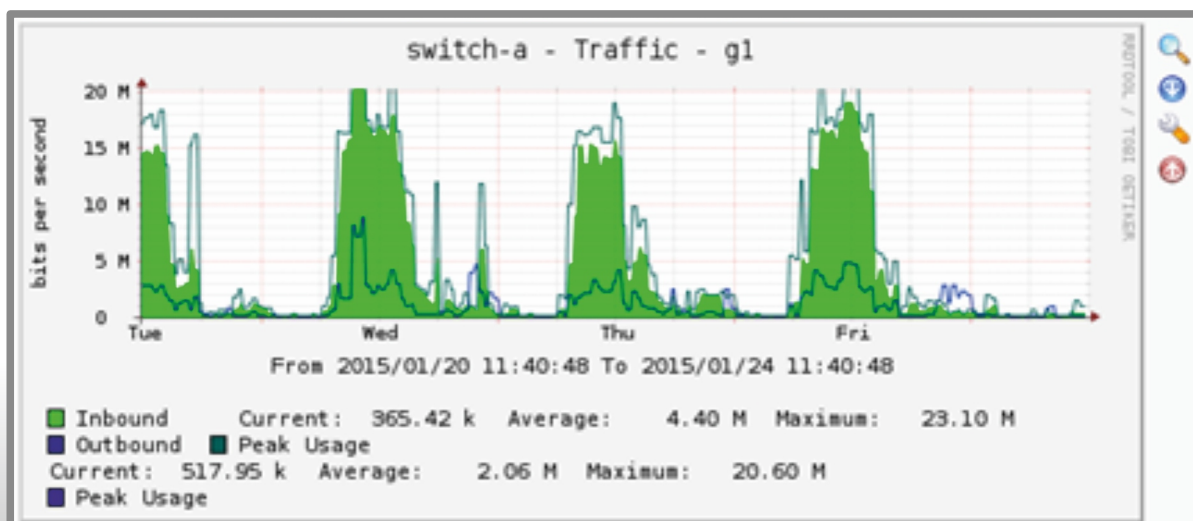
4. Položkou Graph Management v menu vlevo si lze prohlédnout, že zařízení grafy má:

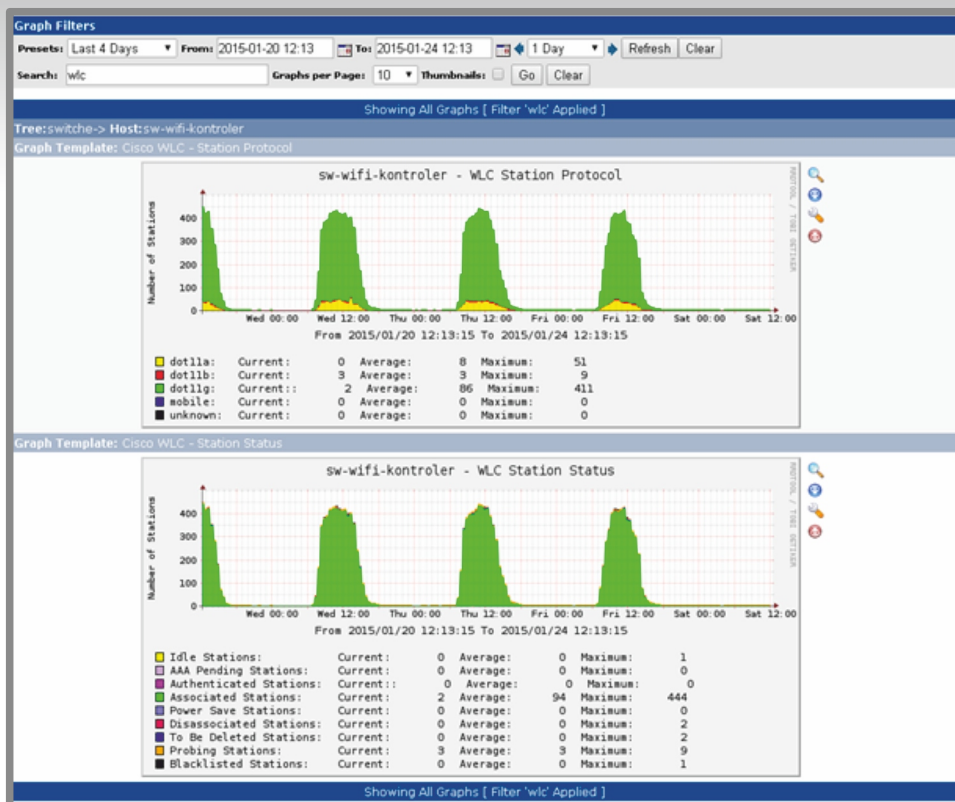


Nečekejme ovšem, že hned budou zobrazovat nějaké relevantní hodnoty. Následuje chvíle čekání (ideální čas jít pracovat na něčem jiném a těšit se, jak to dopadne). Grafy potřebují čas, aby se vyrobily (hlouběji v Cacti lze každému zařízení nastavit, jak často se data tahají a grafy vyrábějí). Po minutě se dozvíme alespoň hodnotu, druhý den pak bude i graf.



Nejzajímavější jsou samozřejmě grafy provozu síťových switchů a u wifi controlleru:



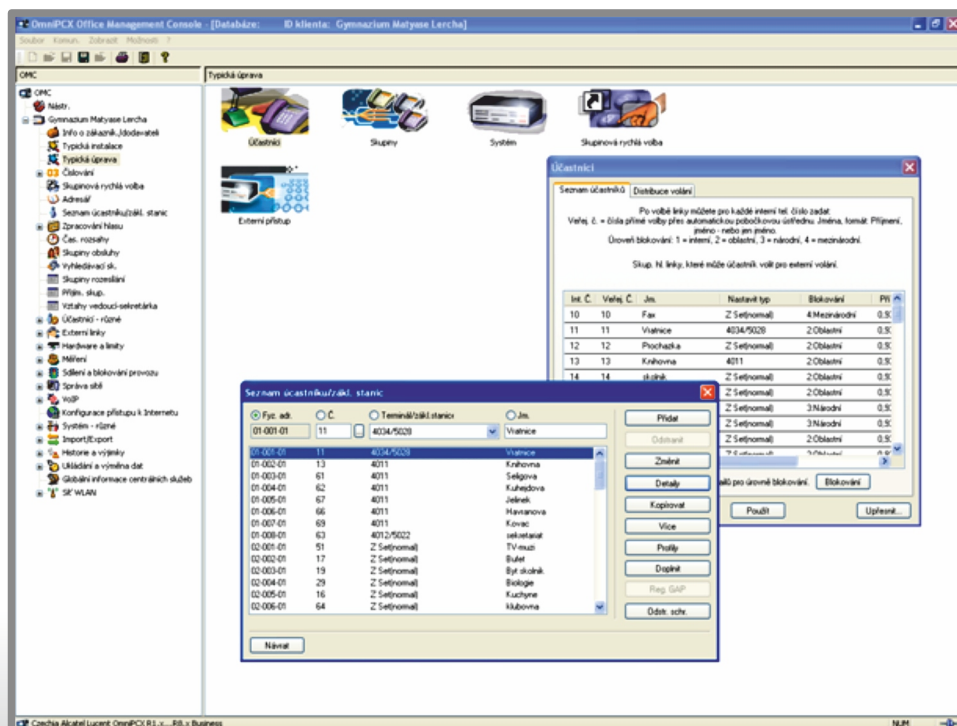


Povšimněte si horní lišty, v níž si můžeme nastavovat libovolnou dobu od-do (počínaje minutami, konče roky) a grafy jsou ihned skriptem překresleny...

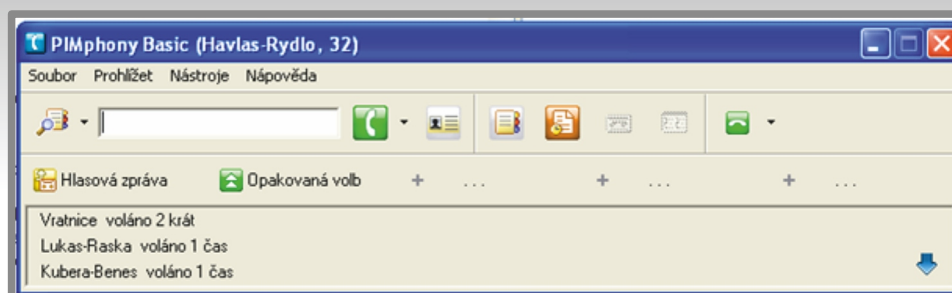
Analogová a VOIP telefonie

Telefonie se správy sítí týká okrajově, proto jen ve zkratce: Běžným standardem je digitální telefonní ústředna s analogovými linkami. Výrobci je mnoho, uživatelské rozhraní je funkčně poměrně podobné. Očekávejte: aplikaci pro správu ústředny (logické pojmenování a oprávnění pro jednotlivé klapky, stahování logů o uskutečněných telefonních hovorech) a aplikaci pro jednotlivé účastníky na klapkách, kteří mohou svoji klapku digitálně ovládat (zejména vidí, kdo volá, historii zmeškaných hovorů, atd.)

Pro ilustraci screenshoty digitální telefonní ústředny Alcatel-Lucent:



Obr.: PCXTools OMC 810, aplikace pro správu telefonní ústředny (detail nastavení stanic)



Obr.: Alcatel PIMphony, aplikace pro jednotlivé účastníky na klapkách

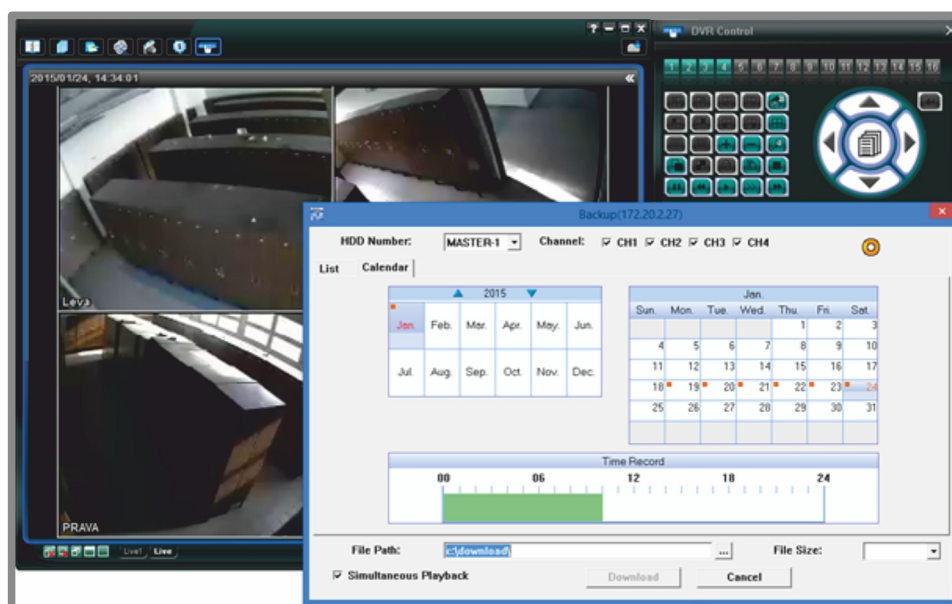
Možná je též digitální telefonní ústředna s digitálními VOIP stanicemi, ty se konfiguruji jako samostatné „stanice“ (mají vlastní IP-adresu, s ústřednou komunikují pomocí TCP/IP). Zkušenost mám pouze s osobní VOIP telefonii (s několika různými samostatně stojícími VOIP branami či VOIP telefony), digitální telefonní ústřednu+digitální stanice jsem blíže nezkoumal.

Kamerové systémy

Autor má zkušenost s digitálním kamerovým systémem s digitálními i analogovými kamerami. Opět platí, že výrobců je mnoho, uživatelské rozhraní je funkčně poměrně podobné. Očekávejte ovládání buď po webovém rozhraní nebo samostatným programem (nebo oboje), možnost stažení videa či prohlížení online.

Pozitivní zkušenost mám s IP kamerami AVTECH AVN-420 a digitálním nahrávacím zařízením.

Pro ilustraci screenshoty programu VideoViewer (připojeného na digitální záznamové zařízení NVR AVTECH AVH-0401):



Centrální správa uživatelů, skupin a oprávnění pomocí Active Directory

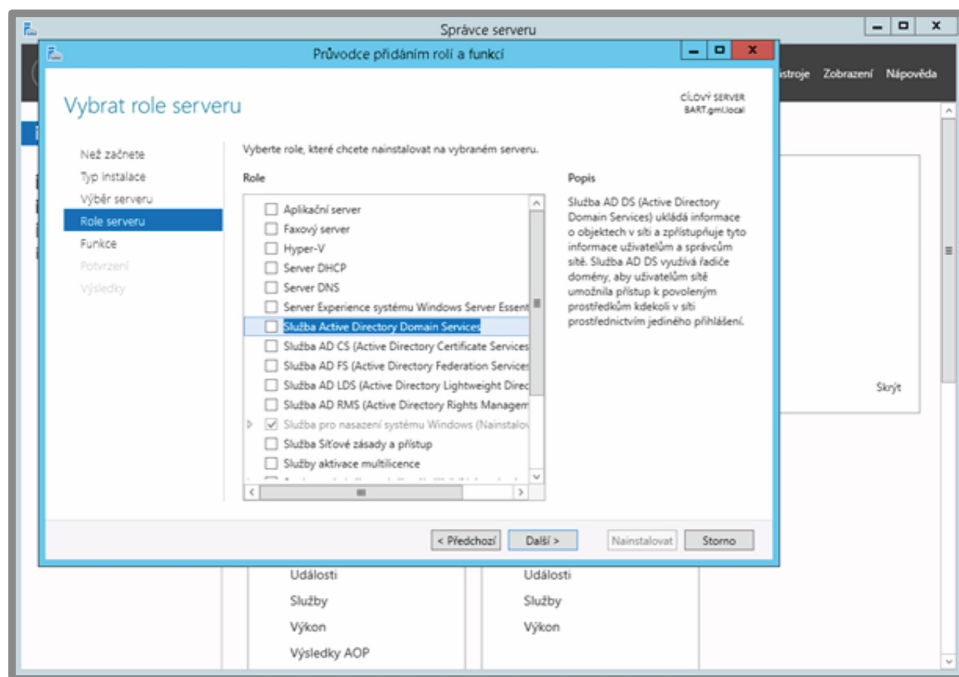
Téma, které nelze shrnout do několika minut. Mluvíme-li o doméně, jde prakticky o předchůdce AD provozovaného dřívějšími Windows Servery, první kvalitní domény byly pod Windows NT 4.0. Na Active Directory (AD) jej přejmenoval Microsoft u verze Windows Serveru 2000, následovala verze Windows Server 2003, Windows Server 2008 a Windows Server 2012, kterou budeme (v subverzi R2) rozebírat níže.

U Windows Serveru je nutné nakoupit hlavní licenci a poté licence pro jednotlivé stanice. V rámci Microsoftího programu Select se dá jedna hlavní licence pořídit za cca 6800,- Kč, jedna stanice pak za cca 220,- Kč.

Provozovat „doménu“ lze i bez Windows Serverů, čistě pod linuxovými servery (na linuxu se rozběhne Samba, když se správně nastaví, umí fungovat jako tzv. PDC, tedy Primary Domain Controller). Není to ale zdaleka ideální řešení, z hlediska úspory času, práce a nervů doporučuji klasický Windows Server pořídit. Případně i více Windows Serverů, další mohou fungovat jako BDC

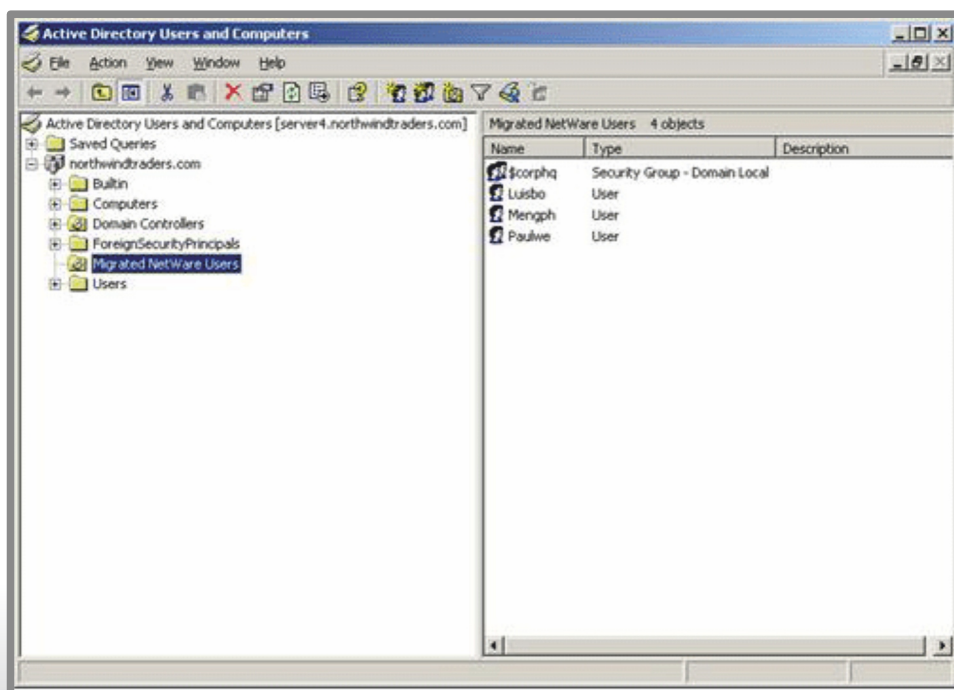
(Backup Domain Controller, v případě, že PDC z nějakého důvodu nefunguje, není paralyzována celá síť).

Po instalaci Windows Serveru mu v panelu Správce Serveru přidáme službu Active Directory Domain Services, nastavíme správné jméno a AD je na světě:



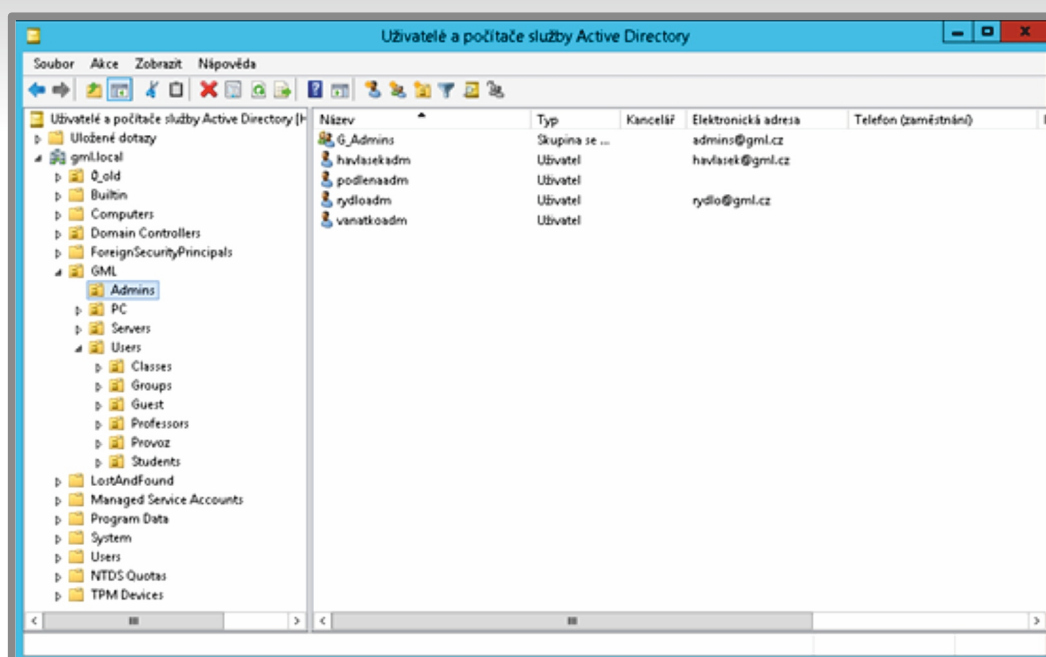
Struktura objektů v AD

V panelu Uživatelé a počítače služby Active Directory je předpřipravená základní struktura:



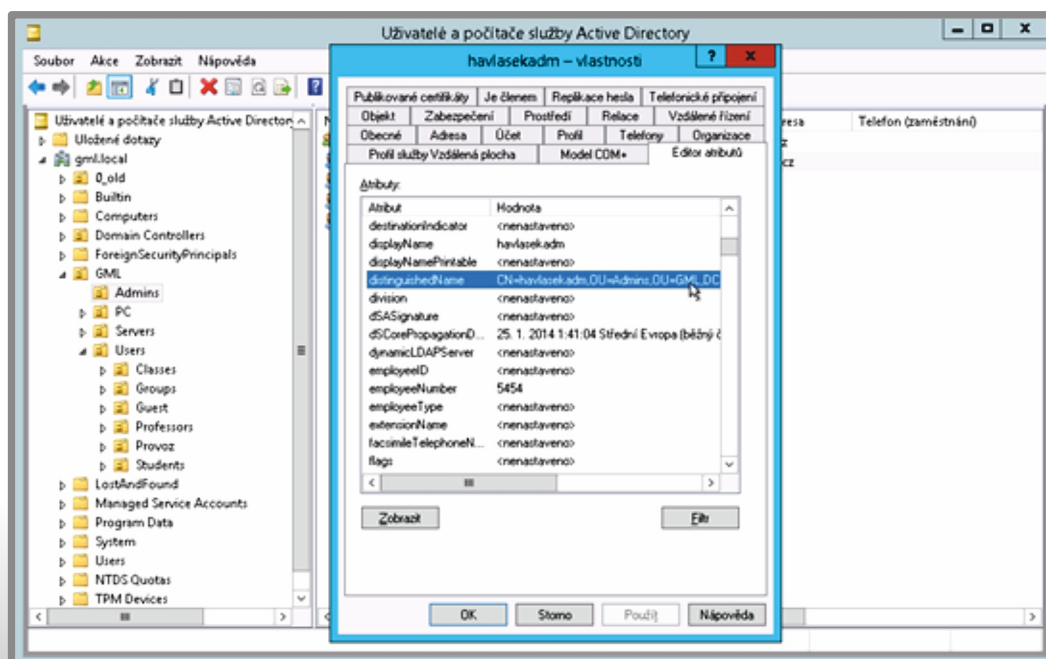
Obr.: [https://technet.microsoft.com/cs-cz/library/ff978903\(v=ws.10\).aspx](https://technet.microsoft.com/cs-cz/library/ff978903(v=ws.10).aspx), po migraci uživatelů z Novell Netware.

Strukturu rozšíříme podle aktuálních potřeb, například:



Ono sice teoreticky žádnou strukturu dodržovat nemusíme (lze nasázet vše do jednoho jediného místa, tedy počítače, uživatele, skupiny, ...), ale to by bylo nepřehledné. Vhodnější je rozdělit jednotlivá data do logické struktury – adminy zvlášť, počítače zvlášť, servery zvlášť, běžné uživatele zvlášť. A v rámci běžných uživatelů pak studentské třídy, uživatelské skupiny,...

Každý záznam uvnitř stromu má jednoznačnou cestu, tzv. Distinguished Name (DN), které třeba pro uživatele havlasekadm z výše uvedeného screenshotu vypadá takto: CN=havlasekadm,OU=Admins,OU=GML,DC=gml,DC=local (Pozor na přesnou syntaxi a velikost písmen, včetně prefixů, každá maličkost je důležitá.) Distinguished Name můžeme zjistit nejrychleji kliknutím na Vlastnosti v kontextovém menu daného záznamu, ve Vlastnostech pak DN dolistujeme v seznamu na záložce Editor atributů:



Vlastnosti uživatelů

Ve vlastnostech uživatelů je obrovské množství záložek, z nichž nejdůležitější jsou:

Obecné: základní údaje o lidech

Telefony: mimo jiné do položky Operátor defaultně linkuje SafeQ server pro číslo čipu (viz kapitola o tisku):

Profil: mj. logon-skript a připojení domovského disku, u cestovních profilů též cesta, kde je profil uložen

Organizace:

Významy, které jednotlivým vlastnostem administrátor přidělí, jsou částečně na něm samotném, částečně do jednotlivých vlastností sahají různé aplikační servery. Sémantika, kterou doporučuji, je v následující tabulce:

český název	karta, kde jej najdeme	anglický název (vlastnost v AD)	příklad u studenta	příklad u kantora
(uživ. jméno)	Obecné	Name	xadam, dále xnovak1	havlasek
Jméno	Obecné	GivenName	Vojtěch	Robert
Příjmení	Obecné	Surname	Adam	Havlásek
Popis	Obecné	Description		Mgr. Havlásek Robert
Kancelář	Obecné	PhysicalDeliveryOfficeName	4.B	32
E-mail	Obecné	Mail	xadam@gml.cz	havlasek@gml.cz
Telefonní číslo	Obecné	TelephoneNumber	bluetrox@hotmail.com	havlasek@gml.cz
Operátor-Další	Telefony	otherPager	0109208B37	04127ED1DA
Funkce	Organizace	Title		ma, inf
Poznámky	Telefony	Info	950910/4352	770608/3913
Oddělení	Organizace	Department	default	kantori

význam u studenta	význam u kantora	provázáno s...
login	login	
křestní jméno	křestní jméno	
příjmení	příjmení	
	celé jméno+příjmení včetně titulů	vypisuje se na web
třída	telefonní klapka (číslo kabinetu)	
GMLácká mailová adresa	GMLácká mailová adresa	
soukromý mail studenta	GMLácká mailová adresa (duplikát vlastnosti Mail)	nesynchronizováno se SASem! použito pro automatický reset hesla
seznam čísel čipů	seznam čísel čipů	Mapuje se v SafeQ, tahá se z kuchyňské databáze (mysql, 172.20.1.122)
	seznam zkratk předmětů, které kantor učí	vystavuje se na web updatováno z ASCTimetables
rodné číslo	rodné číslo	
statický text „default“, aby se odlišil student v SafeQ	statický text „kantori“, aby se odlišil kantor	mapuje se se střediskem v SafeQ (default, kantori)

Velmi elegantně lze k jednotlivým položkám přistupovat pomocí skriptovací technologie PowerShell. Jde o „zobecnění příkazového řádku“, pokud do něj nainstalujete rozšíření pro práci s Active Directory a též rozšíření pro práci s jednotlivými databázemi, které na organizaci fungují, lze pomocí pravidelně spouštěných skriptů synchronizovat celou organizaci...

Ideální stav, kdy by všechny databáze v celé organizaci odkazovaly na jedno místo (např. do Active Directory) ještě dlouho nenastane – integraci do AD mají většinou velké databázové systémy spíše omezenou. Příjemnou výjimkou je SafeQ (tiskový server, viz samostatná

kapitola níže).Jednoduchý script konvertující data o uživateli ze SASu do AD (jako identifikátor slouží jméno+příjmení+třída, kontroluje se rodné číslo):

```
[void][System.Reflection.Assembly]::LoadWithPartialName("FirebirdSql.Data.FirebirdClient")
$ConnectionString="User
ID=sysdba;Password=xxx;Database=172.20.1.3:/opt/firebird/sas/sas.fdb"
$Connection = New-Object
FirebirdSql.Data.FirebirdClient.FbConnection($ConnectionString)
$Connection.Open()
$Command = New-Object FirebirdSql.Data.FirebirdClient.FbCommand("select
max(pk) from skolni_rok_table" ,$Connection)
$data = $Command.ExecuteReader()
if ($data.Read()) {$mpk=$data["max"]} else {die("Nenalezen maximalni skolni
rok, asi chyba v konektovani databaze... :-(")}
$pole_studenti=@();

$string = $("SELECT tv.zkratka, tv.skolni_rok, tv.pk_trida, zv.jmeno,
zv.prijmeni, zv.ADR TRVALE EMAIL, zv.RODNE_CISLO
FROM tridy_view tv, zaci_view zv
WHERE tv.pk_trida=zv.pk_trida
AND tv.pk_sk_rok = '"+$mpk+"'
AND tv.pk_sk_rok = zv.pk_sk_rok
AND tv.pololeti=1
ORDER BY tv.zkratka, tv.skolni_rok")
$Command = New-Object FirebirdSql.Data.FirebirdClient.FbCommand($String
,$Connection)
$data = $Command.ExecuteReader()

while ($data.Read())
{
    $s=New-Object PSObject
    $s | Add-Member -MemberType NoteProperty -Name "JMENO" -Value
    $data["JMENO"]
    $s | Add-Member -MemberType NoteProperty -Name "PRIJMENI" -Value
    $data["PRIJMENI"]
    $s | Add-Member -MemberType NoteProperty -Name "ZKRATKA" -Value
    $data["ZKRATKA"]
    $s | Add-Member -MemberType NoteProperty -Name "ADR_TRVALE_EMAIL" -Value
    $data["ADR_TRVALE_EMAIL"]
    $s | Add-Member -MemberType NoteProperty -Name "RODNE_CISLO" -Value
    $data["RODNE_CISLO"]
    $pole_studenti+=$s;
}

$data.Close()
$Connection.Close()
foreach($student in $pole_studenti){
    $r=$student.RODNE_CISLO;
    $clovek = Get-aduser -Filter {Info -eq $r} -Properties
    Info,office,department
    if ($clovek)
    {
        if ($clovek.office -ne $student.ZKRATKA) {write-host($"U studenta
        "+$student.JMENO+" "+$student.PRIJMENI+" (login "+$clovek.SamAccountName+"
        nesouhlasí třída v SASu ("+$student.ZKRATKA+") s AD ("+$clovek.office+").
        Zaznam v AD jsem opravil na "+$student.ZKRATKA+"."));
        Set-ADUser $clovek -office
        $student.ZKRATKA;}
    }
    else {write-host($"Student ze SASu s rodnym cislem "+$r+" v AD
    nenalezen, zkusim jej pohledat jako "+$student.JMENO+" "+$student.PRIJMENI+"
    "+$student.ZKRATKA+"..."));
    $r1=$student.JMENO;$r2=$student.PRIJMENI;$r3=$student.ZKRATKA;
    $clovek2 = Get-aduser -Filter {(givenname -eq $r1) -and (surname -
    eq $r2) -and (office -eq $r3)} -Properties Info,office,department
    if ($clovek2) {write-host("... slava, nalezen jako
    "+$clovek2.SamAccountName+"!");}
}
}
```

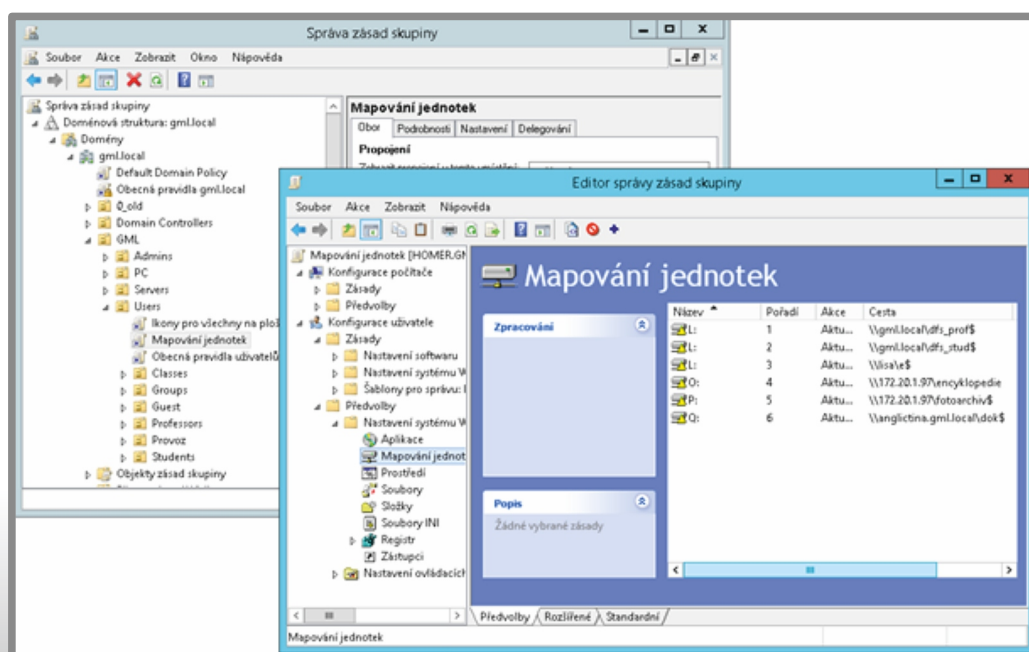
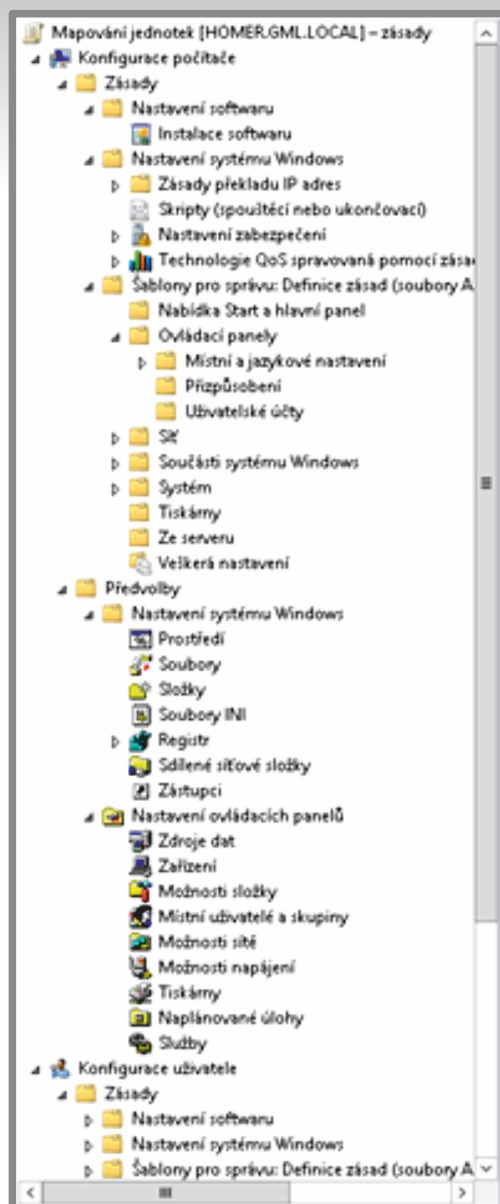
Správa zásad skupiny

Velmi silným nástrojem pro správu AD je tzv. Správa zásad skupiny (známá pod starším pojmenováním Group Policies, editované tehdy Policy Editorem).

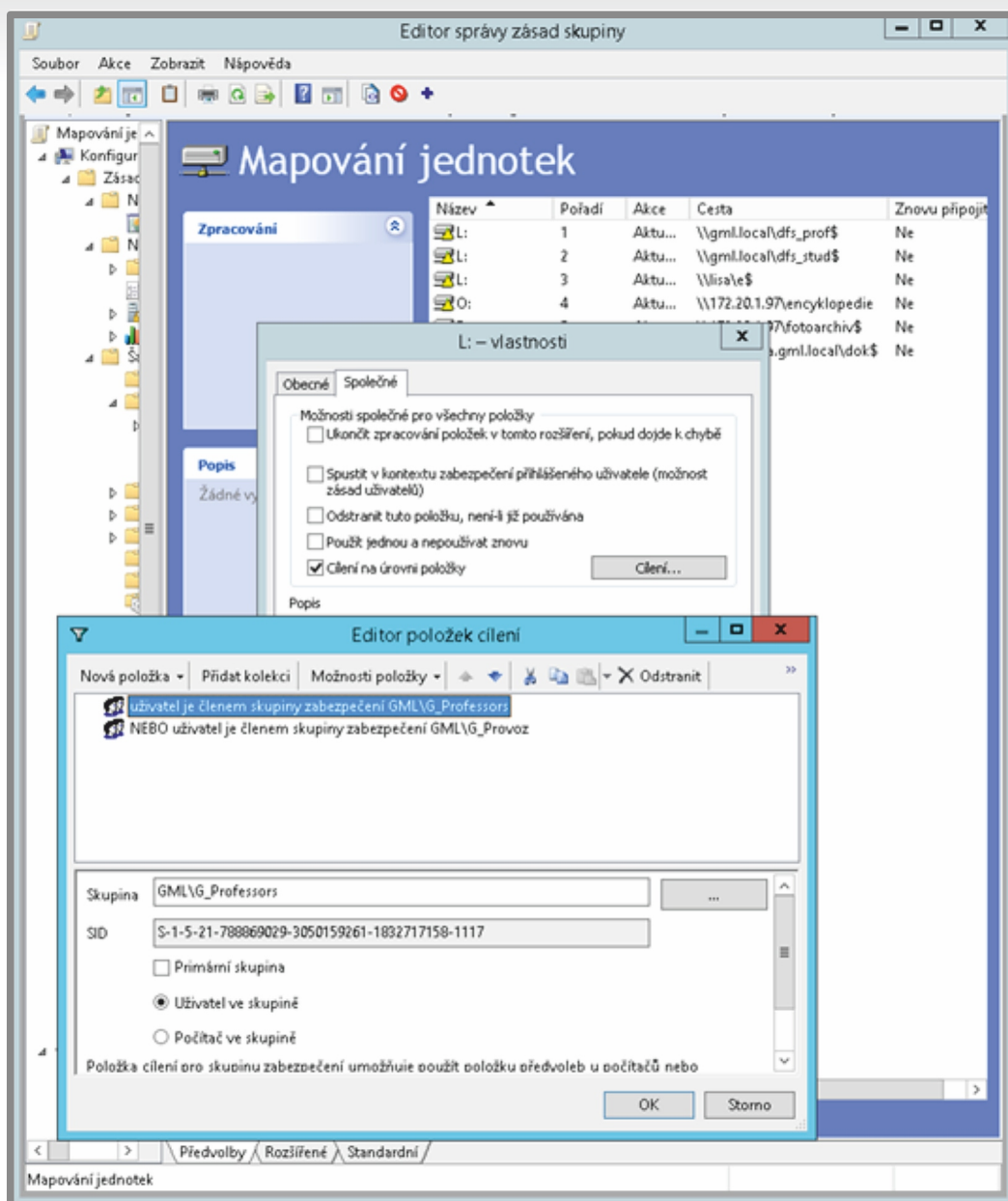
V rámci zásad může administrator činit spoustu společných nastavení pro všechny/některé stanice/uživatele. Otevře okno Správa zásad skupiny, vyrobí si nějakou novou zásadu (nebo přidá pravidla k již existující, pokud spolu nějak logicky souvisejí). Dvojklikne-li na ní, může u Počítače a/nebo u Uživatele měnit Zásady a/nebo Předvolby. Na obr. vpravo vidíte celý strom Zásad a Předvoleb pro počítač, podobné budou i pro uživatele.

Libovolná zásada i předvolba jde omezit stran své působnosti pomocí tzv. Cílení na úrovni položky – kombinacemi mnoha různých filtrů, například: přítomnosti baterie, rychlosti procesoru, místa na disku, velikosti paměti, druhu operačního systému, názvu počítače, domény, IP-adresy či MAC adresy, libovolné systémové proměnné, libovolné položky v registru, shody libovolného souboru, aktuálního času, přihlášeného uživatele, jeho uživatelské skupiny...

Například, připojujeme-li síťové jednotky, je u L: položka uvedena třikrát, pokaždé jinak, s omezením na konkrétní skupinu uživatelů:



Po kliknutí u prvního řádku L: (na němž jej mapujeme jako \\gml.local\dfs_prof\$) na Vlastnosti zvolíme na kartě Společné možnost Cílení na úrovni položky:



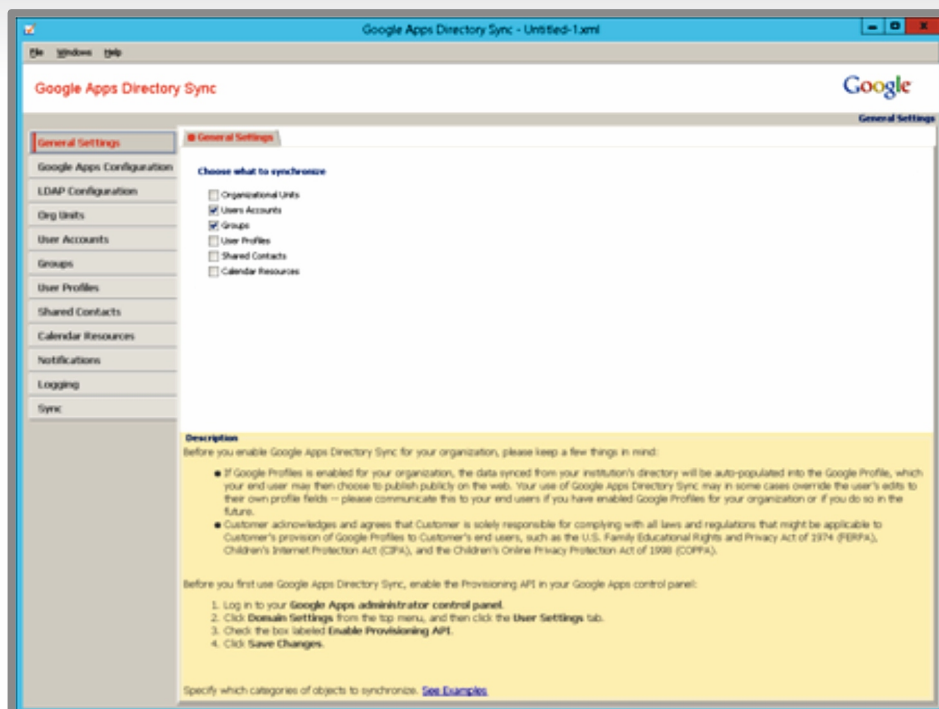
Vidíme, že pravidlo se aplikuje pouze v případě, že je uživatel členem G_Professors nebo G_Provoz.

Klíčových dovedností, které by bylo potřeba u Windows Serverů v AD zmínit, je celá řada, vycházejí obvykle z praxe a jsou poměrně dobře dokumentovány na <https://technet.microsoft.com/> (sice bez obrázků, zato poměrně podrobně).

Interakce Active Directory s Office365 nebo s Google Apps

Spojení AD a Office 365 má velmi široký rozsah. Na AD administrator nainstaluje a jednoduše nakonfiguruje nástroj Azure Active Directory Sync Tool (buď přímo do PDC nebo na nějaký jiný počítač), nakonfiguruje jej pomocí Průvodce, na Office 365 pak jen povolí synchronizaci. Jednoduchý návod najdete na [https://technet.microsoft.com/en-us/library/dn635310\(v=office.15\).aspx](https://technet.microsoft.com/en-us/library/dn635310(v=office.15).aspx)

Spojení s GoogleApps má rozsah mírně omezenější. I pro ně existuje intuitivní nástroj GoogleApps Directory Sync (viz obr. níže) a též nástroj GoogleApps Password Sync, ale Windows jako klient jaksi s Google API hůře spolupracuje. Je například nepříjemné, že si nepředávají informace o uživateli přihlášeném do počítače (zatímco u Office365 spustíte prohlížeč a automaticky jste do Office365 přihlášen účtem převzatým z aktuálního sezení Windows).



Obr.: Jednotlivé položky menu: Co se synchronizuje, konfigurace GoogleApps, konfigurace LDAP, organizační jednotky nemusejí být stejné – lze je ručně sjednotit, rovněž skupiny lze sjednocovat ručně, rovněž atributy uživatelů lze sjednocovat ručně.

Poslední položka menu je Sync, který lze nejprve otestovat a teprve poté spustit ostrý provoz:



Obecně platí, že GoogleApps ani AD nic nesmaže, leč účty, které v druhém systému nejsou, pouze znefunkční...

Centrální správa tiskáren a kopírek

V oblastech centrální správy tiskových zařízení je asi nejdále firma YSoft se systémem SafeQ (aktuálně ve verzi 5). Specializuje se především na kopírky Konica Minolta, ale umí pracovat prakticky se všemi značkami chytřejších tiskáren (viz <http://www.ysoft.cz/Partneri>). Před svojí konkurencí (HP Access Control, <http://www8.hp.com/us/en/solutions/access-control-printing-solutions/overview.html> nebo Xerox Centralware, <http://www.xerox.cz/software/produkty/software-pro-kancelarska-zarizeni/xerox-centreware-web.html>) vyniká především šíří podporovaných výrobců/modelů a komplexností celého rozhraní.

Distribuce SafeQ se provádí pouze prostřednictvím tzv. servisních organizací, což jsou firmy, které licence SafeQ přeprodejí, celý systém nainstalují a poskytují uživatelskou podporu. Obvyklý stav je, že jednotlivé kopírky (tiskárny, ostatní zařízení) zákazník pouze pronajme a platí měsíčně: paušál za pronájem kopírek, paušál za licenci na každé SafeQ zařízení, peníze za každou čb/bar vytištěnou stranu.

Instalace SafeQ serveru (byť ji obvykle dělá odborník ze servisní organizace) není nijak složitá, člověk ji má za hodinku hotovou včetně LDAP propojení s AD. Doporučují se Windows, ale lze SafeQ server provozovat i pod linuxem. Spustíte setup.exe, nainstalujete (ideálně na samostatný server), rozběhne se webové rozhraní a též rezidentní program. Přihlásíte-li se poprvé k webovému rozhraní, uvítá Vás Průvodce, nahrajete licenční klíč, necháte si na portálu <https://portal.ysoft.com> tento klíč ověřit (klíč Vám dodá a ověření musí provést někdo ze servisní organizace, je to docela komplikovaný proces, když jsem SafeQ opakovaně testoval, byly s tím docela komplikace). Nejzajímavější částí je synchronizace s LDAP: po běžném nastavení serverů+portu následuje dotaz na mapování (viz tabulka s vlastnostmi uživatelů v AD, výše):

The screenshot shows the 'Průvodce prvním spuštěním SafeQ' (SafeQ First Run Wizard) window. The 'LDAP' section is selected in the left sidebar. The main area shows configuration options for AD integration. The 'Povolit AD online integraci' checkbox is checked. Below it, there are tabs for 'Základní nastavení', 'Pokročilá nastavení', and 'Expertní nastavení'. The 'Základní nastavení' tab is active, showing fields for 'Typ' (set to AD), 'GUID', 'Login' (set to sAMAccountName), 'Jméno' (set to GivenName), 'Příjmení' (set to sn), 'E-mail' (set to email), 'Karta/PIN' (set to OtherPager), 'Domovská adresa' (set to homeDirectory), 'Mapování skupin' (set to Z kontejneru), 'Mapování středisk' (set to Ze jména v atributu), and 'Atribut se střediskem' (set to department). Navigation buttons '< Zpět' and 'Pokračovat >' are at the bottom right.

Nastavíme CRS (Central Reporting System). Kreditní systém je samostatná aplikace (=samostatná instalace), obvykle se v tomto průvodci přeskakuje, umí krom běžných metod též PayPal

(<https://www.paypal.com/cz/>), DIBS (<http://www.dibspayment.com/>), další platební metody na vyžádání. Samozřejmostí je software pro lokální pokladnu (YSoft SafeQ Credit Charger), kde si přijde uživatel s identifikačním čipem, pípne s ním na čtečce (ta funguje jako „virtuální klávesnice“), odevzdá peníze a pokladní mu „čip nabije“:

The screenshot shows the 'Y Soft SAFEQ - Dobíjecí místo 1.3.20.220' window. The 'SAFEQ Credit' interface is displayed. On the left, there are buttons for 'Kredit' (Dobít kredit, Vybit kredit) and 'Pokladna' (Stav pokladny, Tisk posl. dokladu, Uzavření pokladny). On the right, there are buttons for 'Uživatelé' (Přidat uživatele, Přidat uživatele) and 'Ostatní' (Historie, Čísloček položek). A 'Dobít kredit' dialog box is open, showing the user's credit status: ID karty (04127ed1da), Jméno (Robert Havlasek (Zam)), Login (student.04127ecc50), Aktuální kredit (644,00 Kc [% Kc]), and Částka (input field). The dialog has 'OK' and 'Storno' buttons.

U kopírek jsou pak dvě možná řešení:

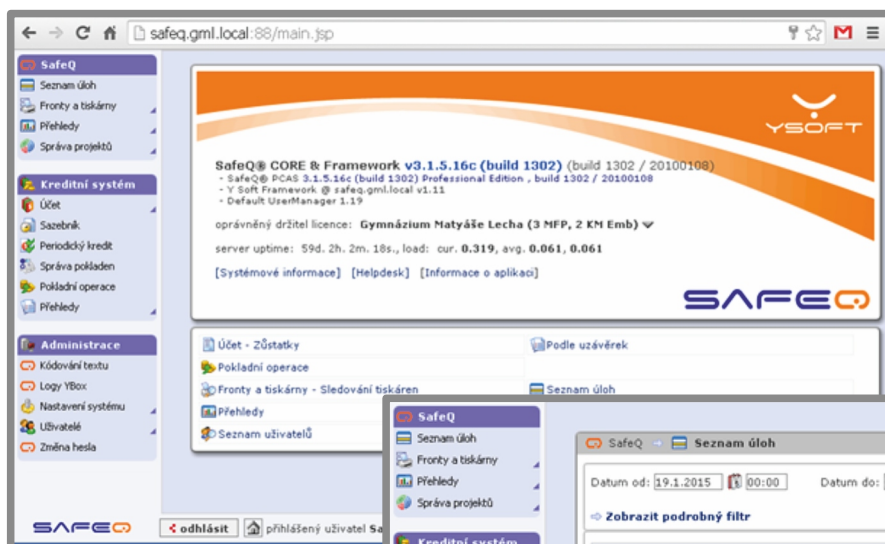
Buď si kromě SafeQ serveru rozběhneme na nějakém Windowsím počítači (klidně na stejném, co je SafeQ server) podpůrnou aplikaci SafeQ Device Server, která čísla čipů přečtených na USB-čtečce (umístěné vedle kopírky) zkonvertuje do podoby přijatelné SafeQ serverem. (Poznámka: Nepříjemné je, že SafeQ Device Server pod linux neexistuje, takže čistě linuxové řešení v této variantě není možné.)

Nebo si vedle kopírky usadíte samostatný terminál, tzv. Embedded Terminal, tedy malou krabičku, mající vlastní IP-adresu, v níž běží linux a která má integrovanou čtečku + umí čísla čipů konvertovat. Toto řešení je více nákladné a méně používané. Osobní zkušenost: Není to ideální, s kopírkou ten Embedded Terminal hůře spolupracuje.

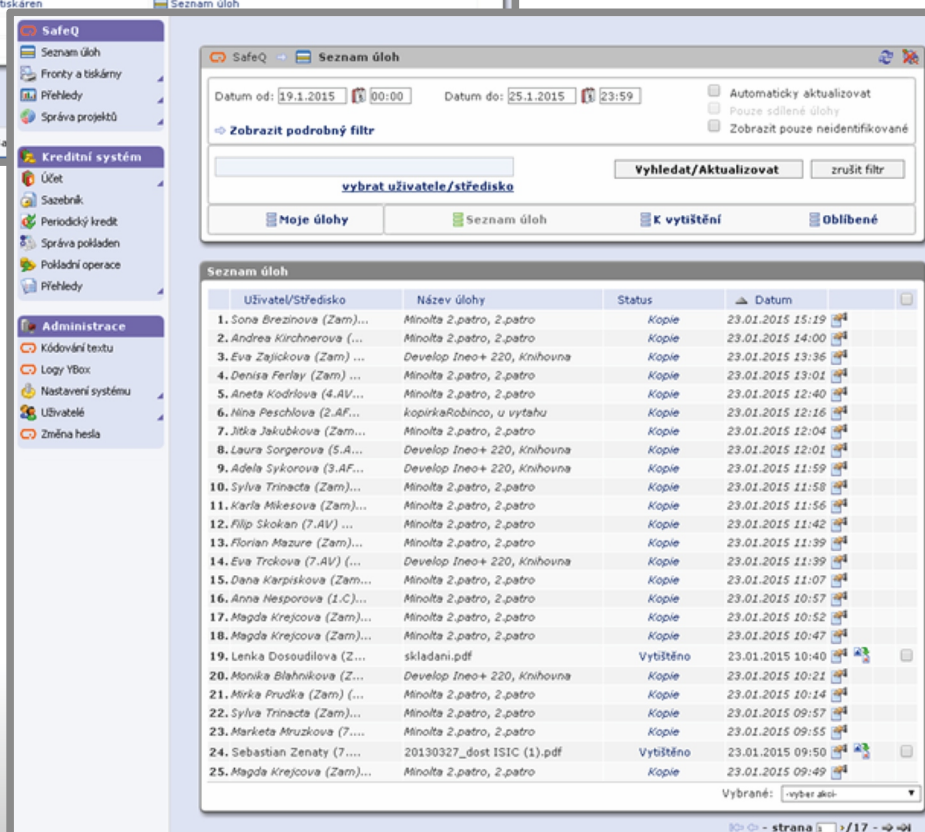
Vlastní SafeQ webové rozhraní je velmi hezky zpracované, lehce konfigurovatelné a nabízí naprostý přehled úplně o všem, co můžete potřebovat:



Zdroj obr.: <http://www.prekon.cz/1391155152/novinka-tiskoveho-reseni-y-soft-safeq-5.html>



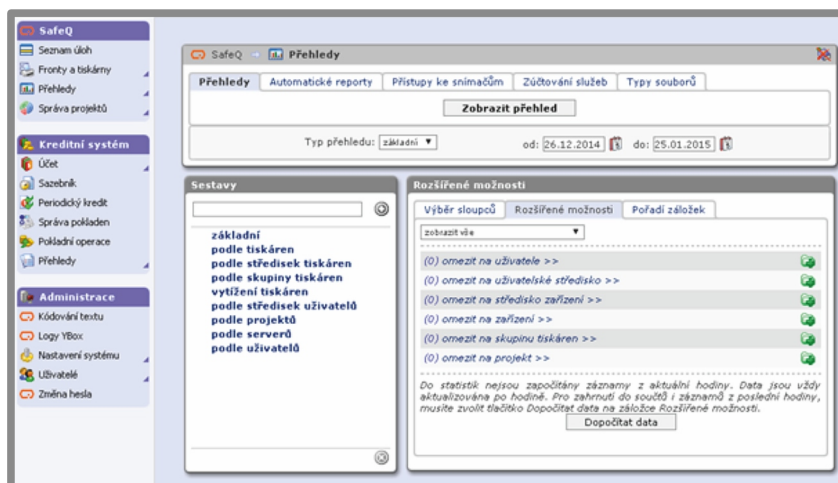
V položce Seznam úloh vidíte seznam, co se naposledy dělo (povšimněte si možnosti filtrování podle času, uživatele, střediska (=uživatelské skupiny):



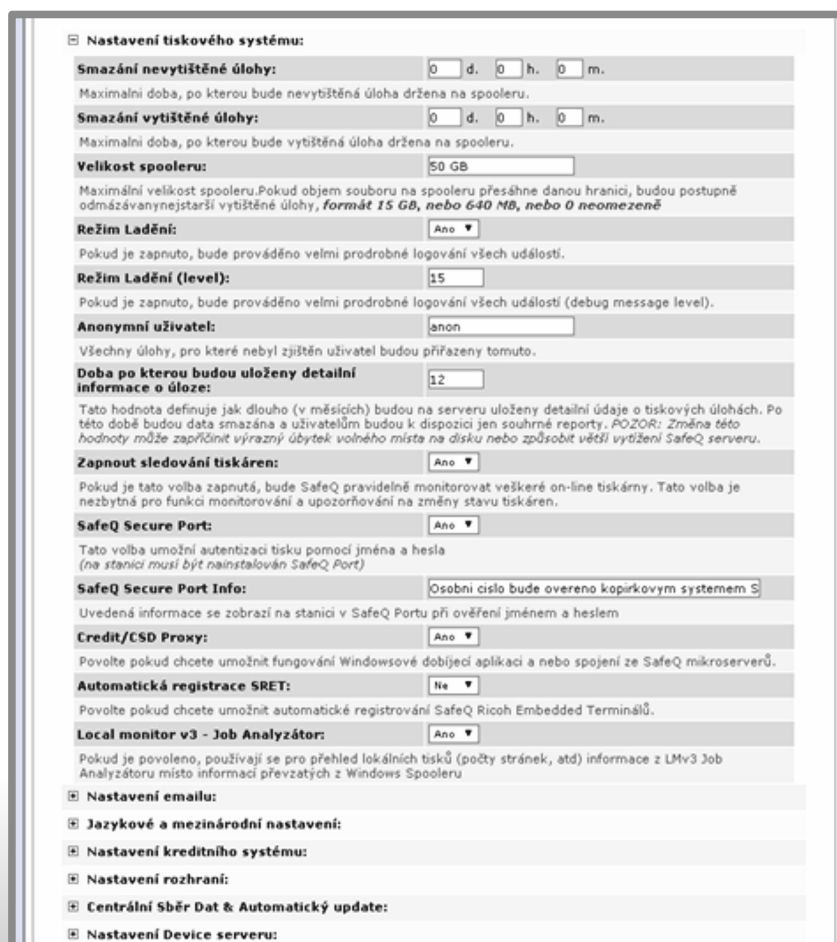
Na každou úlohu lze kliknout a zjistit o ní podrobnosti:

Historie úlohy, job #1 (42663)		
Historie úlohy Informace Status		
Datum	Stav	Zpráva
23.1.2015 15:19:39	Kopie	Bylo zahájeno kopírování (Minolta 2.patro (2.patro))
23.1.2015 15:19:39	Kopie	Úloha byla zaúčtována (12 pg., 18,00 Kc)
		Černobílé kopie: 2 pg á 1,50 Kc
		Černobílé kopie DUPLEX: 10 pg á 1,50 Kc

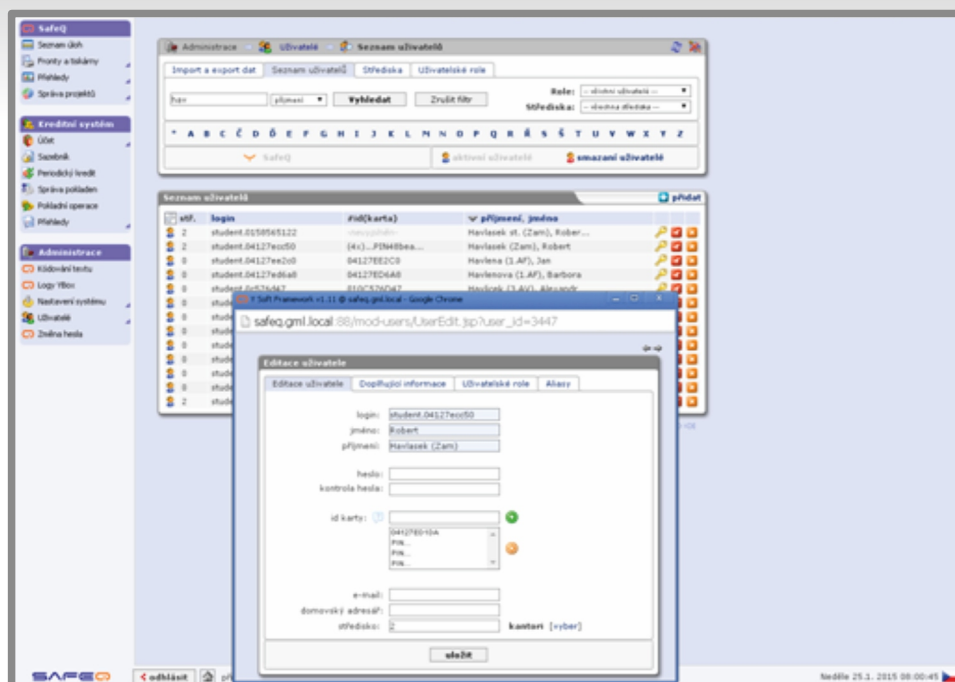
V menu Přehledy-Celkový přehled lze velmi efektivně filtrovat dle všech myslitelných parametrů:



Výsledek můžeme exportovat do .xml, .xls, .csv, nebo na obrazovku. Automatické reporty nabízejí možnost pravidelného „mailu o stavu kopírek“. Záložka Účet nabízí Historii kreditu, dál je v menu Periodicky připisovaný kredit (např. pro učitele), Pokladní operace (lze se připojit k jiné či stejné pokladně, s jakou pracuje pokladník v SafeQ Credit Chargeru), ... V Nastavení systému lze ovlivnit celou řadu parametrů, jak se SafeQ chová, nejzajímavější je pasáž s tiskovým serverem: →

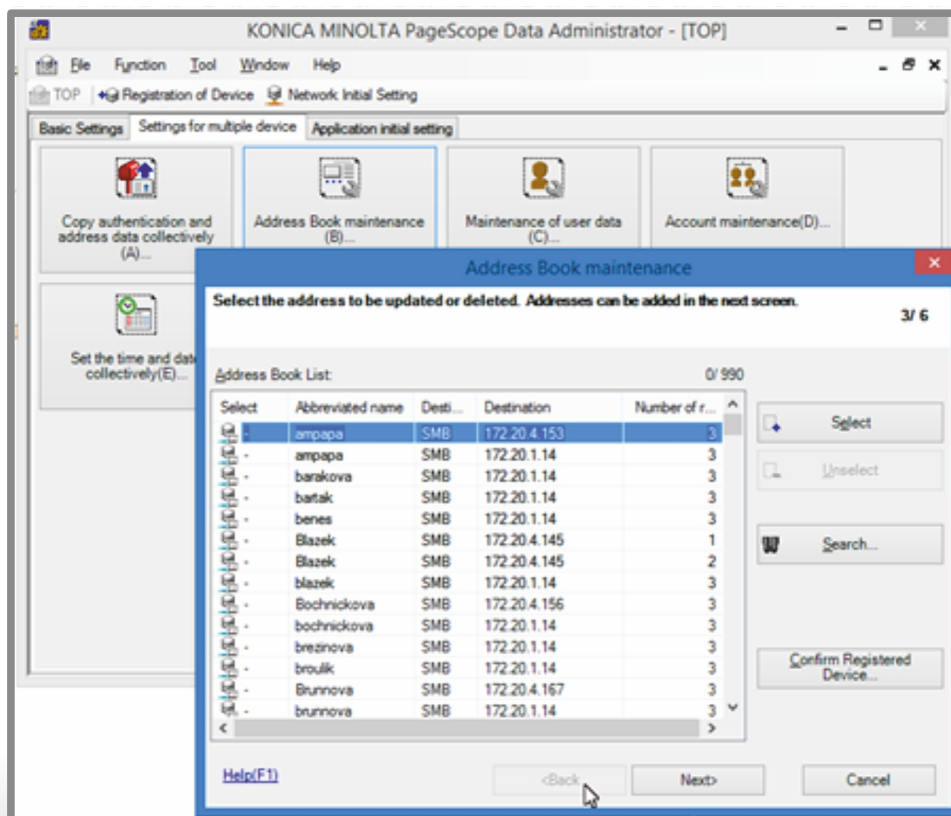


V položce Uživatelé nalezneme Seznam uživatelů, každého lze upravovat:



Správa kopírek jako zařízení

Samostatnou aplikací je Konica Minolta PageScope Data Administrator, který k Minolťáckým kopírkám umí přistupovat přímo po síti, editovat jejich nastavení, zejména AddressBook, do něhož uživatelé skenují (do sdílených adresářů, do mailu, na FTP, na WebDAV, ...)



V centrálním SafeQ5 serveru lze též nastavit možnost spolupráce s AD a skenování přímo do domovského adresáře toho uživatele, jenž je na dané kopírce v tu chvíli přihlášen.

Jinak mají kopírky samozřejmě každá svoje webové rozhraní, přes které je lze detailně nastavovat – nastavení přes web ovšem není tak efektivní, protože to implikuje nutnost kopírku na poměrně dlouhou dobu uzamknout (nepříjemné pro uživatele, který u ní zrovna stojí).

172.20.2.23

wd/a_system.xml

Administrator

Logout

Develop inco+ 220

Ready to Start

Low Paper

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Printer icons

Správa menších databází

Rezervační systém

Na doporučení jednoho z kolegů z Gymnázia Náchod jsme na GML Brno začali používat rezervační systém MRBS (<http://mrbs.sourceforge.net/>). Je free, opensource a i přes drobné výhrady jej mohu doporučit. Lze jej samozřejmě napojit na LDAP (AD), podle skupin přidávat oprávnění k jednotlivým Místnostem/Zdrojům, některé místnosti mohou být otevřené pro kohokoliv, jiné rezervovatelné pouze po schválení správcem místnosti, jiné pouze pro úzkou skupinu osob.

GML Rezervační systém		14.10.2014	Přijít na	Návod	Místnosti/Zdroje	Výpis	Hledat	Jste herešek@gml.cz
		0 čekající na schválení						Odlásk se
Oblasti		září 2014 říjen 2014 listopad 2014						
Data projekty		Po Út St Čt Pá So Ne Po Út St Čt Pá So Ne Po Út St Čt Pá So Ne						
Místnosti ostatní		1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30						
Účebny Inf		1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30						
VT - fotoaparát		1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30						
VT - kamery		1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30						
VT - notebooky		1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30						
		Úterý 14. říjen 2014						
<< Den vzad		Dnes						
		Den vpřed >>						
Hodina		5 AF 4 BF Bi Plenosty (kab. Inf) 2 A 2 B JUB Fy Fy_Lab 4 AV 6 BF Vv 2 BF Ch 3 C						
8:00-8:30		vzr						
8:30-9:00		vzr						
9:00-9:30		vzr						
9:30-10:00		vzr						
10:00-10:30		vzr						
10:30-11:00		vzr						
11:00-11:30		vzr						
11:30-12:00		vzr						
12:00-12:30		vzr						
12:30-13:00		vzr						
13:00-13:30		vzr						
13:30-14:00		vzr						
14:00-14:30		vzr						
14:30-15:00		vzr						
15:00-15:30		vzr						
15:30-16:00		vzr						
16:00-16:30		vzr						
16:30-17:00		vzr						
17:00-17:30		vzr						
17:30-18:00		vzr						
18:00-18:30		vzr						
18:30-19:00		vzr						
19:00-19:30		vzr						
19:30-20:00		vzr						
20:00-20:30		vzr						
20:30-21:00		vzr						
21:00-21:30		vzr						
21:30-22:00		vzr						
<< Den vzad		Dnes						
		Den vpřed >>						
Rozeh		Blokace						
Pronájem		Vedení						
Dny:		08. říj 09. říj 10. říj 11. říj 12. říj 13. říj 14. říj 15. říj 16. říj 17. říj 18. říj 19. říj 20. říj 21. říj						
Týdny:		15. zář 22. zář 29. zář 06. říj 13. říj 20. říj 27. říj 03. lis 10. lis						
Měsíce:		sep/2014 zář/2014 říj/2014 lis/2014 pro/2014 led/2015 úno/2015 bře/2015 dub/2015						

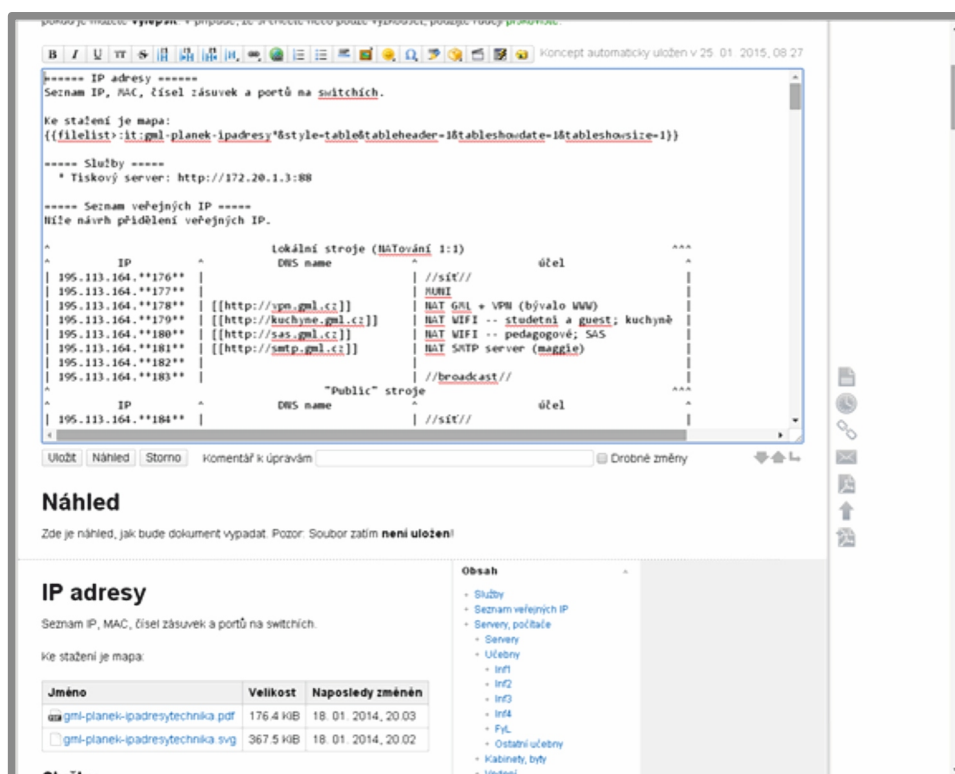
V rámci ročníkové práce nám jeden student zanalyzoval tři tabulky v databázi, kterou MRBS používá, a vyrobil konverzní PHP skript, který obdrží .xml soubor z ASCTimetables a importuje jednotlivé vyučované hodiny do MRBS. Skript není nijak složitý, jde jen o to zanalyzovat si výstup z ASCTimetables. Zájemcům mohu po dohodě poskytnout.

Školní wiki

Doporučuji pro znalostní databázi používat wikipedickou stránku. Ideálně se do ní umísťují návody, jak co zprovoznit (pro studenty i pro učitele), v neveřejné části pak poznámky pro nás administrátory, jak je kde co nastavené. Používáme (k maximální spokojenosti) DokuWiki (<https://www.dokuwiki.org>), je free, opensource.



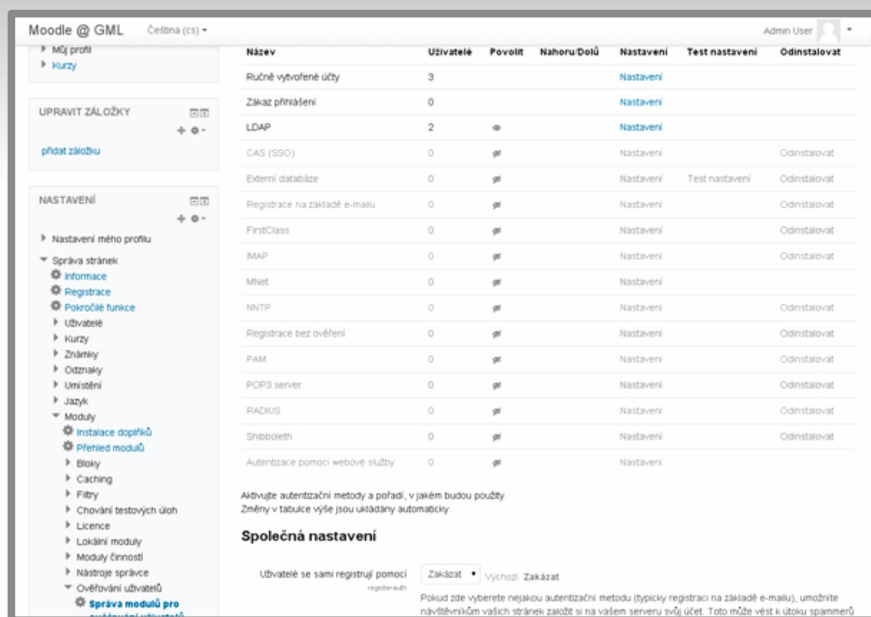
Obsahuje verzovací systém (lze dohledat staré verze dokumentů), pro úpravy stránek se používá mírně speciální syntaxe, na kterou si lze lehce zvyknout:



Mimo jiné umožňuje Dokuwiki pro úpravy použít TExovou syntaxi (přidáme-li do ní balík texlive/latex), jednotlivé stránky lze velmi hezky exportovat do .pdf, čili ji lze použít nejen jako publikační, ale i jako sázecí systém.

Moodle

Moodle určitě není „menší databáze“, jak zní nadpis kapitoly. Jde o komplexní vzdělávací systém, velký projekt, který umí velmi mnoho věcí. Integrovat lze s LDAP (AD), s GoogleApps (buď rovněž přes LDAP nebo <https://code.google.com/p/moodle-google/>) a spoustou dalších způsobů autentifikace:



Moodle obsahuje tzv. kurzy, v jejichž rámci jeden či více školitelů vede skupinu školenců, poskytují jim materiály, zadávají úkoly s konkrétním termínem ukončení, atd.

Administrace Moodle rozhraní je určitě téma na samostatné školení, z technického hlediska jde jen o to vyrobit konkrétní databázi (Postgress, MariaDB, MySQL, MSSQL, Oracle) stáhnout .zip, rozbalit, upravit soubor config.php ručně a dále postupovat pomocí průvodce na našem novém webu. V souboru config.php je v podstatě potřeba jen:

```
$CFG->dbtype = 'mysqli'; // 'pgsql', 'mariadb', 'mysqli', 'mssql', 'sqlsrv' or 'oci'
$CFG->dblibrary = 'native'; // 'native' only at the moment
$CFG->dbhost = 'localhost'; // eg 'localhost' or 'db.isp.com' or IP
$CFG->dbname = 'moodle-2014'; // database name, eg moodle
$CFG->dbuser = 'moodle-2014'; // your database username
$CFG->dbpass = 'xxx'; // your database password
$CFG->prefix = 'mdl_'; // prefix to use for all table names
$CFG->dboptions = array(
    'dbpersist' => false, // should persistent database connections be
                        // used? set to 'false' for the most stable
                        // setting, 'true' can improve performance
                        // sometimes
    'dbsocket' => false, // should connection via UNIX socket be used?
                        // if you set it to 'true' or custom path
                        // here set dbhost to 'localhost',
                        // (please note mysql is always using socket
                        // if dbhost is 'localhost' - if you need
                        // local port connection use '127.0.0.1')
    'dbport' => '', // the TCP port number to use when connecting
                        // to the server. keep empty string for the
                        // default port
);
$CFG->wwwroot = 'http://www.gml.cz/moodle-2014';
$CFG->dataroot = '/var/moodle-2014-upload';
```

Tedy: Typ databáze, jméno počítače, na němž db běží, název databáze, uživatele a heslo, které pro přístup k db použijeme. Též prefix, které jednotlivé tabulky budou mít (v případě, že člověk používá jednu databázi pro více účelů, je prefix důležitým rozlišovacím prvkem, která tabulka k čemu patří). V `dboptions` jsou pak drobnosti typu persistentního (stálého) spojení. Položku `wwwroot` je třeba korektně nastavit, aby se všechny odkazy správně generovaly. Tento text je použit též pro (bezplatnou) registraci na Moodle.org. Položka `dataroot` je místo, kam musí mít webový server možnost ukládat soubory.

Všechna ostatní nastavení se poté dějí pomocí grafického průvodce, jenž se při prvním otevření webové stránky Moodle spustí.

Doporučuji Moodle pravidelně aktualizovat, vzhledem k jeho obsáhlosti jsou poměrně v něm poměrně často nalézány bezpečnostní chyby. Též aktualizace starších dat do nové verze Moodle není vůbec jednoduchá – v této chvíli je například převod dat z verze 1.9 do aktuální 2.5 možný pouze: pomocí specializovaného nástroje (1.9->2.0), který funguje dost nešťastně, a poté 2.0->2.5 složitým postupem. Na MUNI momentálně vyvíjejí v rámci PROEFES (tým zajišťující technickou podporu Moodle na Muni) program Převodník, který umožňuje převod kurzů systému Moodle z verzí 1.x do aktuální verze.

Kuchyňská databáze

...je samostatnou složkou, finanční systém kuchyně může být provozován odděleně nebo integrován do celoškolského systému peněz (z nějž si odebírají kopírky, tisky, kuchyně či různé nepravidelné platby).

Zkušenost máme se stravovacím systémem firmy Z-Ware (<http://www.z-ware.cz/?24-stravovací-systemy>), který funguje stand-alone, pouze do něj / z něj taháme data

o uživateli. Databáze je poměrně obsáhlá a komplikovaná:

DB: kuchyne

SQL příkaz Import Export
Vytvořit tabulku

Tabulky a pohledy

Vyhledat data v tabulkách (173)

Tabulka	Úložné	Porovnání	Velikost dat	Velikost indexů	Volné místo	Auto Increment	Rádů	Komentář
2005_faktury	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
2006_pohyb	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
2006_prijemky	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
2006_pz	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
2006_vydejky	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
2006_zadanky	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
alergeny	InnoDB	utf8_general_ci	16 384	0	540 016 640	15	~ 14	
alergeny_jdlo	InnoDB	utf8_general_ci	16 384	32 768	540 016 640	347	~ 279	
alergeny_sklad	InnoDB	utf8_general_ci	16 384	32 768	540 016 640	2	~ 1	
aukce	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
bufautomat	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
bufceny	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
bufcuts	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
bufet_conf	InnoDB	utf8_general_ci	16 384	0	540 016 640	2	~ 1	
bufkarlog	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
bufobj	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
bufobjpol	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
bufpok	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
bufpokladny	InnoDB	utf8_general_ci	16 384	0	540 016 640	2	~ 1	
bufpri	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
bufpripol	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
bufsklad	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
bufskup	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
bufzasoba	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
diety	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
diety_jdlo	InnoDB	utf8_general_ci	16 384	32 768	540 016 640	1	0	
diety_poradi	InnoDB	utf8_general_ci	16 384	0	540 016 640	1	0	
dodavatel	InnoDB	utf8_general_ci	16 384	0	540 016 640	66	~ 47	

Aktuálně má náš kuchyňský systém uživatele separátně, od firmy Z-Ware je výhled na integraci s běžnými ověřovacími servery.

Rozhraní pro objednávání obědů (iCanteen) je poměrně jednoduché a přehledné:

Souhrn konkurence:

- Astris (<http://www.aktion.cz/>),
- Kredit (<http://www.anete.cz/Stravovací-system-KREDIT/>), velmi hezký a dobře prointegrovaný),
- Job Abacus (<http://www.gacc.cz/stravovací-system/>),
- VIS (<http://web.visplzen.cz/home/stravovací-system/>),
- Tetronik (<http://www.tetronik.cz/products/systems/4>) a další

Jedlíček na den 26.01.2015 - Pondělí

neleze 0 ks | 29.0 Kč | Oběd 1

neleze 1 ks | 29.0 Kč | Oběd 2

Polévka brokolicev krémová, Králičí maso na divoko, dušená rýže s mrkví, zeleninový salát.

Těstoviny s houbovým ragú / Zampiony, smetana /

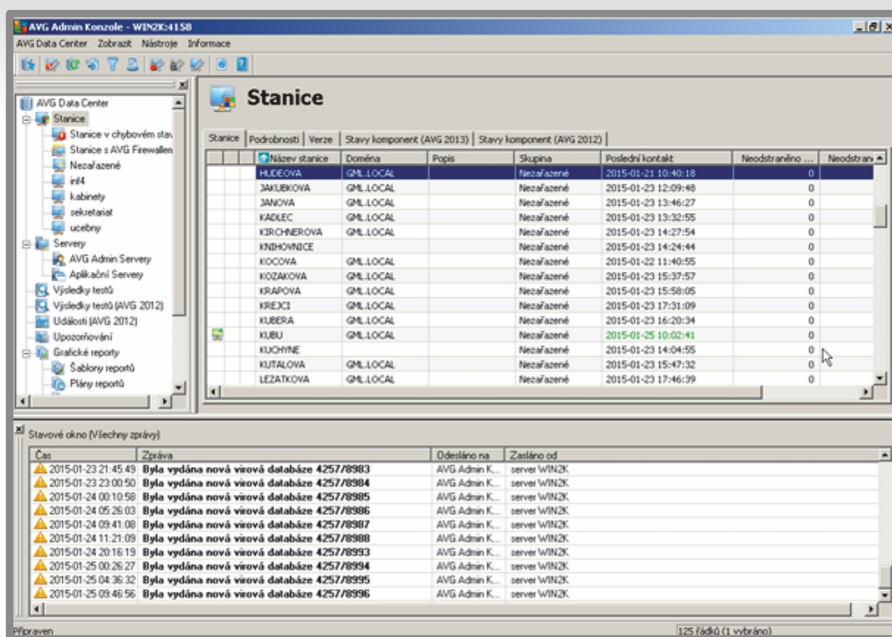
1. No vybraný den je v jídelníčku zadán 2 jídla. 2. Uvedené ceny platí pro objednání následujícího jídla.

Po	Út	St	Čt	Pá	So	Ne
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	
Únor						
						1
2	3	4	5	6	7	8

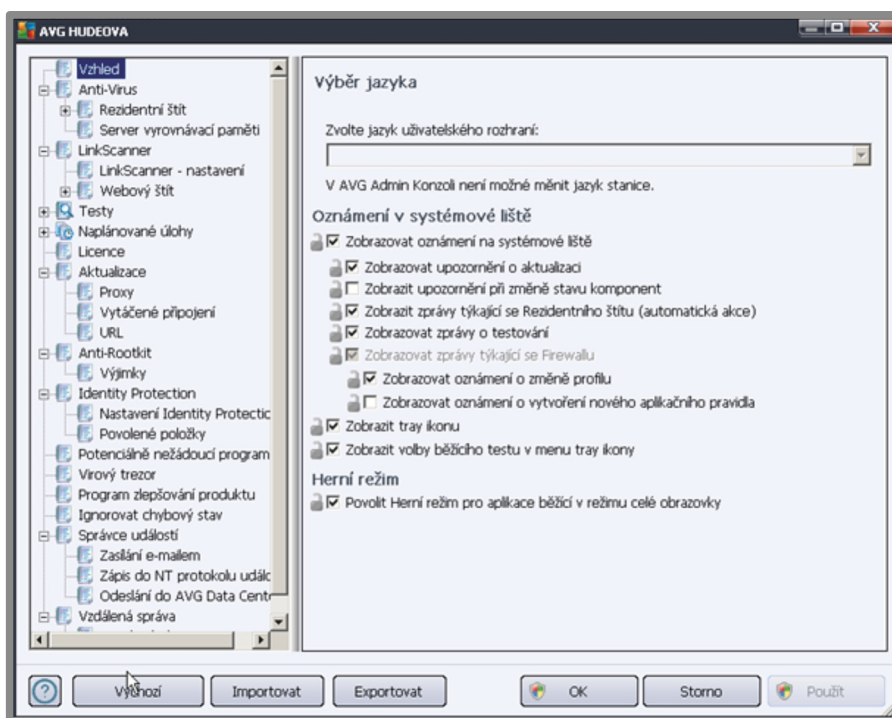
Centrální správa antiviru

Doporučit mohu centrální správu AVG, poměrně kvalitní a dobře spravovatelnou.

Jde o AVG Data Center, s rozhraním AVG Admin Konzole. Poměrně přehledná konzole umožňuje řídit celou síť vzdáleně připojených počítačů:



Počítače lze organizovat do skupin, každou skupinu i každou stanici nastavovat a řídit zvlášť. Detail nastavení stanice (nastavení více stanic v jedné skupině vypadá úplně stejně):



Ikonou zámku lze volbu vynutit (opět pro stanici, pro celou skupinu či pro celou síť).

Nastavovat lze, jak vidíte, prakticky vše: chování Rezidentního štítu, chování Link-Scanneru (chránícího uživatele brouzdajícího po internetových stránkách), Webového štítu (stahuje-li uživatel něco do počítače), druhy Testů (jen paměti, důležitých souborů, všech souborů, souborů ze zadaného adresáře, vše včetně heuristické analýzy). Naplánovanými úlohami lze jednotlivé testy a virové aktualizace spouštět v konkrétních časech. Vznikne-li nějaká událost (např. výskyt viru či dlouhodobě se nehlásící stanice), lze ve Správci událostí nastavit činnost, co se má stát.

Alternativou k AVG Data Center je centrální správa počítačů v Active Directory s nainstalovaným integrovaným antivirem Microsoft Security Essentials. Jeho výhodou je lepší prointegrovanost s MS produkty, nevýhodou pak obtížnější manipulovatelnost s výsledky (standardně jen formou Protokolu událostí v rámci MS Windows).

Virtualizace serverů

Doba, kdy se pojem server ztotožňoval s (poměrně výkonným) počítačem, je dávno pryč. V dnešní době je výhodné mít pro běžnou firmu (i pro běžnou větší školu) jeden až dva velmi kvalitní počítače, na nichž běží virtualizační nástroj a které poskytují své hardwarové prostředky (procesor, paměť, hard-disk, síťovou konektivitu...) pro jednotlivé virtuální servery, které na nich běží.

Srovnání používaných serverů

Pro server můžeme vybírat mezi VMWare Serverem (či VMWare Infrastructure) a mezi Microsoft Hyper-V (provozovaným buď samostatně nebo uvnitř Windows Serveru 2008 či 2012). Velmi těžko se oba produkty srovnávají, každý má své výhody a nevýhody. Oba jsou v běžně používané variantě zdarma. Stahujte:

- VMWare ESXi: <http://www.vmware.com/cz/products/vsphere-hypervisor>
- Hyper-V server 2008: <http://www.microsoft.com/en-us/download/details.aspx?id=3512>
- Hyper-V server 2012 (evaluační verze, bez časového limitu):
<http://www.microsoft.com/en-us/evalcenter/evaluate-hyper-v-server-2012>

Lokální verze („player“) si lze stáhnout na vlastní počítač a vyzkoušet si v něm běžný provoz (vytvoření nového virtuálního počítače, instalaci operačního systému na něm, nastavení detailů a virtuálního železa, které virtuál uvidí a bude používat). Stahujte:

- VMWare Player : https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_player/7_0
- VMWare Workstation (30-denní trial, poté placený, umí s virtuály lépe pracovat, srovnání na <http://www.vmware.com/cz/products/workstation/compare.html#table2>):
https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/11_0
- Microsoft Virtual PC (ten jsem výše nezmiňoval, jde o jednoduchou, malou aplikaci umožňující virtuální běh především starších verzí Windows):
<http://www.microsoft.com/cs-cz/download/details.aspx?id=3702>
- Oracle VM VirtualBox (mezi uživateli velmi oblíbený, stabilní, plně funkční, dostupný pro většinu operačních systémů): <https://www.virtualbox.org/>
- Pro MacOS jednoznačně Parallels (14-denní trial): <http://www.parallels.com/eu/>

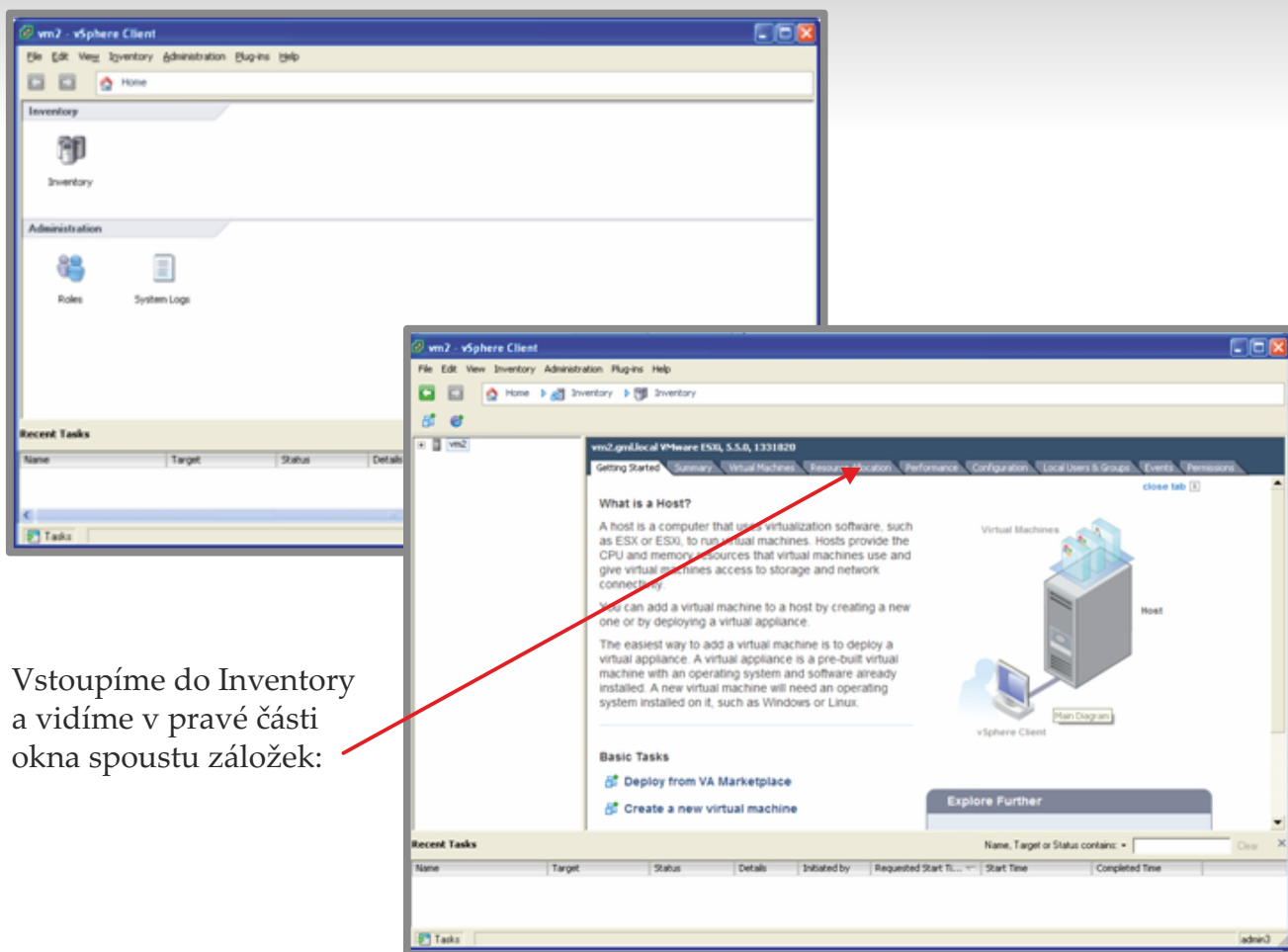
VMWare ESXi Server

Zkušenost mám v VMWare ESXi Serverem (v aktuální verzi 5.5), který zde rozeberu. Na nový „čistý“ počítač nainstalujeme VMWare ESXi Server, instalace se nejlépe provádí ze staženého CD nebo pomocí PXE ze sítě. Jde o derivát linuxu (konkrétně RedHatu).

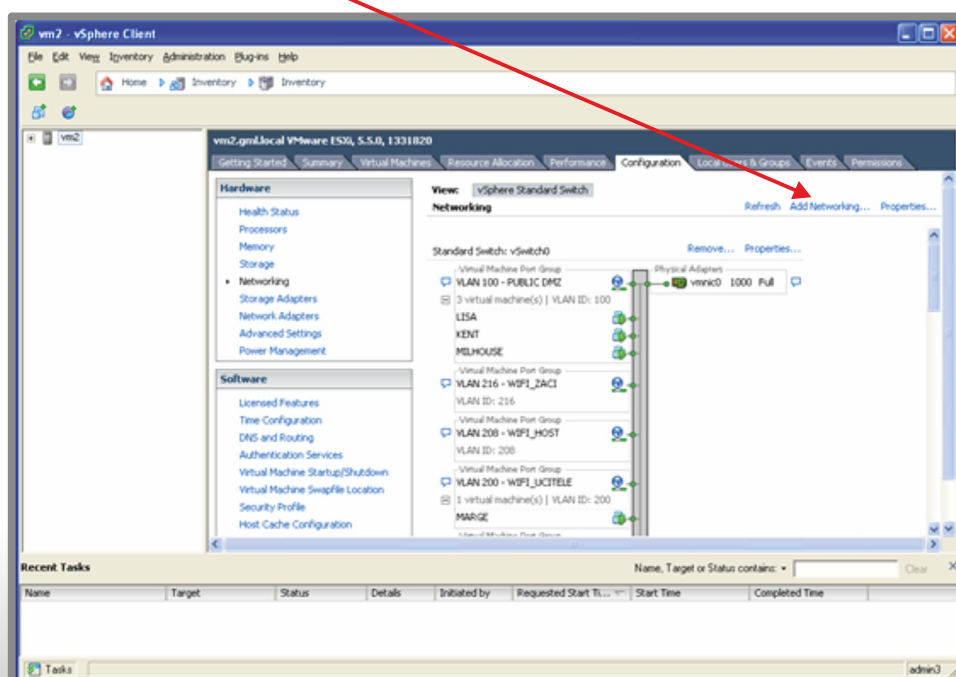
Po standardní instalaci počítač uzavřeme v serverovně a přistupujeme pouze z dálky pomocí VMWare vSphere Klienta (stáhneme např. na http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2089791). Po zalogování lokálním účtem (poprvé nainstalujeme SSL certifikát)...



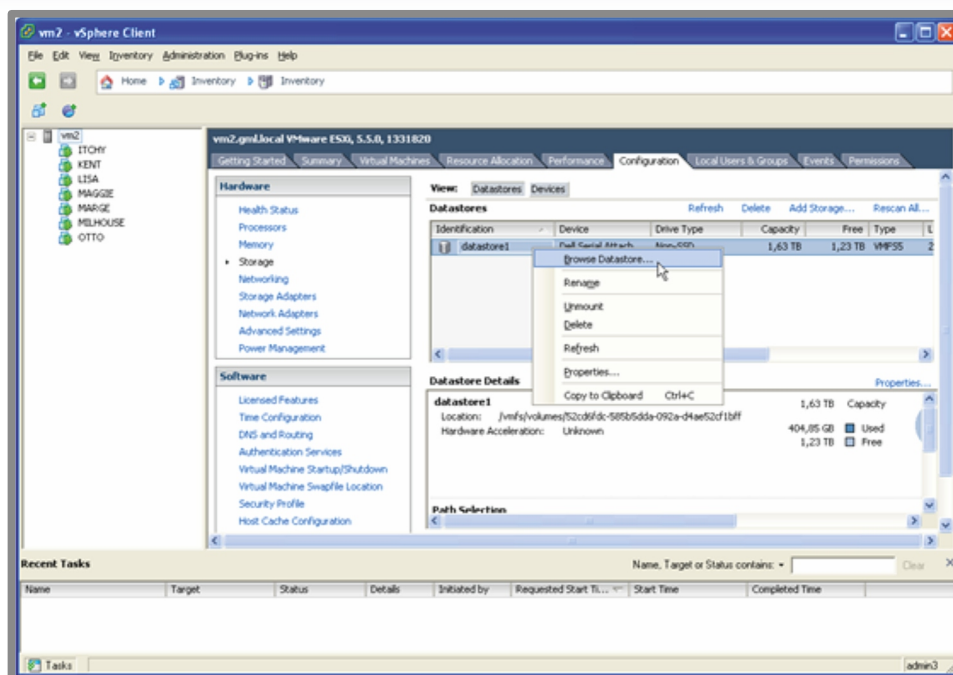
...a vidíme úvodní obrazovku:



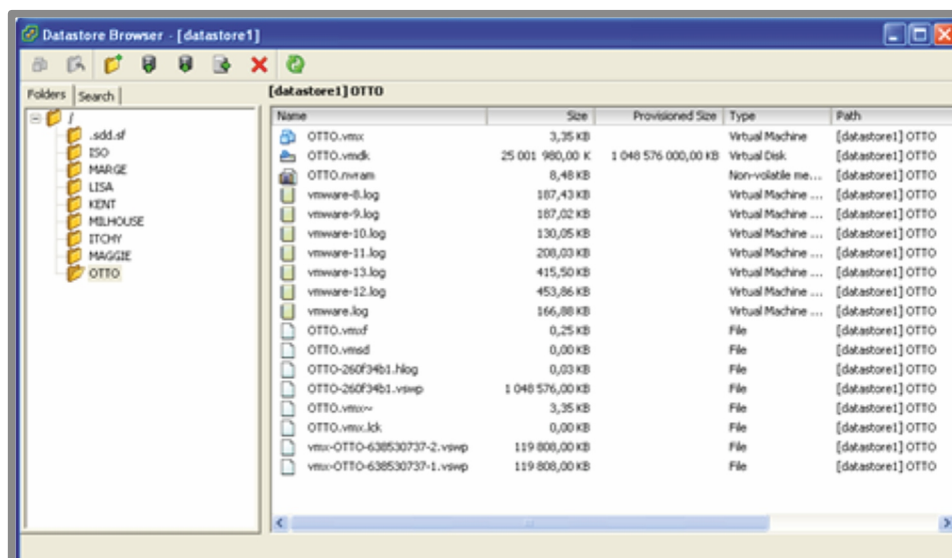
Nejprve je nutné v záložce Configuration v části Storage vytvořit si virtální síťové adaptéry (tlačítkem Add Networking), které pak budeme přidělovat jednotlivým virtuálním počítačům. Například:



Rovněž v záložce Configuration v části Storage musíme vyrobit tzv. Datastore (místo, kam se všechny virtuální disky virtuálních počítačů ukládají, vedle nich lze do Datastore také uploadnout .iso image jejich instalaček a další důležité soubory). Brouzdat uvnitř Datastore lze v samostatném okně, do něhož se dostaneme kliknutím na Browse Datastore v kontextovém menu:



Brouzdání v Datastore je intuitivní a podobá se windowsímu Průzkumníku:

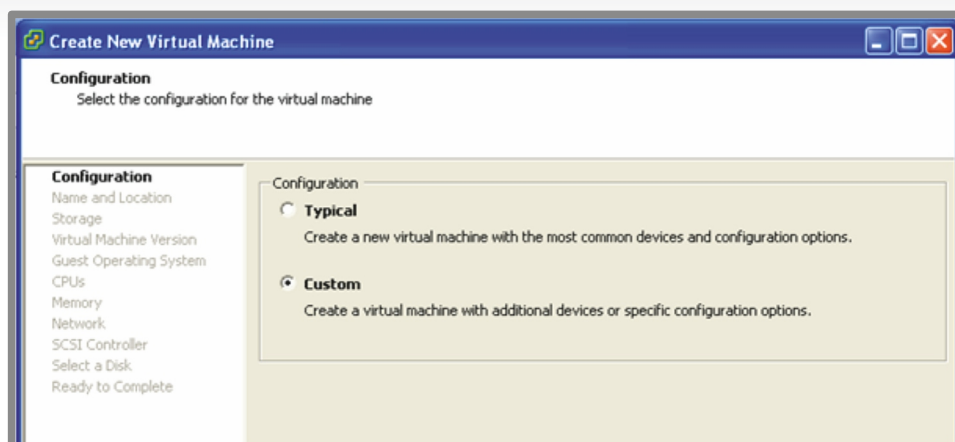


Na obrázku je Datastore s jednotlivými již nainstalovanými počítači uvnitř jejich složek (to je standardní rozdělení, které lze změnit, ale obvykle není důvod). Soubory .xmdk jsou virtuální disky, soubory .vmx jsou pak textové a obsahují popis celého virtuálu (jeho konfiguraci). Přenesením všech souborů lze virtuál odstěhovat někam jinam (do jiného Datastore, na jiný fyzický VMWare ESXi Server, do lokálního VMWare Playeru).

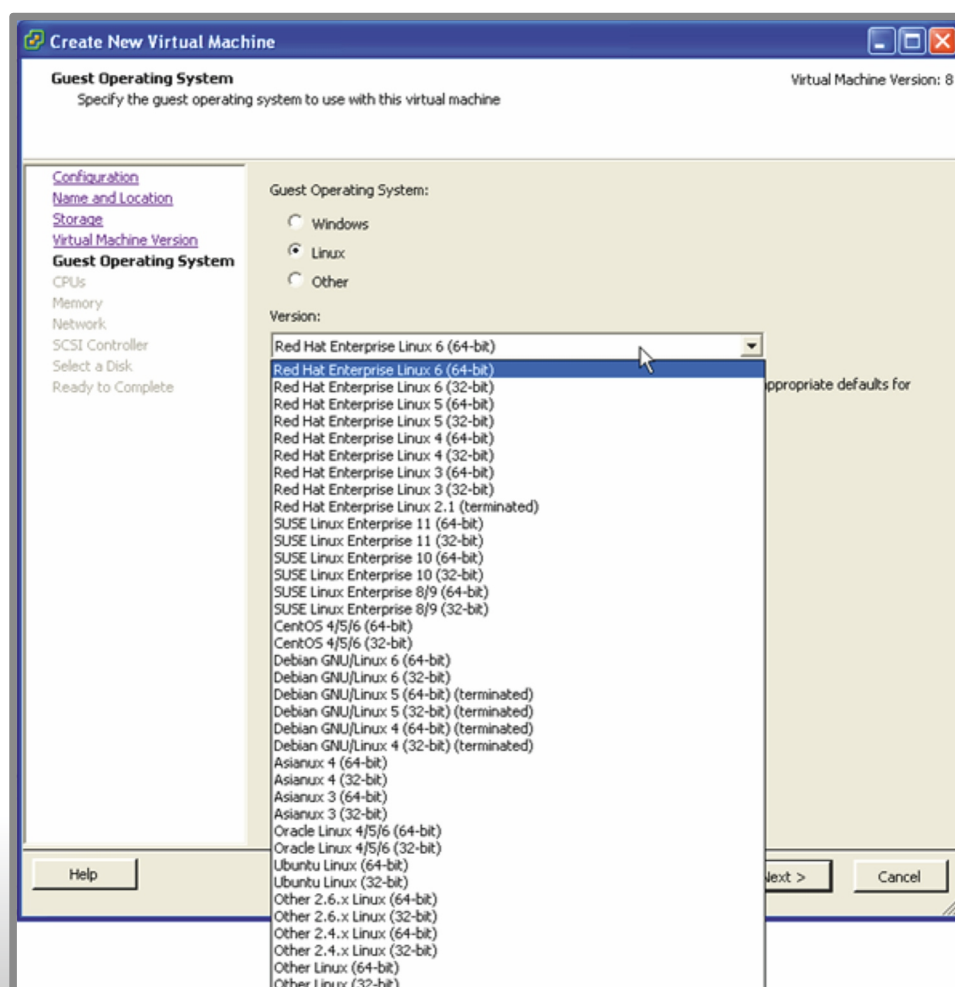
Uvnitř Datastore okna funguje drag&drop pro soubory i adresáře, ale pro přenos mezi Datastore a lokálním počítačem musíme použít ikony   v horní liště.

Výroba a nastavení nového virtuálního počítače

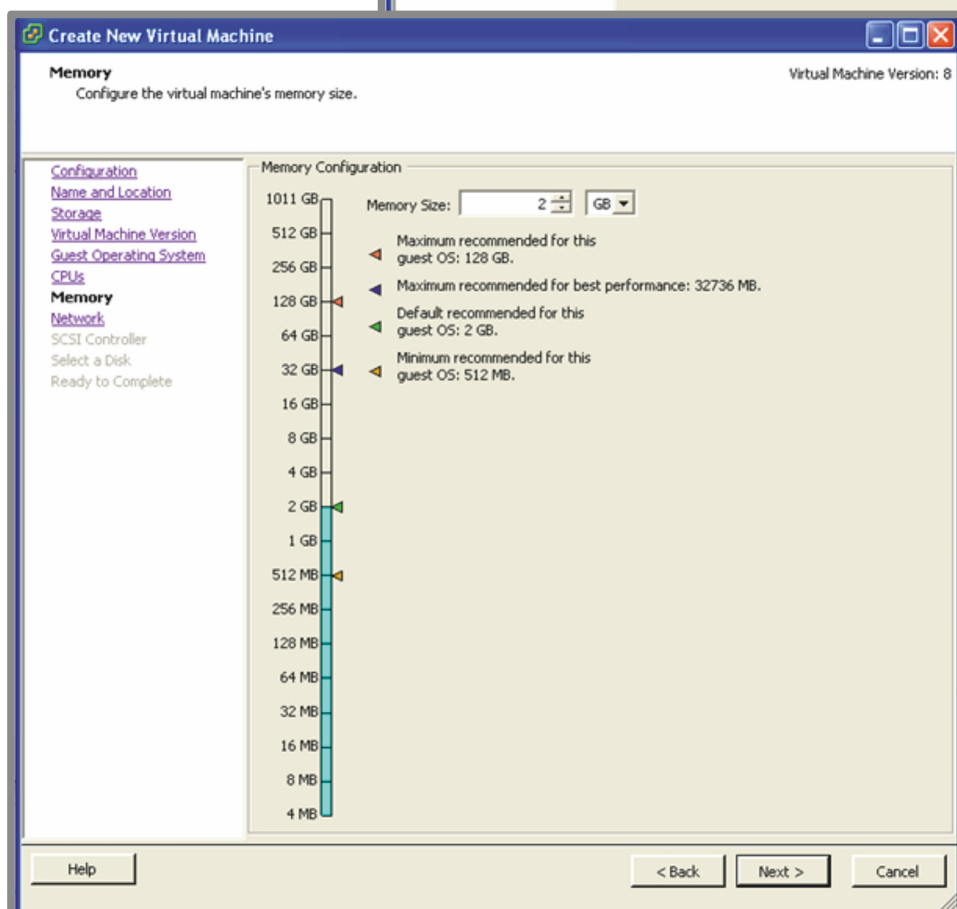
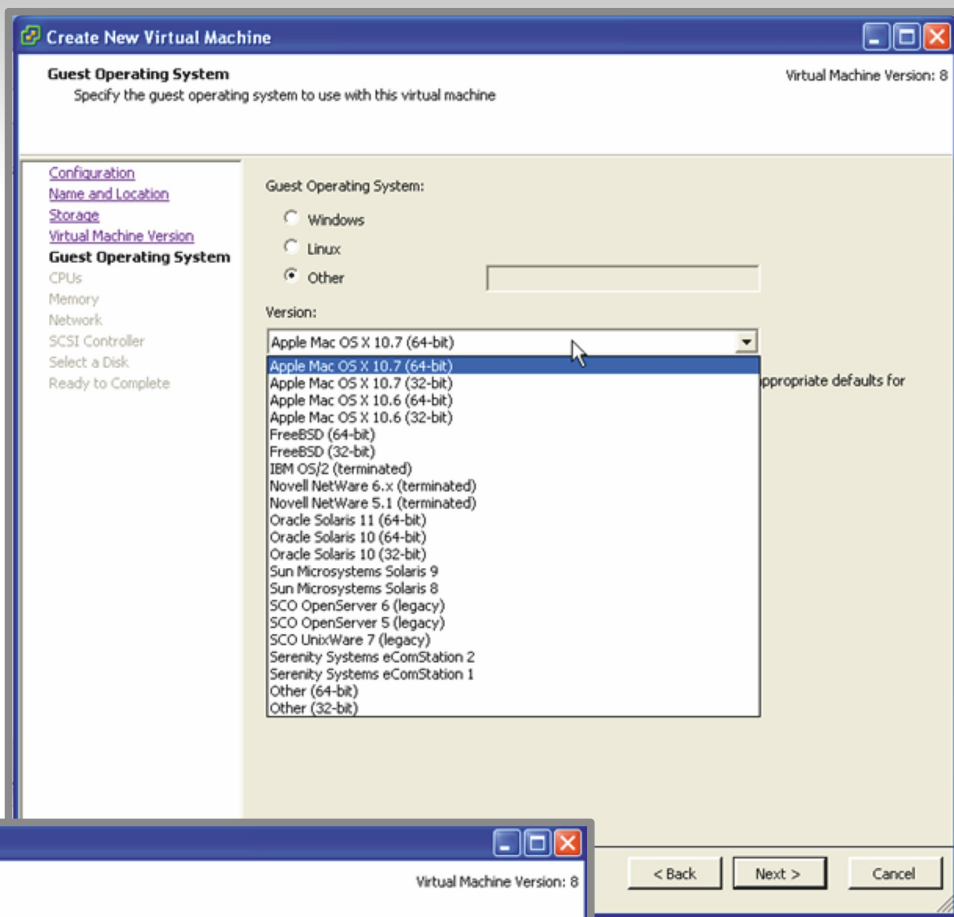
V menu vSphere Clienta zvolíme File-New-Virtual Machine. Zvolíme-li Custom, můžeme nastavit více detailů:



Vybereme jméno virtuálního počítače, pod kterým bude veden v VMWare, vybereme storage (zde asi Datastore1, jiný obvykle nemáme), vybereme verzi VMWare souboru (obvykle verze 8, starší nemá smysl). Vybereme očekávaný hostovaný operační systém – formálně vzato to není nutné, ale doporučuji vždy po pravdě WMWaru odpovědět, nastaví nám podle této odpovědi nejvhodnější konfiguraci virtuálního počítače. Pro Windows jsou k dispozici templates všechny běžné verze, počínaje MS-DOSem, přes Windows 3.1, atd., konče Windows 8 a Windows 2012, obvykle vždy v 32bitové i 64bitové verzi. Pro Linux jsou k dispozici:



Ve volbě Other
pak najdete:



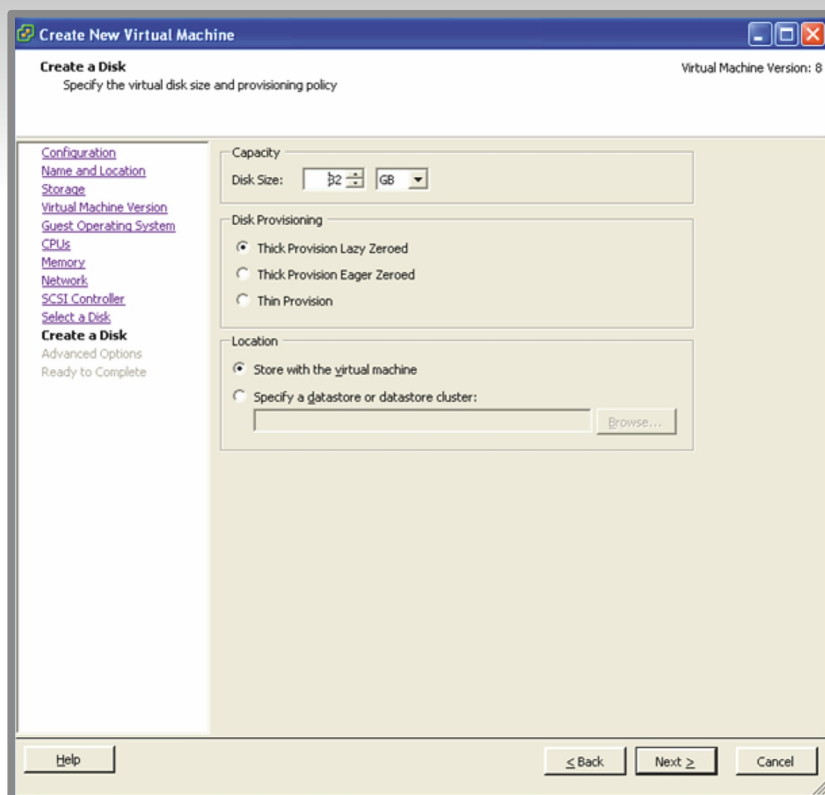
Nastavíme počet procesorů a počet jader. Nastavíme paměť– zde nám již VMWare napovídá, například pro operační systém Windows 8 navrhuje:

Nastavíme počet síťových karet a jednotlivé VLANy, v nichž jsou umístěny. Vybrat lze zde maximálně 4 síť. karty, další je ale možné přidat následně, ve Vlastnostech hotového virtuálního počítače.

Nastavíme Disk – buď nový nebo lze připojit již vytvořený disk (typicky: kopii nějakého disku jiného virtuálu).

Vyrábíme-li nový, na další stránce se nás VMWare zeptá, jak má být velký a kde má být uložen (standardně ve složce Datastore spolu s nastavením virtuálního počítače):

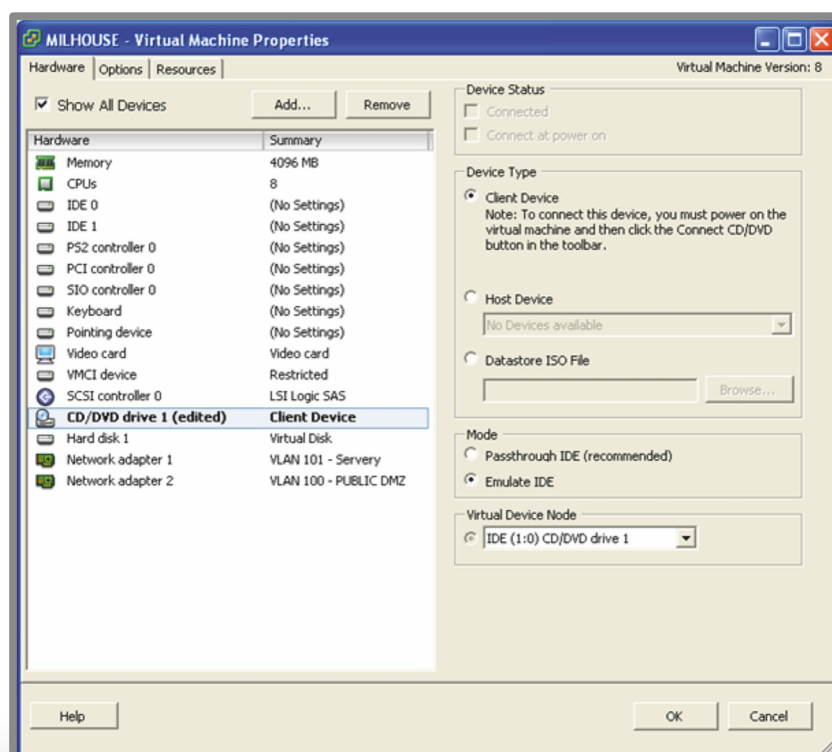
Je-li disk Thick, je mu rovnou alokováno příslušné množství gigabytů, nelze jej zmenšit. Je-li Thin, není mu alokováno nic, soubor umístěný v Datastore roste spolu se zvětšujícím se obsahem obsazeného prostoru na disku uvnitř virtuálního počítače.



Zvolíme-li v Advanced Options, že budou disky Independent, znamená to, že nebudou zahrnovány do tzv. snapshotů (záloh virtuálních počítačů, viz samostatná kapitola níže). V posledním dialogu nám VMWare nabízí editaci vlastností nově vyrobeného virtuálu.

Vlastnosti virtuálního počítače

Vlastnosti virtuálu lze upravovat kdykoliv, některé za běhu (typicky třeba připojit nový disk – chová se, jako bychom jej právě zasunuli), jiné až po jeho vypnutí. Postačí ve vSphere Clientovi na jméno virtuálu kliknout pravým tlačítkem a zvolit Edit Settings. Dialog s vlastnostmi vypadá takto:

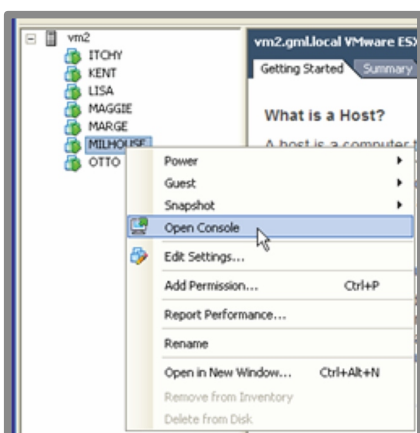
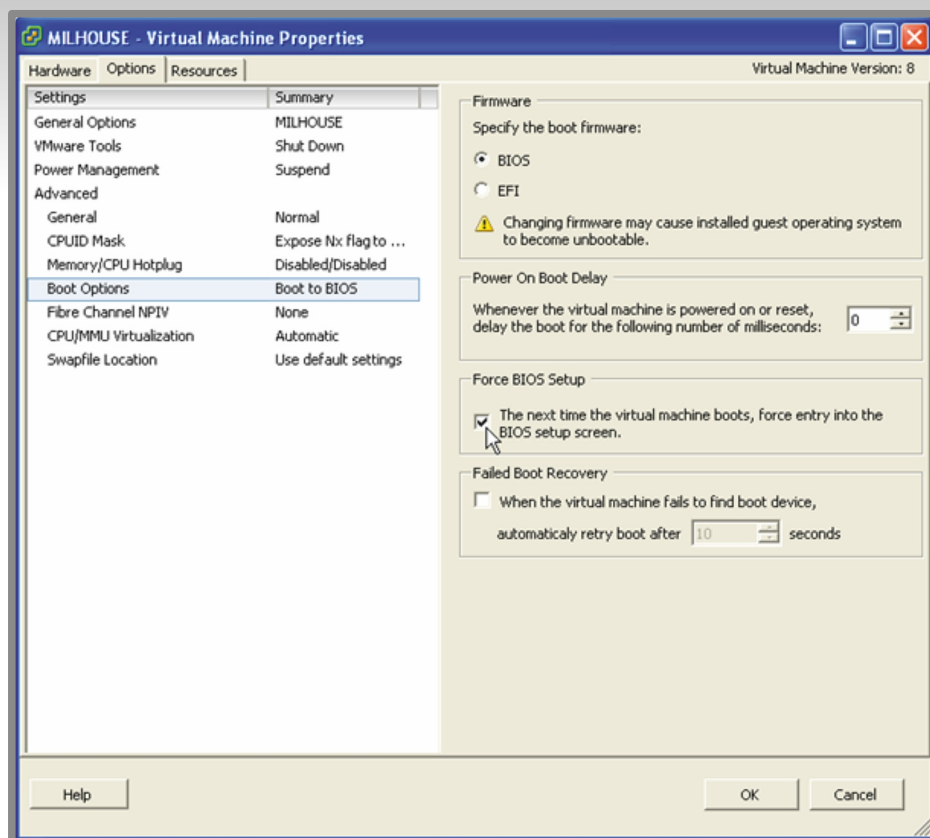


Na obrázku je nejzajímavější část nastavení, a sice virtuální CD/DVD mechanika. Tu je možné připojit přímo z klientského počítače (=mojí pracovní stanice, z níž mám spuštěn vSphere Clienta), z počítače hosta (=serveru, na němž fyzicky běží VMWare ESXi Server) nebo z .iso souboru uloženého na Datastore. Krásné, že?

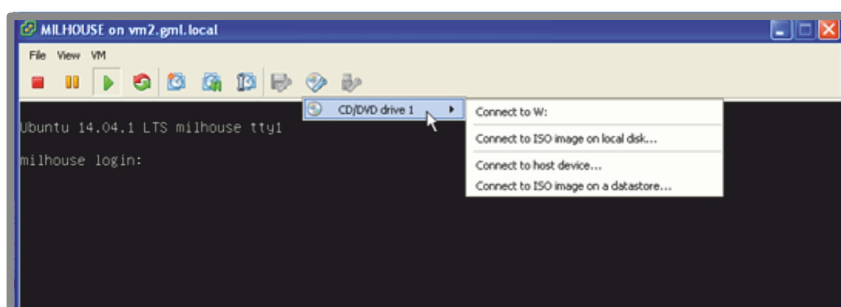
V záložce Options lze zvolit několik důležitých detailů, zejména ze v části Boot Options vybrat přímý vstup do BIOSu virtuálního počítače:

Konzole virtuálního počítače

Každému virtuálnímu počítači lze zobrazit tzv. Konzoli, kliknutím na jméno virtuálu ve vSphereClientovi a volbou Open Console z kontextového menu:



Je-li virtuál spuštěný, vidíme rovnou jeho plochu (jako bychom seděli před jeho monitorem), je-li virtuál vypnutý, vidíme černé okno. Screenshot typické konzole:



Nejzajímavější je opět připojování CD/DVD mechaniky pomocí ikony  (na obrázku).

Klikneme-li dovnitř konzole, ovládáme pak (kurzorem myši i klávesami) pouze virtuální počítač. Abychom myš/klávesnici „osvobodili“, stiskneme současně Ctrl+Alt, okno konzole převezme zpátky focus a můžeme klikat i jinam.

Snapshoty

Snapshot je termín pro zálohu celého virtuálního počítače, a to i běžícího (pouze se na dobu tvorby snapshotu uspí, lépe řečeno „vytuhne“). Uloží se stav procesoru, celá RAM paměť, všechny disky (bez těch, které jsou nastaveny jako Independent). Disky jsou uloženy inkrementální zálohou vzhledem k předchozímu snapshotu, což je příjemné, obvykle snapshoty nezabírají tolik místa.

Snapshot není klasická záloha (i když obsahuje data a nastavení), doporučuje se samozřejmě dělat zálohu i jinými klasickými cestami.

VMWare ve free verzi neumožňuje online snapshot (bez chvilkového uspání virtuálu, který snapshotujeme), jednou z výhod Hyper-V je, že ta podobnou věc umí...

Snapshotovat můžeme i speciální aplikaci, která k VMWare přistupuje přes :22 (ssh protokolem). Dobrou zkušenost mám s aplikací bazaarvcb (<http://www.magiksys.net/bazaarvcb/>). Snapshot umí vyrobit buď do zadaného adresáře v datastore1 nebo do nějakého lokálního adresáře (na stroj, z nějž byl bazaarvcb spuštěn).

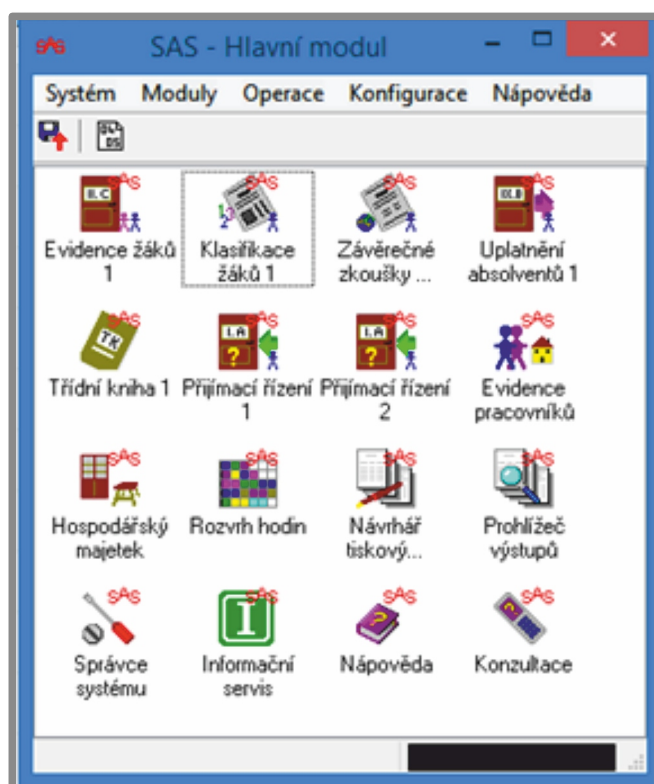
Obecně platí, že VMWare lze ovládat i přes ssh (je-li na něm port :22 otevřen pro komunikaci) a veškeré operace dělat pomocí příkazů textové konzole. Např. příkaz pro snapshotování má syntaxi `vim-cmd vmsvc/snapshot.create [VmId] [snapshotName] [description] [includeMemory] [quiesced]`

Databáze pro vedení školní agendy

Toto téma se netýká úplně správy sítě, takže jen telegraficky. Nejpoužívanějšími programy pro školní administrativu jsou SAS (Systém Agend Školy) a Bakaláři.

SAS

SAS je původně aplikace psaná v Delphi, dnes uzavřený systém obsahující několik samostatně spouštěných modulů (aplikací):



De facto je SAS pouze .exe aplikace přistupující k Firebird databázi (od roku 2000 se lokální databáze Interbase přistupovaná z Delphi pomocí ODBC změnila na vzdálenou Firebird databázi; no, a to byla od té doby prakticky jediná modernizace celého SASu). Stále jde pouze o .exe soubory, spolupráce s online světem (exporty na web a přístupy k databázi pomocí http) sice existuje, ale je velmi omezená.

Účty jsou v SASu lokální (nelze je s ničím prointegrovat), samostatně lokálně jsou pak řešeny účty pro přístup z webu pomocí http.

Aktualizace SASu se děje formou administrátorova stažení souboru .zip a rozbalení do příslušného adresáře. Je tedy účelné mít jednu instalaci SASu na síťovém disku. Je poměrně komplikované nastavit síťovému disku správně práva, většinou to administrátor (po metodě pokus-omyl a neustálých konzultacích se supportem) vzdá a nastaví read-write pro celý adresář SAS celé skupině třídních...

Bakaláři

Přímou konkurencí je systém Bakaláři, který v jednotlivých svých modulech nabízí evidenci žáků, klasifikaci (žakovskou knížku, která jediná je formou webové aplikace), rozvrh hodin+suplování, třídní knihu, přijímací zkoušky, atd.

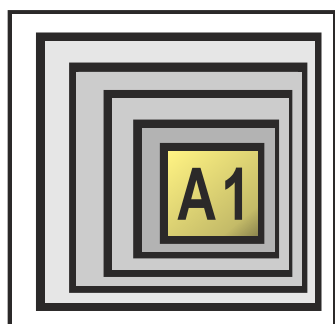
Ostatní zajímavé webové aplikace

- <http://www.edookit.cz/>
... poměrně mladý systém, vypadá nadějně
- <http://edupage.org/>
... dobrá provázanost s ASCTimetables, který je hojně rozšířen coby (velmi kvalitní) rozvrhový program

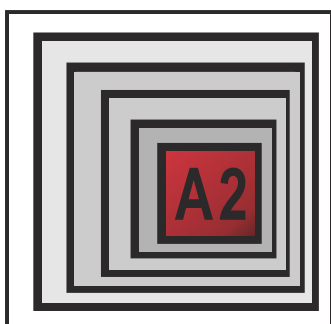
Žádný další komplexní program pro vedení školní agendy mi není znám. Poměrně hodně softwarů obsahuje dílčí části (zejména ty krásné, webové, tedy třídní knihu, absence, žakovskou knížku, ...), ale do školní byrokracie, v níž by byl tak potřebný nový, svěží vítr, se žádné firmě nechce...



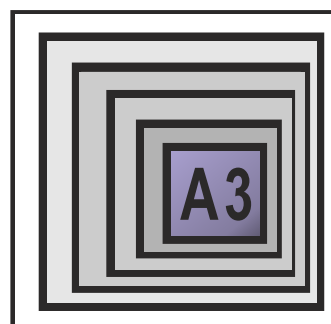
Kantor Ideál



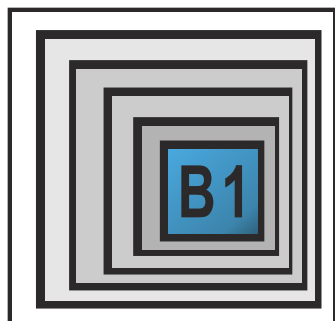
VZDĚLÁVÁNÍ ŘEDITELŮ



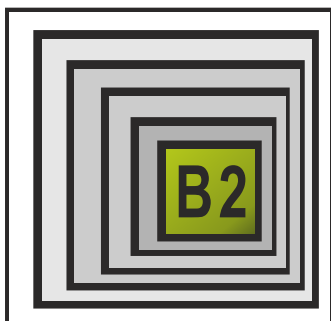
MENTORING



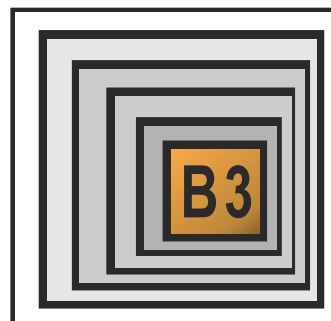
METODIK ICT VE ŠKOLE



CO UŽ MÁME



CO CHCEME



OBOROVÉ DIDAKTIKY