

RADIUS server - riadenie prístupu klientov do WiFi siete

Prístup do WiFi siete pomocou zdieľaného kľúča je trochu nepraktický, ak potrebujeme povoliť prístup klientov do WiFi siete, a naopak ak potrebujeme prístup zakázať. Problém sa rozrastie, ak máme v LAN viac AP (Access Point), pretože je potrebné konfigurovať každý AP zvlášť a ak požadujeme aj nejaký stupeň bezpečnosti, potom RADIUS server je ideálnym riešením. Neplánujem vysvetľovať ako RADIUS funguje, nakoniec to nájdete na mnoho iných stránkach, ako napríklad:

[RADIUS - Wikipedie](#)

[Radius autentifikácia \(Radius server\)](#)

[Protokol RADIUS](#)

Skôr by som sa zameral na to, aký hardvér postačí na takýto server, ako nainštalovať RADIUS, konfiguráciu RADIUS servera a klientov. Hardvér som zvolil taký, pre ktorý by sa dnes už asi nenašlo iné využitie. RADIUS server som nainštaloval na HP Brio.

1. Hardvér

HP Brio - parametre

CPU: Intel Celeron (Mendocino) 467MHz

RAM: 192MB

HDD: 8GB ST38421A

CD-ROM

USB 1.1

Sieť. karta: 3Com Corporation 3C905C-TX/TX-M [Tornado] (rev 6c)

2. Softvér

Po niekoľkých neúspešných pokusoch s FreeRadius na Debiane a Ubuntu kvôli problému s právami pre šifrovaný SSL protokol, môže byť FreeRadius šírený len vo forme zdrojových kódov, z ktorých som sa pokúsil skompilovať binárny FreeRadius avšak neúspešne, zvolil som ako základ RADIUS servera jednoduchý, ale výkonný systém **ZeroShell**, ktorý podľa popisu spĺňa všetky moje požiadavky na RADIUS server a tou najpodstatnejšou je schopnosť šifrovania PEAP MS CHAP V2.

Minimálne požiadavky na hardvér:

CPU: Pentium 233 MHz

RAM: 96MB

HDD: min. 1,5 GB (podporované sú všetky typy IDE, SATA, SCSI, USB disky)

USB, CDROM (USB nie je podmienkou, ale inštalácia je jednoduchšia)

Grafika: VGA

Sieť. karta: všetky PCI, USB, PCMCIA podporované linuxovým jadrom (napr. 3Com, Realtek, NE)



2. Inštalácia

Zo stránky [ZeroShell-1.0.beta16.iso](#) si stiahneme ISO obraz CD a

[ZeroShell-1.0.beta16-CompactFlash-IDE-USB-SATA-1GB.img.gz](#) komprimovaný obraz disku. ISO obraz CD je potrebné napáliť na CD a získame bootovateľné CD, z ktorého je možné spustiť Live distribúciu ZeroShell. Ešte potrebujeme nainštalovať ZeroShell na disk počítača. Stiahnutý obraz disku

ZeroShell-1.0.beta16-CompactFlash-IDE-USB-SATA-1GB.img.gz, ktorý má 164 MB skopírujeme na USB kľúč.

- nabootojeme Live CD Zeroshell
- po nabootovaní, na obrazovke vyberieme klávesou: **s** prístup do príkazového riadku

```

-----
Z e r o S h e l l - Net Services  1.0.beta14           March 21, 2011 - 18:57
-----
Hostname : radius.gljs.sk
CPU (1)  : Celeron (Mendocino)  467MHz
Kernel   : 2.6.25.20
Memory   : 189596 kB
Uptime   : 0 days, 0:3           User      : admin
Load     : 0.30 0.21 0.09       Password  : zeroshell
Profile  : gljs
-----

COMMAND MENU
<A> Activate Profile           <P> Change admin password
<D> Deactivate Profile        <T> Show Routing Table
<S> Shell Prompt              <F> Show Firewall Rules
<R> Reboot                    <N> Show Network Interface
<H> Shutdown                  <Z> Fail-Safe Mode
<B> Create a Bridge           <I> IP Manager
<W> WiFi Manager

                                     Select: █

```

Type exit or Ctrl+D to return to main menu.

```
root@radius root> █
```

- zasunieme USB disk
- primountujeme USB príkazom: **mount /dev/sda1 /mpoint**
- prepne sa do adresára mpoint príkazom: **cd /mpoint**
- rozbalime komprimovaný obraz disku a skopírujeme ho na disk príkazom:
gunzip -c ZeroShell-1.0.beta16-CompactFlash-IDE-USB-SATA-1GB.img.gz > /dev/hda
 Čakajte, pokiaľ sa znova neobjaví príkazový riadok, kopírovanie môže trvať aj niekoľko minút, až desiatok minút, v závislosti od rýchlosti diskov a USB.
 (Ak kopírovanie neperebehne korektne, môžete ešte použiť metódu, ktorú som použil aj ja. Najprv som gunzipom rozbalil obraz disku priamo na USB kľúči, ale USB musí mať min 1,5 GB, a potom príkazom dd if=obraz.img of=/dev/hda skopírovať obraz na pevný disk)
- prepne sa do koreňového adresára príkazom: **cd /**
- odmountujeme USB príkazom: **umount /mpoint**
- vytiahneme USB
- musíme nakonfigurovať príznak bootovania pre 1. partition príkazom: **fdisk /dev/hda**
- Na obrazovke uvidíte: **Command (m for help):**
- teraz stlačíme klávesu: **p** a uvidíme takýto výpis:

```
root@radius root> fdisk /dev/hda
```

```
The number of cylinders for this disk is set to 8460.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)
```

```
Command (m for help): p
```

```
Disk /dev/hda: 8455 MB, 8455200768 bytes
32 heads, 61 sectors/track, 8460 cylinders
Units = cylinders of 1952 * 512 = 999424 bytes
```

Device	Boot	Start	End	Blocks	Id	System
/dev/hda1		1	14	13633+	83	Linux
/dev/hda2		15	175	157136	83	Linux
/dev/hda3		176	1015	819840	83	Linux
/dev/hda4		1016	8460	7266320	83	Linux

```
Command (m for help): █
```

- teraz stlačíme klávesu: **a**, a objaví sa dotaz:

Partition number (1-4): stlačíme klávesu **1**, pretože systém bude bootovať z 1. partition

```
root@radius root> fdisk /dev/hda
```

```
The number of cylinders for this disk is set to 8460.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)
```

```
Command (m for help): p
```

```
Disk /dev/hda: 8455 MB, 8455200768 bytes
32 heads, 61 sectors/track, 8460 cylinders
Units = cylinders of 1952 * 512 = 999424 bytes
```

Device	Boot	Start	End	Blocks	Id	System
/dev/hda1		1	14	13633+	83	Linux
/dev/hda2		15	175	157136	83	Linux
/dev/hda3		176	1015	819840	83	Linux
/dev/hda4		1016	8460	7266320	83	Linux

```
Command (m for help): a
```

```
Partition number (1-4): 1█
```

- skontrolujeme klávesou: **p** a mali by sme dostať nasledovný výpis:

```

root@radius root> fdisk /dev/hda

The number of cylinders for this disk is set to 8460.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)

Command (m for help): p

Disk /dev/hda: 8455 MB, 8455200768 bytes
32 heads, 61 sectors/track, 8460 cylinders
Units = cylinders of 1952 * 512 = 999424 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/hda1  *           1           14       13633+   83  Linux
/dev/hda2             15          175       157136   83  Linux
/dev/hda3            176         1015       819840   83  Linux
/dev/hda4           1016         8460      7266320   83  Linux

Command (m for help): █

```

Rozdiel je len v znaku * pri partition **/dev/hda1**, ale teraz už máme nastavený príznak bootovania z 1. partition správne

- zapíšeme nastavenie klávesou: **w**
- opustíme príkazový riadok kombináciou kláves: **Ctrl+d**
- reštartujeme ZeroShell klávesou: **r** a potvrdíme klávesou: **y**, počas reštartu vyberieme z mechaniky CD a ZeroShell by mal nabootovať z pevného disku. Týmto je inštalácia ukončená, teraz treba server nakonfigurovať.

```

WARNING: if you continue the system will be restarted.
Are you sure you want to continue (y/n)? █

```

4. Konfigurácia siete v ZeroShell

Ako prvé, je potrebné nakonfigurovať IP adresu, aby sme ďalšie nastavenia mohli urobiť cez webové rozhranie ZeroShell-u.

- Po nabootovaní, v základnej obrazovke stlačíme klávesu: **i** IP manager a vstúpime do sekcie konfigurácie IP adresies.

```

-----
ETH00 - 3Com Corporation 3c905C-TX/TX-M [Tornado] (rev 6c)
      Status: 10Mb/s Half Duplex
      (1) 192.168.1.4 / 255.255.255.0 (up)
-----
                                     Default Gateway: 192.168.1.1
COMMANDS
  <A> Add IP address           <D> Delete IP address
  <M> Modify IP address       <G> Set Default Gateway
  <S> Change Interface status <H> Dynamic IP configuration
  <I> Show Info               <Q> Quit
>> █

```

- Stlačíme klávesu: **m** Modify IP address
- Keď sa objaví výpis

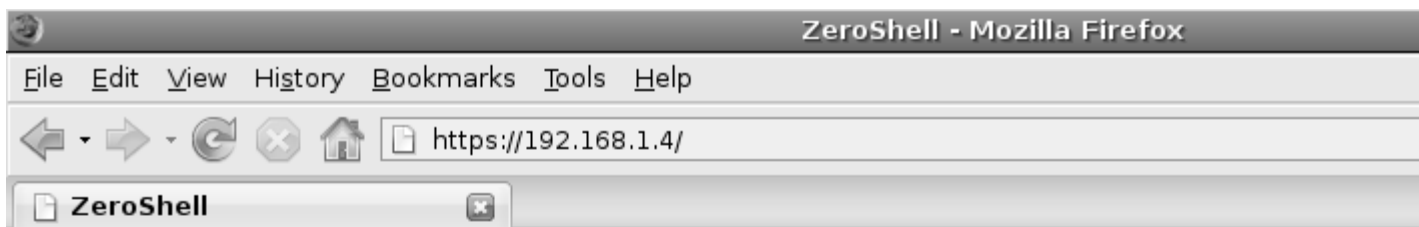
Interface [ETH00]: stlačíme **Enter** (Ak máte v systéme viac sieť. rozhraní a chcete konfigurovať IP adresu pre ďalšiu sieť. kartu, potom najprv zadajte označenie rozhrania napr. ETH01 a až potom Enter)

```
-----  
ETH00 - 3Com Corporation 3c905C-TX/TX-M [Tornado] (rev 6c)  
Status: 10Mb/s Half Duplex  
(1) 192.168.1.4 / 255.255.255.0 (up)  
-----  
Default Gateway: 192.168.1.1  
COMMANDS  
<A> Add IP address          <D> Delete IP address  
<M> Modify IP address      <G> Set Default Gateway  
<S> Change Interface status <H> Dynamic IP configuration  
<I> Show Info              <Q> Quit  
>> m  
  
Interface [ETH00]:  
-----  
ETH00 - 3Com Corporation 3c905C-TX/TX-M [Tornado] (rev 6c)  
Status: 10Mb/s Half Duplex  
(1) 192.168.1.4 / 255.255.255.0 (up)  
-----  
IP to modify [1]: 192.168.0.10█
```

- Teraz môžete zadať IP adresu, ktorú bude mať Váš RADIUS server a potom aj sieťovú masku.

Ja som si nastavil IP adresu na: **192.168.1.4** a táto IP je použitá vo všetkých nasledovných príkladoch

- Ostatné nastavenia už urobíme cez web rozhranie ZeroShellu, nasmerujeme prehliadač na IP adresu ktorú sme nastavili v predchádzajúcom kroku
https://192.168.1.4
- Potvrdíme prijatie certifikátu
- Prihlásime sa do webového rozhrania, meno: **admin** heslo: **zeroshell**



ZEROSHELL

Net Services

Username

Password

Done

- Po prihlásení, môžeme skontrolovať a upraviť IP adresu ZeroShell servera nasledovne vľavo **Setup** hore **Network** vyberieme IP adresu, ktorú chceme zmeniť, vpravo **Edit IP**

ZS:192.168.1.4 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://192.168.1.4/

ZS:192.168.1.4

ZEROSHELL
Net Services

Release 1.0.beta14
[About](#)

[Logout](#) [Reboot](#) [Shutdown](#)

SETUP **AutoUpdate** Profiles Network Time https

Show ALL

<input type="radio"/> ETH00	10Mb/s Half Duplex 3Com Corporation 3c905C-TX/TX-M [Tornado] (rev 6c)	UP
<input checked="" type="radio"/>	192.168.1.4	255.255.255.0

https://192.168.1.4 - IP Configuration - Moz

IP Configuration (ETH00) VLAN Native

IP

Netmask

Done 192.168.1.4

<input type="radio"/> VPN99	Connection Host-to-LAN OpenVPN In
<input type="radio"/>	192.168.250.254

Mar 19 12:42:09 SUCCESS: System successfully started with Linux kernel 2.6.25.20 and ZeroShell 1.0.beta14
Mar 19 13:09:51 SUCCESS: Session opened from host 192.168.1.2 (Admin)

Done

- Nastavíme predvolenú bránu, hore **GATEWAY**

Release 1.0.beta14
About

Logout Reboot Shutdown

SETUP AutoUpdate Profiles Network Time https

Show ALL GATEWAY New VPN New BRIDGE New BOND New PPPoE

Default Gateway 192.168.1.1

OK Cancel

Done 192.168.1.4

VPN99	Connections from Road Warrior clients not accepted	
	Host-to-LAN OpenVPN Interface	
	192.168.250.254	255.255.255.0

Mar 19 21:33,27 SUCCESS: System successfully started with Linux kernel 2.6.25.20 and ZeroShell 1.0.beta14
Mar 19 21:42,36 SUCCESS: Session opened from host 192.168.1.2 (Admin)

Done

- Nastavíme meno nášho servera, vľavo **Hosts**, označíme meno, ktoré tam už je **zeroshell** a hore klikneme na **Delete**



- Potom **Add** vyplníme polia a klikneme na **Submit**

Browser window: ZS:192.168.1.4 - Mozilla Firefox

Address bar: https://192.168.1.4/

Page Title: ZS:192.168.1.4

Release 1.0.beta14
[About](#)

ZEROSHELL
 Net Services

[Logout](#) [Reboot](#) [Shutdown](#)

HOSTS	List	View	Add	Edit	Delete
radius.gljs.sk					
Hostname	<input type="text" value="radius"/>				
Domain	<input type="text" value="gljs.sk"/>				
Description	<input type="text" value="RADIUS ZeroShell server"/>				
Administrator's E-Mail	<input type="text" value="servis@gljs.sk"/>				
Kerberos 5 Authentication	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled				

SYSTEM
 • Setup
 • Logs
 • Utilities
USERS
 • Users
 • Groups
 • LDAP / NIS
 • RADIUS
 • Captive Portal
NETWORK
 • Hosts
 • Router
 • DNS
 • DHCP
 • VPN
 • QoS
 • Wireless
 • Net Balancer
SECURITY
 • Kerberos 5
 • Firewall
 • X.509 CA
 • HTTP Proxy

Mar 19 12:42,09 SUCCESS: System successfully started with Linux kernel 2.6.25.20 and ZeroShell 1.0.beta14
 Mar 19 13:09,51 SUCCESS: Session opened from host 192.168.1.2 (Admin)

Done

- Tieto základné nastavenia musíme uložiť, inak by sme ich museli robiť pri každom reštarte ZerosShell servera. Prepne sa hore do sekcie **Profiles** a klikneme na partition, na ktorej bude uložený náš profil, v našom prípade na **sda3**

ZS:192.168.1.4 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://192.168.1.4/

RADIUS server ZS:192.168.1.4

Release 1.0.beta14
About

ZEROSHELL
Net Services

Logout Reboot Shutdown

SETUP AutoUpdate Profiles Network Time https

Partition: sda3 Create Profile Restore Profile View FS Delete Fo

Warning:
This software is NOT guaranteed to be bug free. It is your responsibility to properly test production devices with important data. In any case, the author is not responsible for a software.

Model: ATA SAMSUNG HD080HJ (sda)		
sda3 Profiles	Type: ext3	Capacity: 788 MB
	Profile	Description
	_DB.002	Profil
sda4	Type: ext2	Capacity: 72 GB
	Profile	Description
	_DB.001	Profil

Mar 23 19:47,46 SUCCESS: System successfully started with Linux kernel 2.6.25.20 and ZeroShell 1.0.beta14
Mar 23 19:48,54 SUCCESS: Session opened from host 192.168.1.2 (Admin)

Done


- Klikneme na **Create Profile** vyplníme polia, v položke **Description** pomenujeme profil, nezbudneme vyplniť polia **Admin password** a **Confirm password**, toto je heslo a potvrdenie hesla pre vstup do webového rozhrania ZerloShellu. a takisto vyplníme aj predvolenú bránu **Default gateway**
Ak je všetko potrebné vyplnené, stlačíme **Create**

The screenshot shows the ZeroShell web interface in a Mozilla Firefox browser window. The main page is titled 'ZEROSHELL Net Services' and includes a navigation menu with options like 'Setup', 'AutoUpdate', 'Profiles', 'Network', 'Time', and 'https'. A sidebar on the left contains a tree view of system settings under categories like SYSTEM, USERS, NETWORK, and SECURITY. The 'Profiles' section is active, displaying a 'Create Profile' form for a new profile named 'ST38421A (hda)'. The form fields are as follows:


ST38421A (hda) New Profile on partition hda3	
Description	testprofile
Hostname (FQDN)	radius.gljs.sk
Kerberos 5 Realm	GLJS.SK
LDAP Base	dc=gljs,dc=sk
Admin password	
Confirm password	
NETWORK CONFIG	
Ethernet Interface	ETH00 - 3Com Corporation 3c905C-TX/TX-M [Tornado]
IP Address / Netmask	192.168.1.4 / 255.255.255.0
Default Gateway	


At the bottom of the sidebar, there is a 'Done' button.


- Nový profil s názvom **testprofile** sme vytvorili, uložili, ešte je potrebné ho aktivovať
Označíme profil, hore stlačíme **Activate**



ZS:192.168.1.4 - Mozilla Firefox

File Edit View History Bookmarks Tools Help


https://192.168.1.4/

 RADIUS server

 ZS:192.168.1.4





 Release 1.0.beta14
[About](#)

[Logout](#) [Reboot](#) [Shutdown](#)

SETUP
AutoUpdate
Profiles
Network
Time
https

Profile: _DB.005 (sda3)
Activate
Deactivate
Info
Delete
Backup

Warning:
 This software is NOT guaranteed to be bug free. It is your responsibility to properly test production devices with important data. In any case, the author is not responsible for any software.

Model: ATA SAMSUNG HD080HJ (sda)			
	Type: ext3	Capacity: 788 MB	
<div style="border: 1px solid gray; padding: 2px;">  sda3 Profiles </div>	Profile	Description	
	<input type="radio"/> _DB.004	profile	
	<input checked="" type="radio"/> _DB.005	testprofile	
<div style="border: 1px solid gray; padding: 2px;">  sda4 </div>	Type: ext2		
	Profile	Description	
	<input type="radio"/> _DB.001	profile	

Mar 29 20:10,43 SUCCESS: Session opened from host 192.168.1.2 (Admin)

Mar 29 20:11,34 SUCCESS: Profile _DB.005 successfully created on partition sda3

Done

- Zobrazia sa nám informácie o profile a znova stlačíme **Activate**

File Edit View History Bookmarks Tools Help

https://192.168.1.4/

RADIUS server ZS:192.168.1.4

ZEROSHELL Net Services

Release 1.0.beta14
About

Logout Reboot Shutdown

SETUP AutoUpdate Profiles Network Time https

Profile: _DB.005 (sda3) Activate Deactivate Info Delete Backup

ATA SAMSUNG HD080HJ (sda)
Profile _DB.005 on partition sda3

PROFILE INFO

Description	:	testprofile
HostName	:	radius.gljs.sk
K5 Realm	:	GLJS.SK
LDAP Base	:	dc=gljs,dc=sk
Last Activation	:	Never
Last Backup	:	Never

Warning: after the profile activation the system will be rebooted. This https connection will be closed and network firewall, VPNs and VLANs will be reconfigured. As a result, you could be not able to connect to the web interface system into Fail-Safe mode using the local console. For these reasons, you should never activate a new profile if console.

Done

- Aktiváciu je potrebné potvrdiť ešte raz stlačením **OK** a bude nasledovať **reboot** ZeroShell servera s nastaveniami uloženými v novom profile **testprofile**

ZS:192.168.1.4 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://192.168.1.4/

RADIUS server ZS:192.168.1.4

ZEROSHELL Net Services

Release 1.0.beta14
About

Logout Reboot Shutdown

SETUP AutoUpdate Profiles Network Time https

Profile: _DB.005 (sda3) Activate Deactivate Info Delete Backup

ATA SAMSUNG HD080HJ (sda)
Profile _DB.005 on partition sda3

PROFILE INFO

Description	: testprofile
HostName	: radius.gljs.sk
K5 Realm	: GLJS.SK
LDAP Base	: dc=gljs,dc=sk
Last Activation	: Never
Last Backup	: Never

Warning: after the profile activation the system will be rebooted. This https connection will be closed and network firewall, VPNs and VLANs will be reconfigured. As a result, you could be not able to connect to the web interface system into Fail-Safe mode using the local console. For these reasons, you should never activate a new profile if console.

The page at https://192.168.1.4/ Are you sure you want to activate

Done

- Po reštarte sa znova prihlásime cez webové rozhranie a nastavíme certifikát. (Nastavenie certifikátu môžete aj vynechať, ak Vám neprekáža, že certifikát bude mať označenie ZeroShell Example CA, ale doporučujem ho radšej nastaviť)
- Vľavo v sekcii **SECURITY** klikneme na **X.509 CA** a potom vpravo hore **Setup**
- Zaškrtneme voľbu vpravo hore **key** a hneď vedľa zvolíme typ **PEM**
- Vyplníme **Common Name** tu si napíšete označenie, pod ktorým bude Váš certifikát identifikovaný
- **Key Size** ponecháme na hodnote **1024 bits**
- **Validity (days)** počet dní platnosti certifikátu, **3650** znamená 10 rokov.
- Nasledovné 3 položky radšej vyplňte len dvojpísmenovou skratkou, pretože keď som skúsil zadať do týchto políček dlhšie reťazce, tak sa nový certifikát vygeneroval, ale s pôvodnými, teda predvolenými nastaveniami. Dôvod takéhoto správania som síce nezistil, ale pri použití dvojpísmenových skratiek, sa certifikát vygeneroval správne.
- Ešte vyplňte 3 posledné polia a potom stlačte vpravo hore **Generate**

ZS:192.168.1.4 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://192.168.1.4/

RADIUS server ZS:192.168.1.4

Release 1.0.beta14
About

ZEROSHELL
Net Services

Logout Reboot Shutdown

X.509 CA	List	Manage	CRL	Imported	Trus
----------	------	--------	-----	----------	------

CA Certificate and Private Key

Common Name radius.gljs.sk CA

Key Size 1024 bits

Validity (Days) 3650

Country Name SK

State or Province EU

Locality KN

Organization gljs.sk

Organizational Unit school

E-Mail Address servis@gljs.sk

CA Default Parameters

Key Size 1024 bits

Certificate Validity (days) 365

Export user/host certificates on the authentication page No

Apply

Mar 30 19:57,30 SUCCESS: System successfully started with Linux kernel 2.6.25.20 and ZeroShell 1.0.beta14
Mar 30 20:03,01 SUCCESS: Session opened from host 192.168.1.2 (Admin)

Done

- Nasleduje upozornenie o strate platnosti všetkých certifikátov vygenerovaných na tomto serveri, ale keďže sme ešte žiadny certifikát z tohoto servera nepoužili u klienta, môžeme bez obáv stlačiť **OK**

The page at https://192.168.1.4 says:

WARNING: if you continue with this operation you will lose all Certificates and Private Keys (Host and User Cetificates too) and the Certification Authority will be reset. If you actually want it then press [OK]

Cancel OK

- Nový certifikát je týmto vygenerovaný, teraz je potrebné urobiť Export dôveryhodného (Trusted) certifikátu
- Vpravo hore prejdeme na **Trusted CAs**

ZS:192.168.1.4 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://192.168.1.4/

RADIUS server ZS:192.168.1.4

Release 1.0 beta14

Trusted Certification Authorities

View CA View CRL Export

Trusted CAs list

radius.gijs.sk CA/emailAddress=servis@gijs.sk (Local CA) [CRL:Mar 30 2011]
--

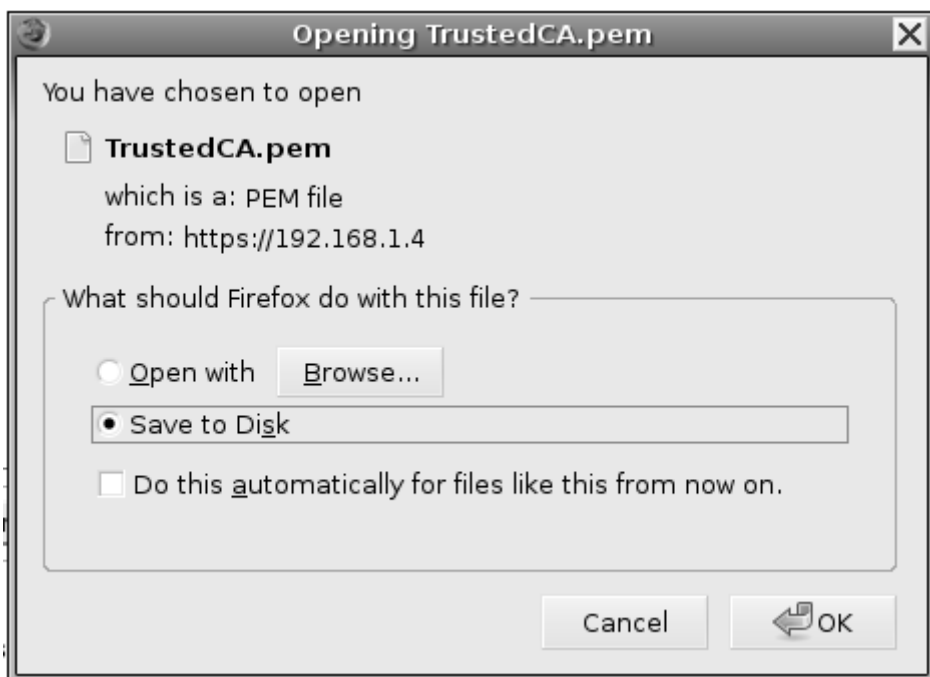
Import Browse... Remove

Note:
You can specify a file which contains the X.509 certificate of the CA to import, the CRL or both in

Done

Done

- V zozname označíme certifikát, ktorý budeme exportovať, vpravo hore nastavíme typ **PEM** a stlačíme **Export**



- **Takto vygenerovaný certifikát si uložte na USB, bude ho potrebné nakopírovať do každého klientského počítača, ktorý má byť overovaný cez RADIUS server.**
- Ako importovať certifikát, bude popísané neskôr, v časti Konfigurácia klienta
- Ešte musíme v ZeroShelli zapnúť **RADIUS** server

Browser: ZS:192.168.1.4 - Mozilla Firefox
 URL: https://192.168.1.4/
 Page Title: ZS:192.168.1.4

ZEROSHELL Net Services
 Release 1.0.beta14
[About](#) [Logout](#) [Reboot](#) [Shutdown](#)

RADIUS Manage Access Points Proxy Acc

RADIUS Server for Wireless and Identity Based Networking Services

Status: **ACTIVE**

802.1x Configuration

X.509 Host Certificate
 Local CA
 Status: OK

Some Notes
 This RADIUS server supports EAP-TLS, PEAP and EAP-TTLS because through TLS they guarantee a strong authentication (WPA). In order to encrypt the communication between the RADIUS server and the clients you need to select an X.509 user certificates and related keys on the client-side in order to authenticate the users. In PEAP you need to use MSCHAPv2 that authenticate the clients with the same usernames and passwords used with Kerberos 5. In any case you need to use a shared secret between the RADIUS server and the Access Points in order to permit their connection to the WLAN. Don't forget to set a shared secret between Access Points and the RADIUS server in order to permit their connection to the WLAN.

Mar 19 12:42:09 SUCCESS: System successfully started with Linux kernel 2.6.25.20 and ZeroShell 1.0.beta14
 Mar 19 13:09:51 SUCCESS: Session opened from host 192.168.1.2 (Admin)

Done

- Vľavo v sekcii **USERS** klikneme na **RADIUS**, vpravo nastavíme **Enabled** a potom **Save**
- Nastavíme AP (Access Point, aspoň jeden)
- Klikneme hore na **Access Point** alebo **RADIUS AUTHORIZED CLIENTS** (vo verzii beta 16)

Release 1.0.beta14
About

Logout Reboot Shutdown

RADIUS Manage Access Points Proxy Acc

SYSTEM

- Setup
- Logs
- Utilities

USERS

- Users
- Groups
- LDAP / NIS
- RADIUS
- Captive Portal

NETWORK

- Hosts
- Router
- DNS
- DHCP
- VPN
- QoS
- Wireless
- Net Balancer

SECURITY

- Kerberos 5
- Firewall
- X.509 CA
- HTTP Proxy

Done

Access Point List

Access Point Name	IP or Subnet	Shared Secret
<input type="text"/>	<input type="text"/> / <input type="text"/>	<input type="text"/>

	Access Point Name	IP or Subnet	
	CANYON	192.168.1.5	tes

- AP nejakým spôsobom pomenujeme, zadáme jeho IP adresu, a tzv. **Shared Secret** je to ľubovoľný reťazec znakov, ale rovnaký musí byť nastavený aj v AP
- Stlačíme **Add** potom **Close** a nakoniec znova **Save**

DHCP Server

DHCP server potrebujeme, aby boli dynamicky pridelované IP adresy počítačom, ktoré sa budú pripájať cez wifi do našej siete.

Ak už máte v sieti nejaký DHCP server, potom DHCP server v ZeroShelli ponechajte vypnutý !
Ak by boli v jednej sieti 2 DHCP servery, mohlo by dôjsť ku konfliktu IP adres a tým k problémom v celej LAN

Ak nemáte iný DHCP server, potom pre pridelovanie IP adres bude takýto server potrebný

- Vľavo v sekcii **NETWORK** kliknite na **DHCP**, potom vpravo hore **New** a nastavíme podsieť, potom **OK**

ZS:192.168.1.4 - Mozilla Firefox
 File Edit View History Bookmarks Tools Help
 https://192.168.1.4/
 ZS:192.168.1.4 RADIUS server
 Release 1.0.beta14
 About Logout Reboot Shutdown
ZEROSHELL
 Net Services
DHCP SERVER Manage Leases
 Active on: Sub
 WARNING: DHCP Server is not started because there is not a subnet configured.
 Save
 Dynamic IP Configur
 Default Days 00
 Range 1
 Range 2
 Range 3
 Subnet Options
 Default Gateway
 DNS 1
 DNS 2
 DNS 3
 Domain Name
 NIS Domain
 Done
 Apr 14 18:19,25 SUCCESS: DHCP subnet 192.168.1.0/255.255.255.0 successfully saved.
 Apr 14 18:27,23 SUCCESS: DHCP subnet 192.168.1.0/255.255.255.0 successfully deleted.

- Vpravo zaškrtnúť **Enabled** a doplniť rozsah IP adries **Range 1**, ktoré budú pridelované dynamicky. IP adresy, ktoré sú mimo tohoto rozsahu, nebudú pridelované DHCP serverom, a môžu byť použité staticky.
- Na záver uložíme konfiguráciu **Save** a DHCP server je pripravený pridelovať IP adresy.

File Edit View History Bookmarks Tools Help

https://192.168.1.4/

ZS:192.168.1.4

ZEROSHELL
Net Services

Release 1.0.beta14
[About](#)

[Logout](#) [Reboot](#) [Shutdown](#)

DHCP SERVER Manage Leases

Active on: ETH01 Subnet 192.168.1.0/255.25

Save Changes not saved

Dynamic IP Configuration

	Default Lease Time			Max Lease Time		
	Days	Hours	Minutes	Days	Hours	Minutes
Range 1	00	08	00	00	12	00
Range 2						
Range 3						

Range 1: 192.168.1.200 - 192.168.1.254

Range 2: -

Range 3: -

Subnet Options Advanced

Default Gateway	192.168.1.1
DNS 1	192.168.1.1
DNS 2	192.168.1.2
DNS 3	
Domain Name	gljs.sk
NIS Domain	
NTP Server	

Static IP Entries

Fixed IP	MAC

Apr 15 18:56,36 SUCCESS: Session opened from host 192.168.1.2 (Admin)
Apr 15 18:56,56 SUCCESS: DHCP subnet 192.168.1.0/255.255.255.0 successfully created.

Done

Uživatelia

Najprv vymažeme skupinu **nobody**, nepýtajte sa prečo, ak som mal nadefinovanú túto skupinu užívateľov, tak autentifikácia cez RADIUS neprebehla korektne, po vymazaní skupiny **nobody** už išlo všetko správne.

Predpokladám, že to súvisí s obmedzenými, alebo žiadnymi právami tejto skupiny

- Vľavo v sekcii **USERS** klikneme na **Groups** označíme skupinu **nobody** a potom vpravo hore **Delete** a klik na **OK**

ZS:192.168.1.4 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://192.168.1.4/

ZS:192.168.1.4 RADIUS server

ZEROSHELL Release 1.0.beta14
Net Services [About](#) [Logout](#) [Reboot](#) [Shutdown](#)

GROUPS

Entries found: **1** Group GID

	Group	GID	Secondary Group's
<input checked="" type="radio"/>	nobody	1	

The page at https://192.168.1.4 says:

Are you sure you want to delete the group?

Cancel

Apr 14 18:57,55 SUCCESS: DNS service successfully enabled
Apr 14 18:57,57 SUCCESS: DNS service successfully disabled

Done

- Teraz nadefinujeme mená a heslá užívateľov, ktorým chceme povoliť pripojenie cez WiFi
- Vľavo, v sekcii **USERS** klikneme na **Users** potom **Add**
Vyplníme **meno** toto je prihlasovacie meno do Wifi siete,
ďalej klikneme do poľa vpravo od **home directory** a systém sám doplní domovský adresár,
vpravo v sekcii **Default Shell** vyberieme **other** a prepíšeme na **/bin/false**.
- Vyplníme údaje o užívateľovi **krstné meno, priezvisko, e-mailovú adresu** a **2 x heslo**
Toto **heslo** spolu s **prihlasovacím menom** budú použité na autentifikáciu prístupu do Wifi siete.

File Edit View History Bookmarks Tools Help

https://192.168.1.4/

ZS: 192.168.1.4 RADIUS server

ZEROSHELL Release 1.0.beta14
Net Services [About](#) [Logout](#) [Reboot](#) [Shutdown](#)

USERS List View Add Edit Delete

(New User)

Account Information

Username UID

Home Directory Default Shell bash

User Information

Firstname Lastname

Description E-Mail

RADIUS Accounting

Expiration (mm/dd/yyyy) / /

Accounting Class

Limits Costs

User Password

Password

Confirm

Apr 14 19:18,06 SUCCESS: entry "uid=sergej,ou=People,dc=gljs,dc=sk" deleted
Apr 14 19:18,06 SUCCESS: Kerberos 5 principal and X.509 certificate related to the user sergej deleted

Done

- Nakoniec stlačíme **Submit**, bude nasledovť generovanie osobného certifikátu, ktorému nemusíme venovať pozornosť a môžeme sa vrátiť vľavo do sekcie **USERS Users** a uvidíme zoznam užívateľov.

File Edit View History Bookmarks Tools Help

https://192.168.1.4/

ZS:192.168.1.4 RADIUS server

ZEROSHELL Release 1.0.beta14
Net Services About

Logout Reboot Shutdown

USERS List View Add Edit Delete

Entries found: 3 Search

	Username	Group	Description
🔄	admin	0	System Administrator
🔄	dolinsky	65534	Jozef Dolinsky
🔄	sergej	65534	Sergej Nikitcenko

Apr 14 19:34,59 SUCCESS: entry "uid=abc,ou=People,dc=gljs,dc=sk" deleted
Apr 14 19:34,59 SUCCESS: Kerberos 5 principal and X.509 certificate related to the user abc deleted

Done

Týmto máme RADIUS server nastavený a nastavíme Access Point AP

Konfigurácia Access Pointu AP

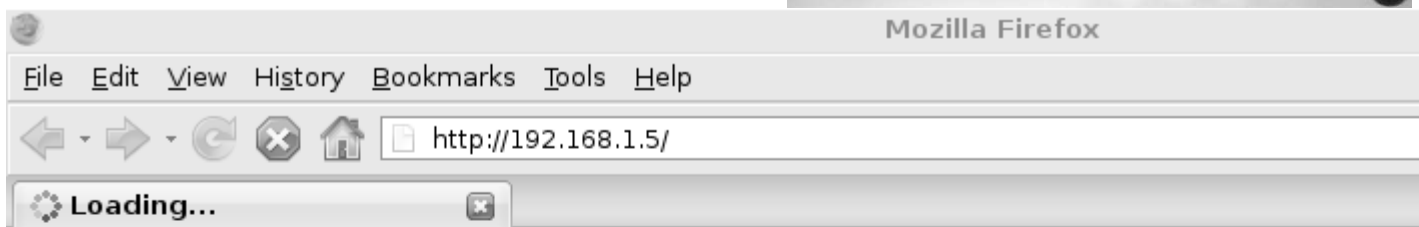
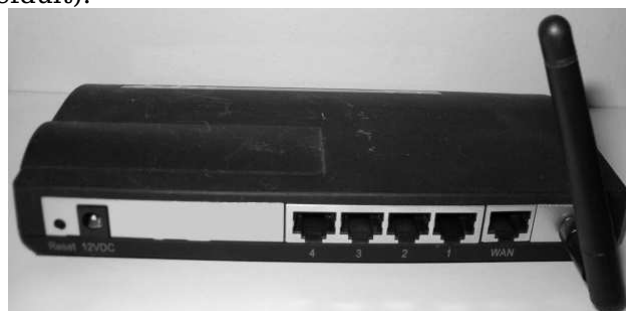
Na bezdrôtové pripojenie som použil **CANYON 802.11g Wireless Router CN-WF514**

- Resetnite AP do výrobných nastavení tlačítkom na zadnej stene.
- Tlačítko pre Reset je vedľa konektora napájacieho zdroja
- Po resete má AP nastavenú IP adresu **192.168.2.1**
- Nastavte si na PC IP adresu 192.168.2.2, spojte ho prekříženým ethernet káblom s AP, alebo priamym ethernet káblom cez switch
- Switch musí byť od LAN odpojený.
- Ethernet kábel pripojte na AP do portu s označením **1**, nie WAN.
- Teraz sa pripojte na webové rozhranie AP,



cez ľubovoľný web prehliadač, do ktorého zadajte IP adresu: **192.168.2.1**

- Meno pre prihlásenie: **admin** (default) heslo: **1234** (default).



- Po prihlásení, uvidíte nasledovnú obrazovku, potom kliknite na **General Setup**

Wireless Router - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.1.5/index.asp

Wireless Router

Broadband Router

Quick Setup

General Setup

Status Info

Tools

Quick Setup Wizard

The Quick Setup Wizard provides only the necessary configurations to connect your Broadband router to your Internet Service Provider (ISP) through an external cable or a DSL modem.

General Setup

The Broadband router supports advanced functions like Virtual Server, Access Control, Hacker Attack Detection and DMZ. We highly recommend you keep the default settings.

Status Information

The Broadband router's status information provides the following information about your Broadband router: Hardware/Firmware version, Serial Number, and its current operating status.

Tools

Broadband router Tools - Tools include Configuration tools, Firmware upgrade and Reset. Configuration tools allow you to Backup, Restore, or Restore to Factory Default setting for your Broadband router. The Firmware upgrade tool allows you to upgrade your Broadband router's firmware. The RESET tool allows you to reset your Broadband router.

Done

- Kliknite na **System**, **Time Zone** a nastavte časové pásmo a IP adresu Time Servera.
- Každé nastavenie je potrebné potvrdiť tlačidlom **Apply**

Wireless Router - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.1.5/index.asp

Wireless Router

Broadband Router

- ✓ System
 - ▶ Time Zone
 - ▶ Password Settings
 - ▶ Remote Management
- WAN
- LAN
- Wireless
- QoS
- NAT
- Firewall

Time Zone

Set the time zone of the Broadband router. This information is used for logging.

Set Time Zone :	(GMT+01:00)Belgrade, Bratislava, Budape
Time Server Address :	192.43.244.18
Daylight Savings :	<input type="checkbox"/> Enable Function Times From January 1 To

http://192.168.1.5/systimezone.asp

- Nastavte si nové heslo užívateľa **admin**, pre prístup cez web kliknutím na **Password Settings**
- Ak ste heslo ešte nemenili potom **Current Password: 1234**
- Nové heslo zapíšte 2x do ďalších riadkov, potom **Apply**

Wireless Router - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.1.5/index.asp

Wireless Router

Broadband Router

- System
 - Time Zone
 - Password Settings
 - Remote Management
- WAN
- LAN
- Wireless
- QoS
- NAT
- Firewall

Password Settings

You can change the password required to log into the broadband router's default, the password is 1234. So please assign a password to the Adminis a safe place. Passwords can contain 0 to 30 alphanumeric characters, and

Current Password :

New Password :

Confirmed Password :

http://192.168.1.5/syspasswd.asp

- Nastavíme základné sieťové parametre pre router **IP adresu, masku**
- Ak máte v sieti DHCP server, potom tento ponechajte vypnutý

Wireless Router - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.1.5/index.asp

Wireless Router

Broadband Router

- System
- WAN
- LAN**
- Wireless
- QoS
- NAT
- Firewall

LAN Settings

You can enable the Broadband router's DHCP server to dynamically allocate IP addresses to PCs. The broadband router must have an IP Address for the Local Area Network.

LAN IP

IP Address :	192.168.1.5
IP Subnet Mask :	255.255.255.0
802.1d Spanning Tree :	Disabled
DHCP Server :	Disabled
Lease Time :	Forever

DHCP Server

Start IP :	192.168.2.100
End IP :	192.168.2.200
Domain Name :	

Done

- Zapneme bezdrôtové pripojenie cez **WiFi**, teda funkciu Access Pointu AP

Wireless Router - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.1.5/index.asp

Wireless Router

Broadband Router

- System
- WAN
- LAN
- Wireless**
 - Basic Settings
 - Advanced Settings
 - Security Settings
 - Access Control
- QoS
- NAT
- Firewall

Wireless Settings

The gateway can be quickly configured as a wireless access point for roaming access identifier and channel number. It also supports data encryption and...

Enable or disable Wireless module function : Enable Disable

Done

- Nastavíme základné parametre pre WiFi **mod AP**, **frekvenciu**, **ESSID** teda názov bezdrôtovej siete a **kanál**

Wireless Router - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.1.5/index.asp

Wireless Router

Broadband Router

- System
- WAN
- LAN
- Wireless**
 - Basic Settings
 - Advanced Settings
 - Security Settings
 - Access Control
- QoS
- NAT
- Firewall

Wireless Setting

This page allows you to define ESSID, and Channel for the wireless connection. The stations to connect to the Access Point.

Mode :	AP
Band :	2.4 GHz (B+G)
ESSID :	D
Channel Number :	11
Associated Clients :	Show Active Clients

Done

- V rozšírených nastaveniach zvolíme **Authentication Type: Auto**
- Aby bola WiFi sieť viditeľná **Broadcast ESSID: Enabled**

Wireless Router - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.1.5/index.asp

Wireless Router

Broadband Router

- System
- WAN
- LAN
- ✓ Wireless
 - ▶ Basic Settings
 - ▶ **Advanced Settings**
 - ▶ Security Settings
 - ▶ Access Control
- QoS
- NAT
- Firewall

Advanced Settings

These settings are only for more technically advanced users who have a su
These settings should not be changed unless you know what effect the cha
router.

Authentication Type :	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto	
Fragment Threshold :	<input type="text" value="2346"/>	(256-2346)
RTS Threshold :	<input type="text" value="2347"/>	(0-2347)
Beacon Interval :	<input type="text" value="100"/>	(20-1024 ms)
Data Rate :	Auto ▾	
Preamble Type :	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Short Preamble	
Broadcast ESSID :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
IAPP :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
802.11g Protection :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	

http://192.168.1.5/wladvance.asp

- V nasledovnom kroku nastavíme parametre nevyhnutné pre spoluprácu AP s RADIUS serverom.
- Zabezpečenie **Encryption: WPA RADIUS**
- Kľúč **WPA Unicast Cipher Suite: WPA2 Mixed**
- IP adresa RADIUS servera, IP ktorú sme prideliť RADIUS serveru **RADIUS Server IP address: 192.168.1.4**
- **RADIUS Server Port: 1812** čo je štandardný port protokolu TCP/IP pre RADIUS server
- **RADIUS Server Password** musí byť rovnaký reťazec, aký sme nastavili na RADIUS serveri v **Shared Secret**

Wireless Router - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.1.5/index.asp

Wireless Router

Broadband Router

- System
- WAN
- LAN
- Wireless**
 - Basic Settings
 - Advanced Settings
 - Security Settings
 - Access Control
- QoS
- NAT
- Firewall

Security

This page allows you setup the wireless security. Turn on WEP or WPA by using En access to your wireless network.

Encryption :	WPA RADIUS
WPA Unicast Cipher Suite :	<input type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input checked="" type="radio"/> WPA
RADIUS Server IP address :	192.168.1.4
RADIUS Server Port :	1812
RADIUS Server Password :	*****

http://192.168.1.5/wlencrypt.asp

- Prekladanie IP adres **NAT** necháme vypnuté **Disable**, pretože teraz nepotrebujeme smerovať pakety do rôznych sietí.

Wireless Router - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.1.5/index.asp

Wireless Router

Broadband Router

- [System](#)
- [WAN](#)
- [LAN](#)
- [Wireless](#)
- [QoS](#)
- [NAT](#)
 - ▶ [Static Routing](#)
- [Firewall](#)

NAT Settings

Network Address Translation (NAT) allows multiple users at your local s through a single Public IP Address or multiple Public IP Addresses. NAT protection from hacker attacks and has the flexibility to allow you to ma Public IP Addresses for key services such as the Web or FTP.

Enable or disable NAT module function : Enable Disable

Done

- **Firewall** necháme tiež vypnutý **Disable**

Enable Disable'. The browser status bar at the bottom shows 'Done'."/>

Wireless Router - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.1.5/index.asp

Wireless Router

Broadband Router

- System
- WAN
- LAN
- Wireless
- QoS
- NAT
- Firewall

Security Settings (Firewall)

The Broadband router provides extensive firewall protection by restricting... thus limiting the risk of hacker attack, and defending against a wide array... However, for applications that require unrestricted access to the Internet... specific client/server as a Demilitarized Zone (DMZ).

Enable or disable Firewall module function : Enable Disable

Done

- Nakoniec stlačíme **Apply**, počkáme, kým sa router reštartuje a týmto je jeho konfigurácia ukončená
- Ešte môžeme skontrolovať nastavenia kliknutím na **Status**

Wireless Router - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.1.5/index.asp

Wireless Router

Broadband Router

Status

- Internet Connection
- Device Status
- System Log
- Security Log
- Active DHCP Client
- Statistics

Current Time
1/1/2000

Status and Information

You can use the Status page to monitor the connection status for the Broadband Router firmware and hardware version numbers, any illegal attempts to access your network, and the DHCP client PCs currently connected to your network.

System

Model	Wireless Router
Up time	Oday:0h:21m:44s
Hardware Version	Rev. A
Boot Code Version	1.0
Firmware Version	1.49

javascript:goSta();

Wireless Router - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.1.5/index.asp

Wireless Router

Broadband Router

Status

- ▶ Internet Connection
- ▶ **Device Status**
- ▶ System Log
- ▶ Security Log
- ▶ Active DHCP Client
- ▶ Statistics

Current Time
1/1/2000

Device Status

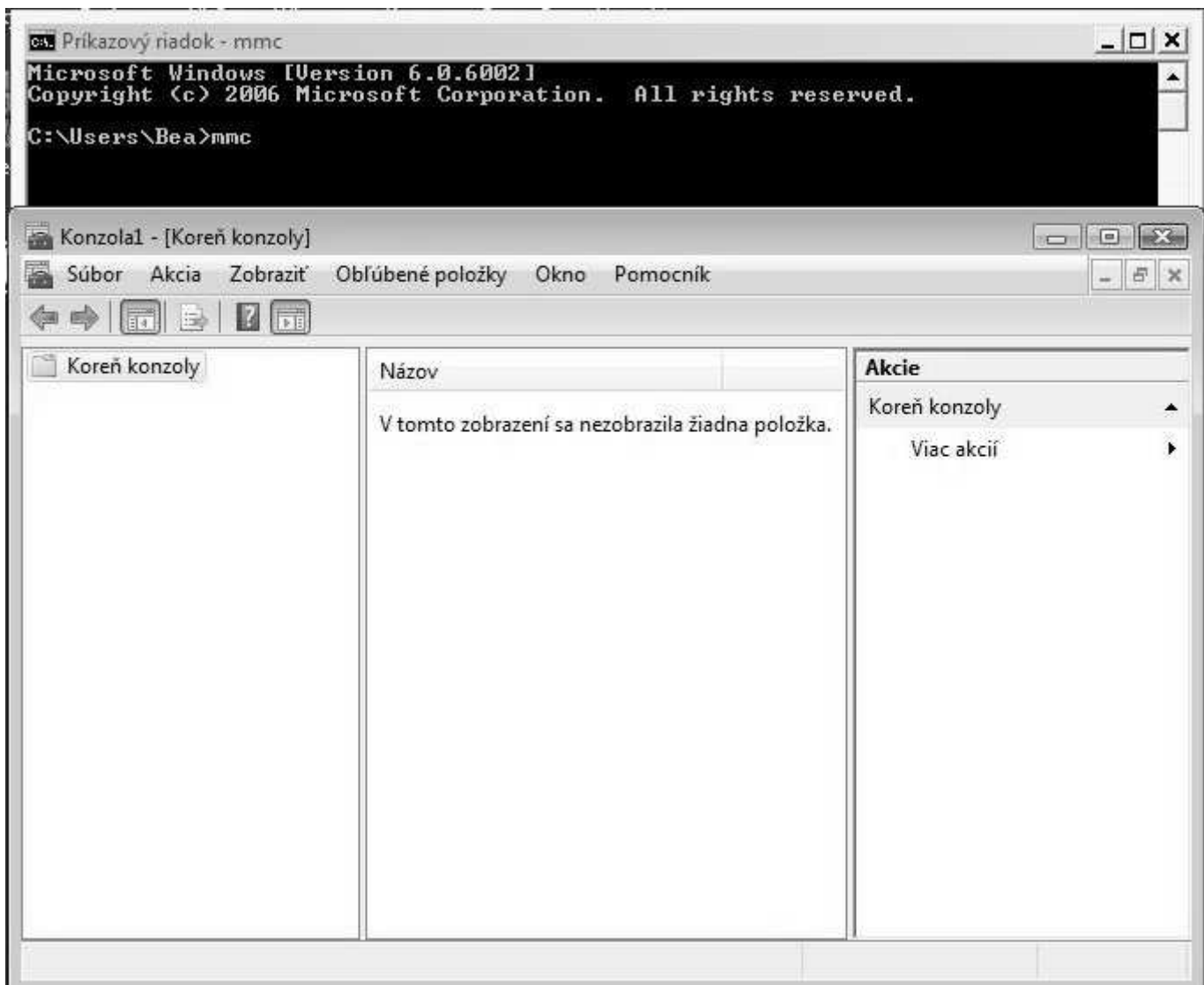
View the current setting status of this device.

Wireless Configuration	
Mode	AP
ESSID	D
Channel Number	11
Security	WPA RADIUS
Associated Clients	0
BSSID	00:0e:2e:d8:6b:e5
LAN Configuration	
IP Address	192.168.1.5
Subnet Mask	255.255.255.0
DHCP Server	Disabled
MAC Address	00:0e:2e:d8:6b:e5

http://192.168.1.5/stadevice.asp

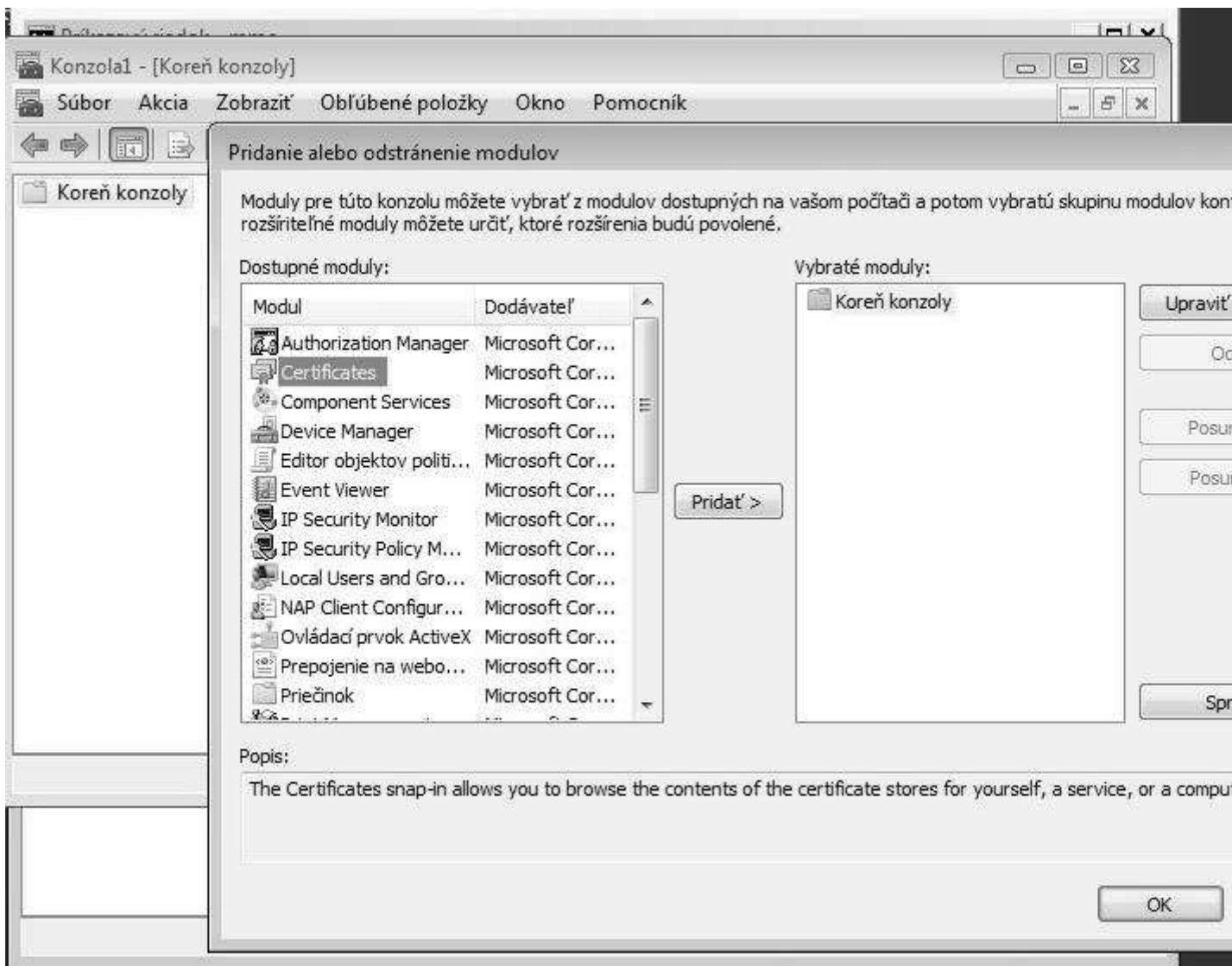
Konfigurácia klienta - W7/Vista/XP

- Spustíte príkazový riadok a v ňom zadajte príkaz **mmc**

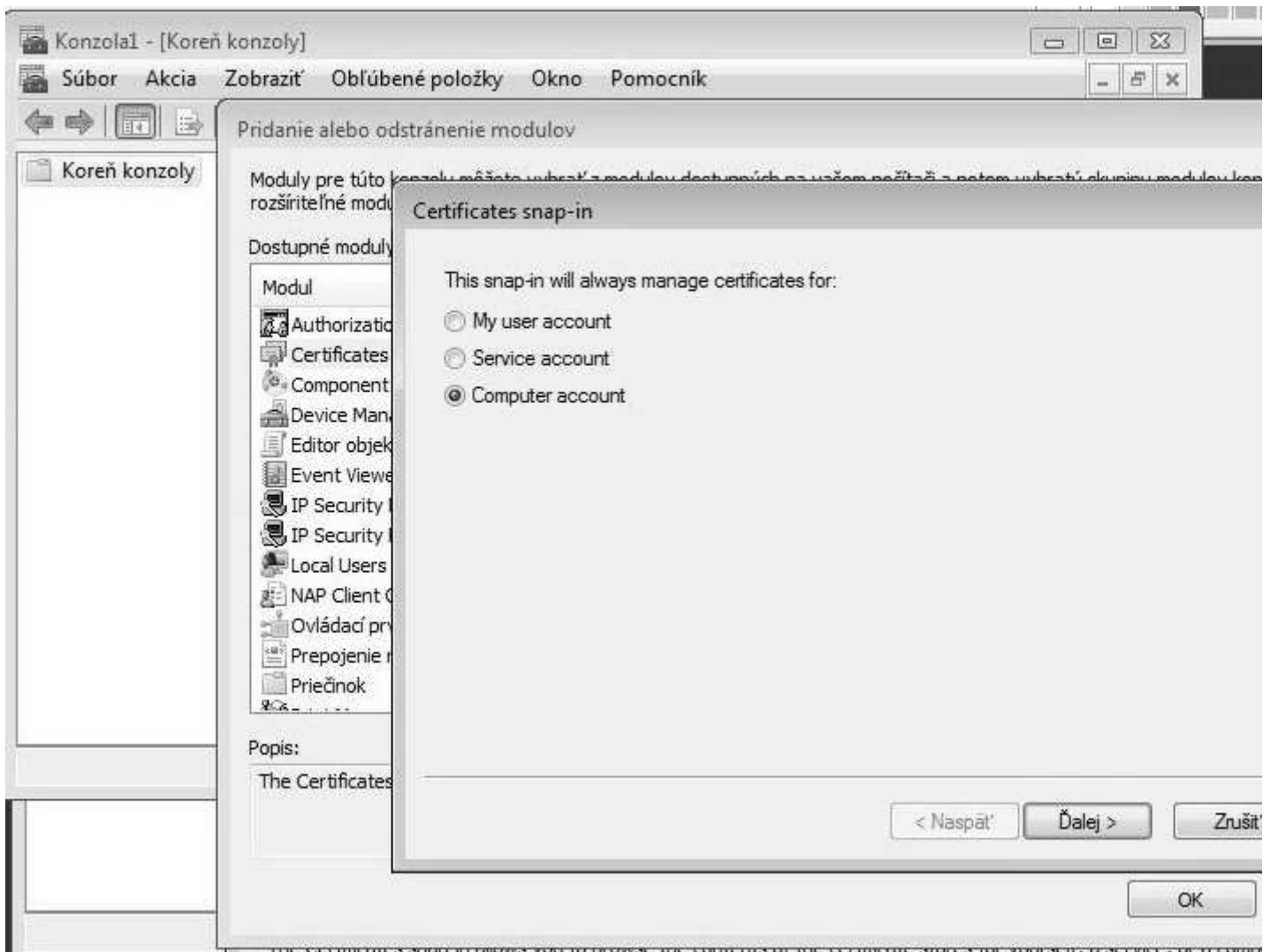


Týmto príkazom sa spustí **Konzola1** a v nej sa zobrazí **[Koreň konzoly]**

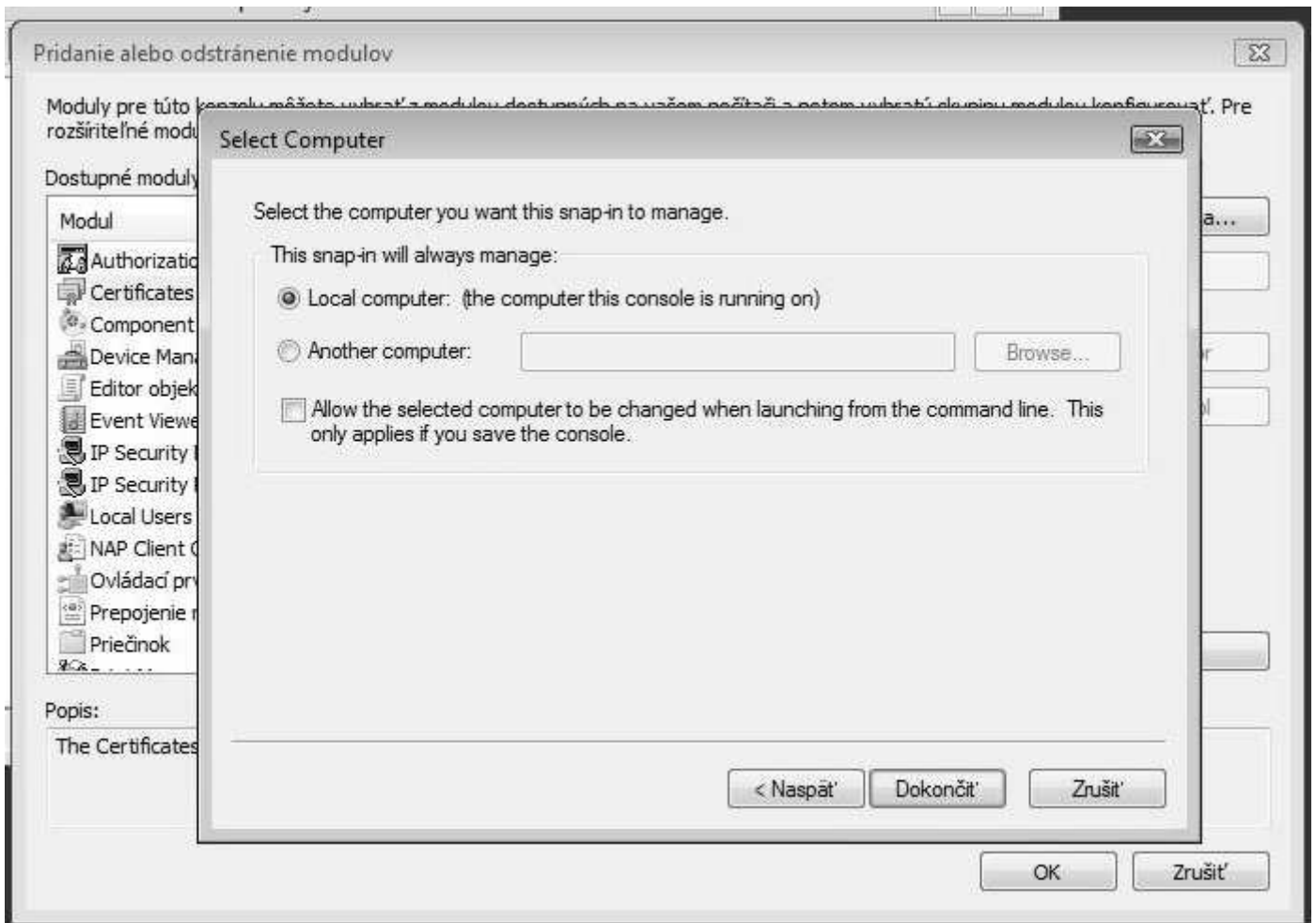
- Kliknite na **Súbor** (File), potom **Pridať** (Add/Remove Snap-in...)
- Potom dole **Pridať** (Add...), v ďalšom okne kliknúť na **Certifikáty** ďalej **Pridať**



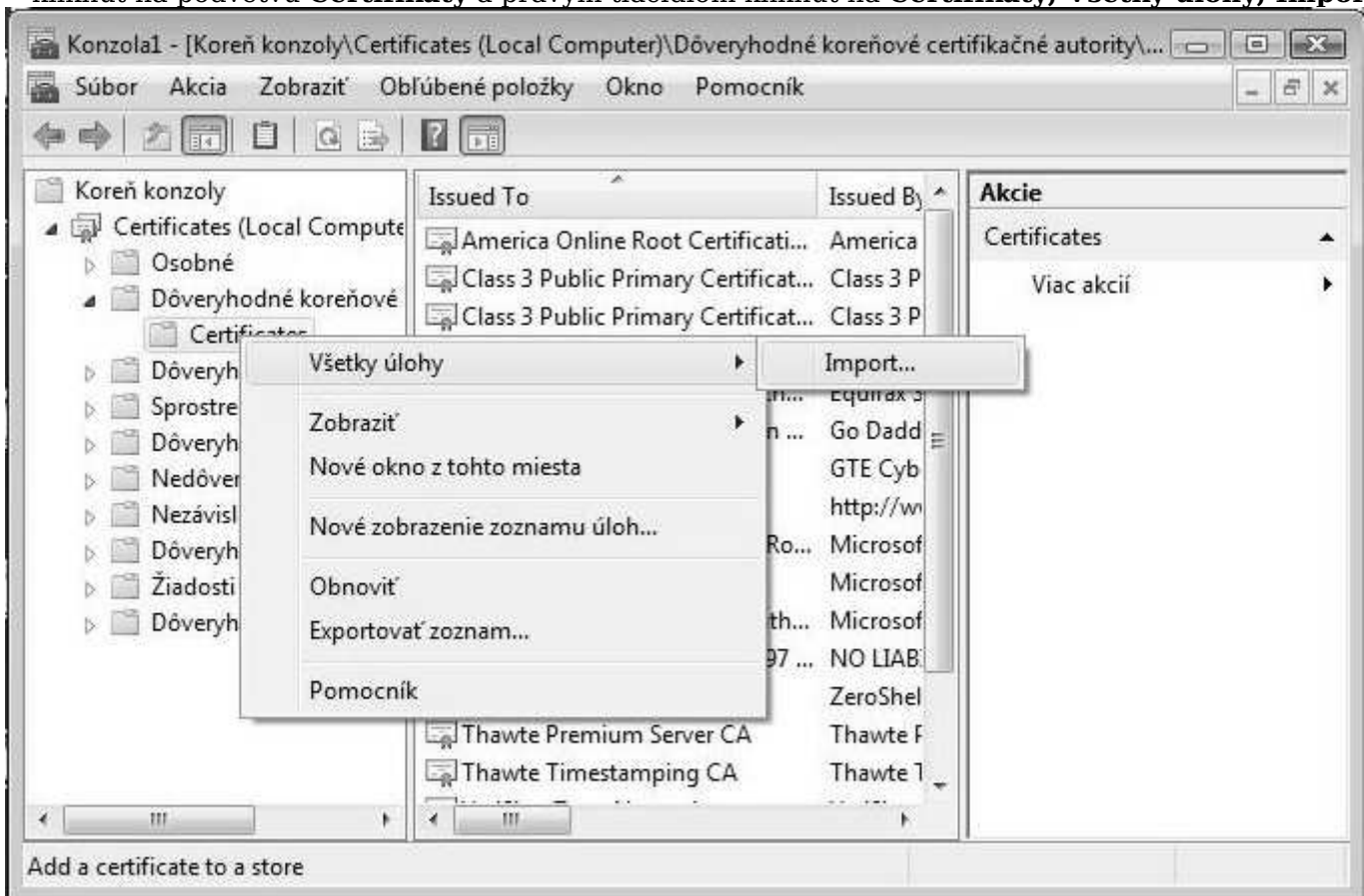
- Potom vybrať **Konto počítača**



- Pokračovať kliknutím dole na tlačítko **Ďalej** (Next),



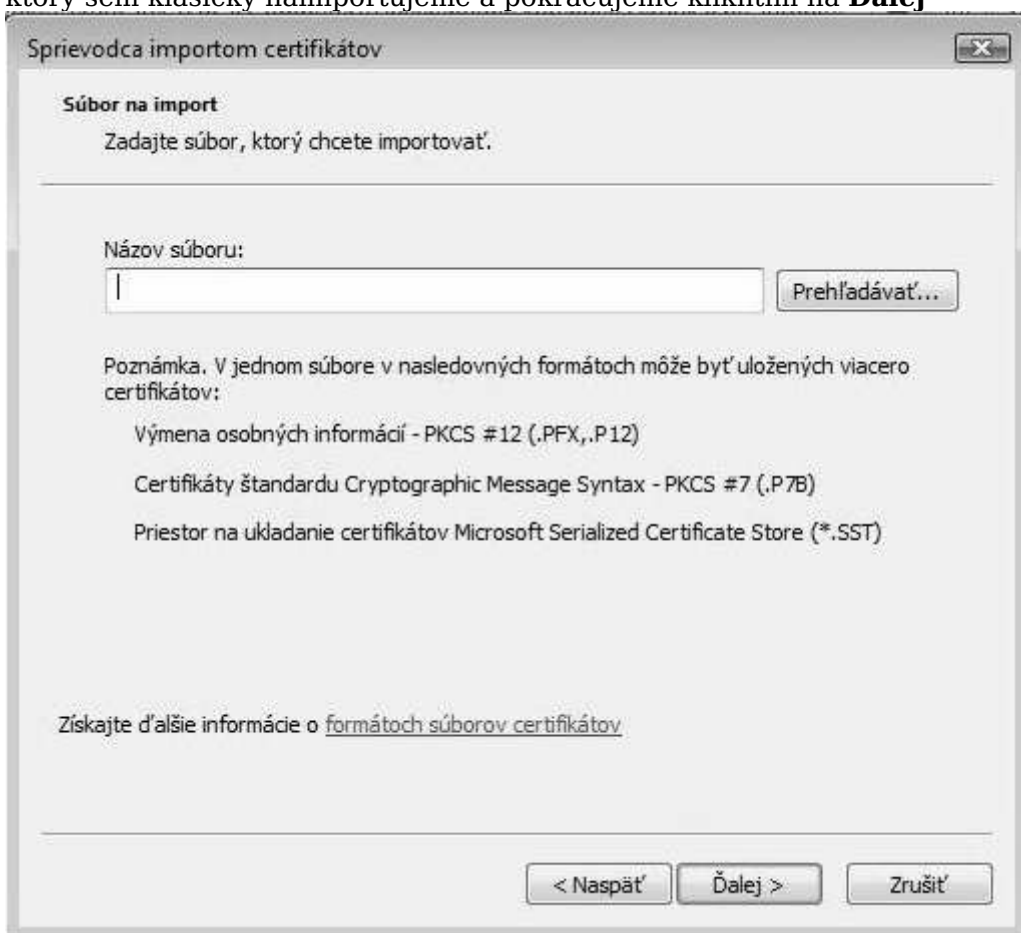
- potom **Dokončiť**
- Vrátiť sa do okna **Konzola1 - [Koreň konzoly]**, rozbaľiť strom **Dôveryhodné koreňové**
- kliknúť na podvetvu **Certifikáty** a pravým tlačidlom kliknúť na **Certifikáty, Všetky úlohy, Import**



- Spustí sa **Sprievodca importu certifikátov**



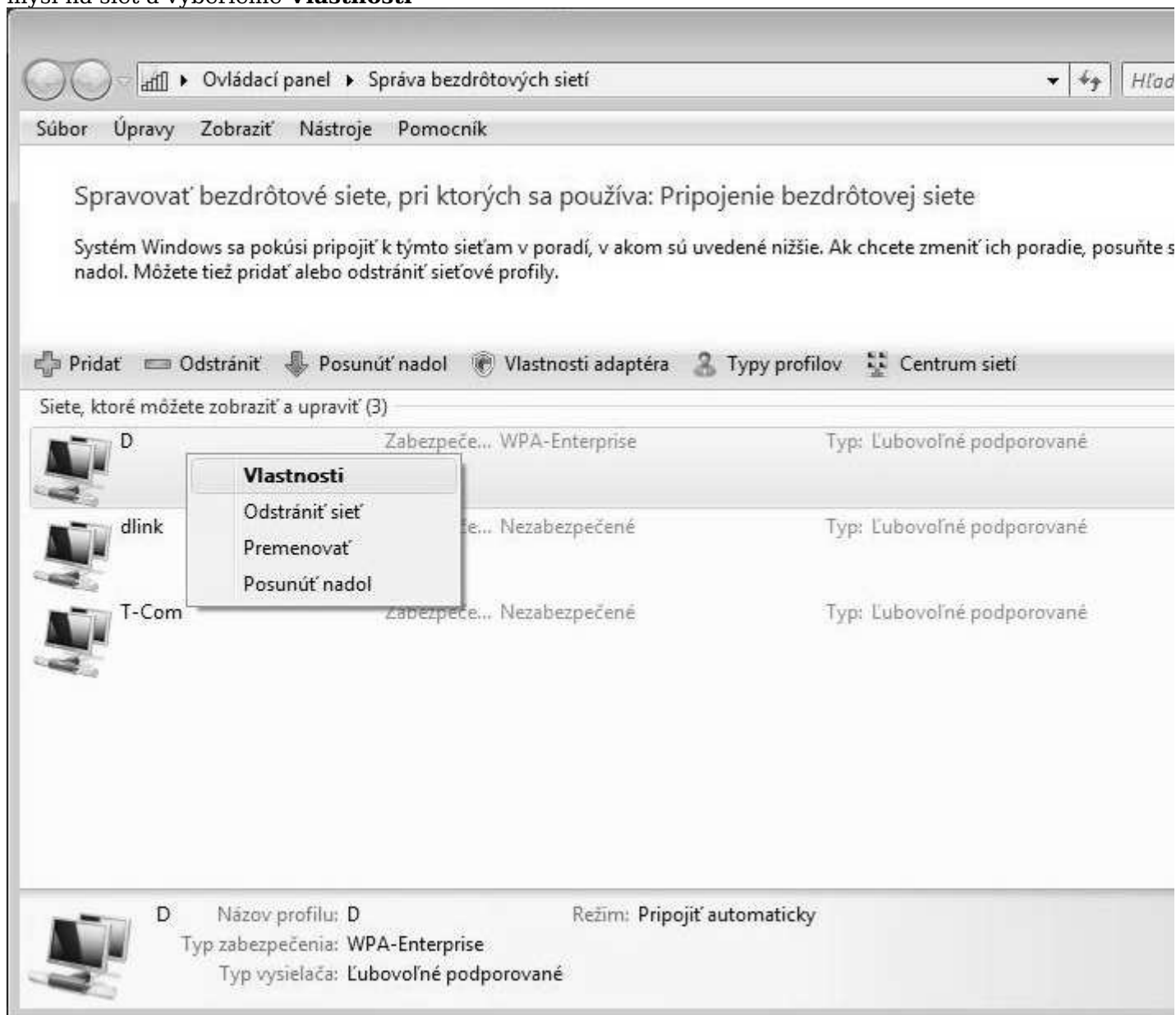
Pokračujeme tlačidlom **Ďalej** a pripravíme si súbor **TrustedCA.pem**, ktorý sem klasicky nainportujeme a pokračujeme kliknutím na **Ďalej**



Po úspešnom importe certifikátu zveríme všetky okná, a otvoríme **Centrum sietí**. Ak sieť ku ktorej sa chceme pripojiť v zozname nieje, môžeme ju ručne

pridať stlačením tlačítka **+** **Pridať**

Ak sieť, s názvom SSID ktorý sme nastavili na AP v zozname existuje, tak klikneme pravým tlačidlom myši na sieť a vyberieme **Vlastnosti**

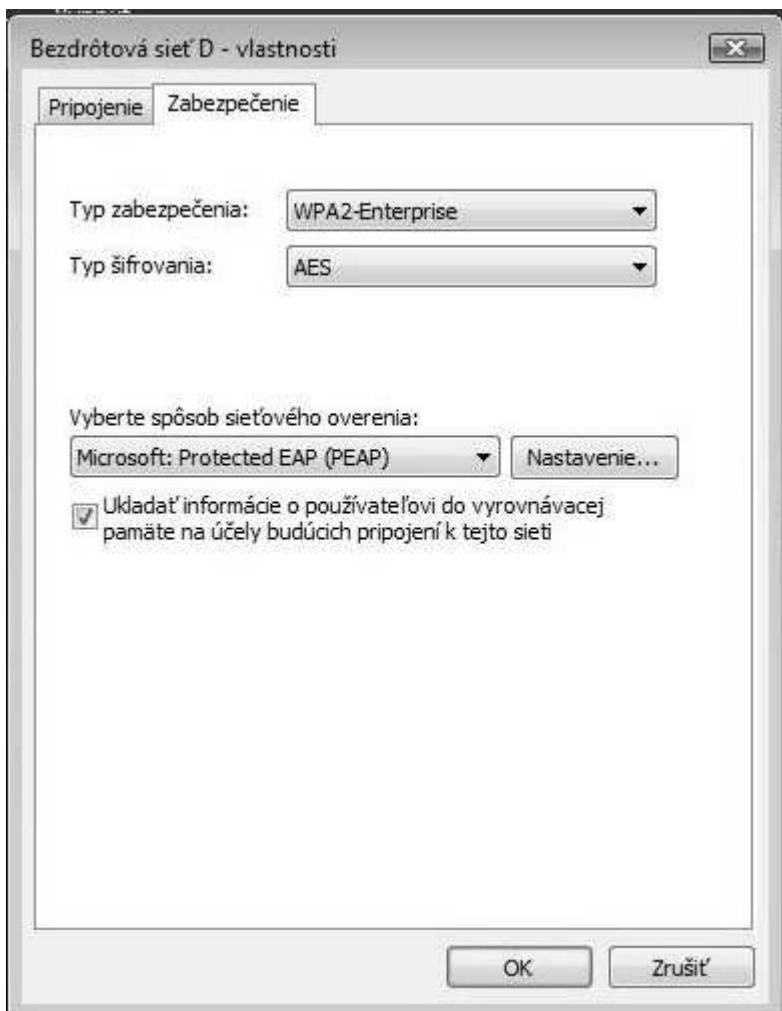


Kliknutím na **Vlastnosti** sa dostaneme k nasledovným voľbám

Tu je potrebné nastaviť Typ zabezpečenia: **WPA2-Enterprise** a Typ šifrovania: **AES**

Spôsob sieťového overenia: **Microsoft: Protected EAP(PEAP)**

Nakoniec klikneme na **Nastavenie...**



Tu musíme zaškrtnúť **Overiť certifikát servera**

Ďalej zaškrtnúť **Pripojiť sa na tieto servery**

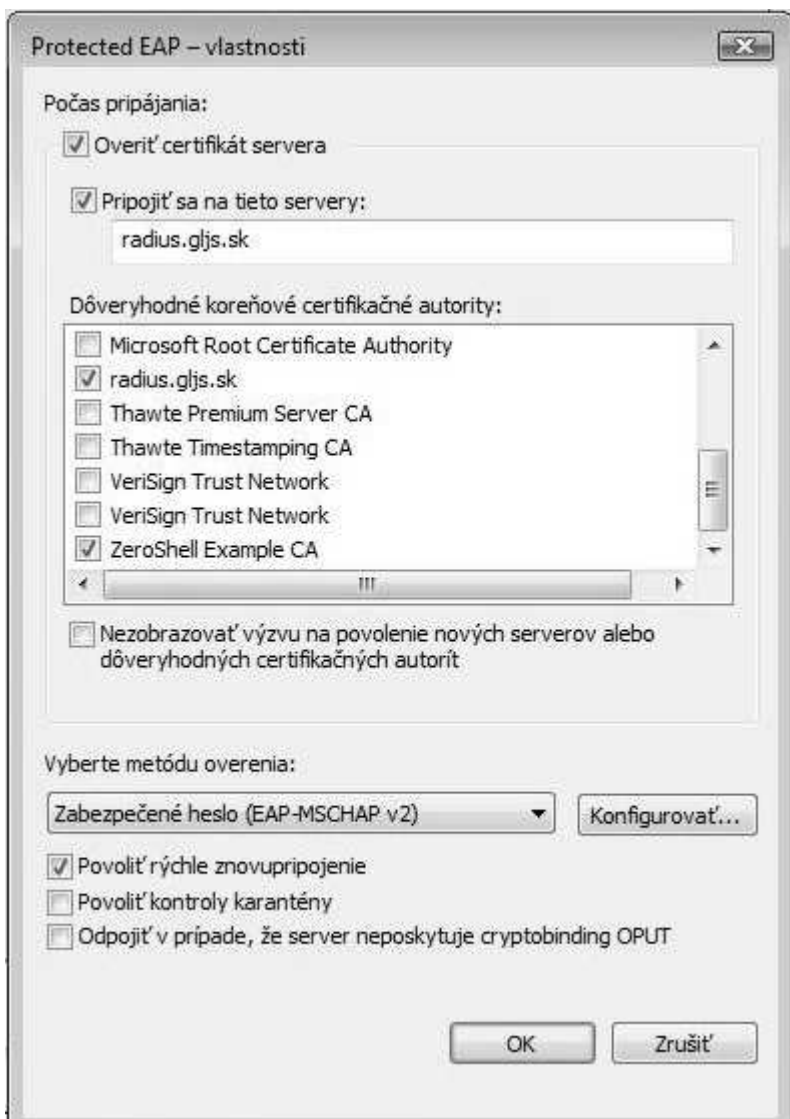
Do prázdneho políčka zadať **meno radius servera** (alebo jeho IP adresu)

V zozname **Dôveryhodných koreňových certifikačných autorít**

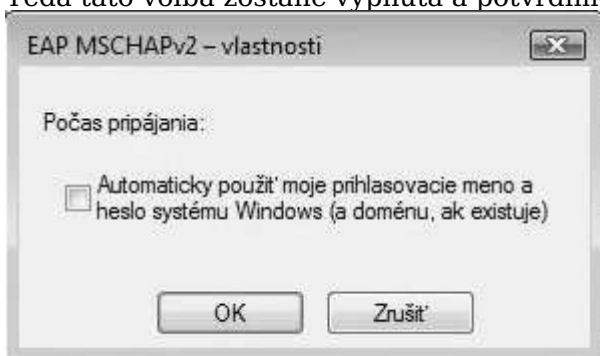
vyľadáme náš **nainportovaný certifikát** a **zaškrtneme** jeho overovanie.

Ďalej Vyberieme metódu overovania: **Zabezpečené heslo (EAP-MSCHAP v2)**

Klikneme na **Konfigurovať**

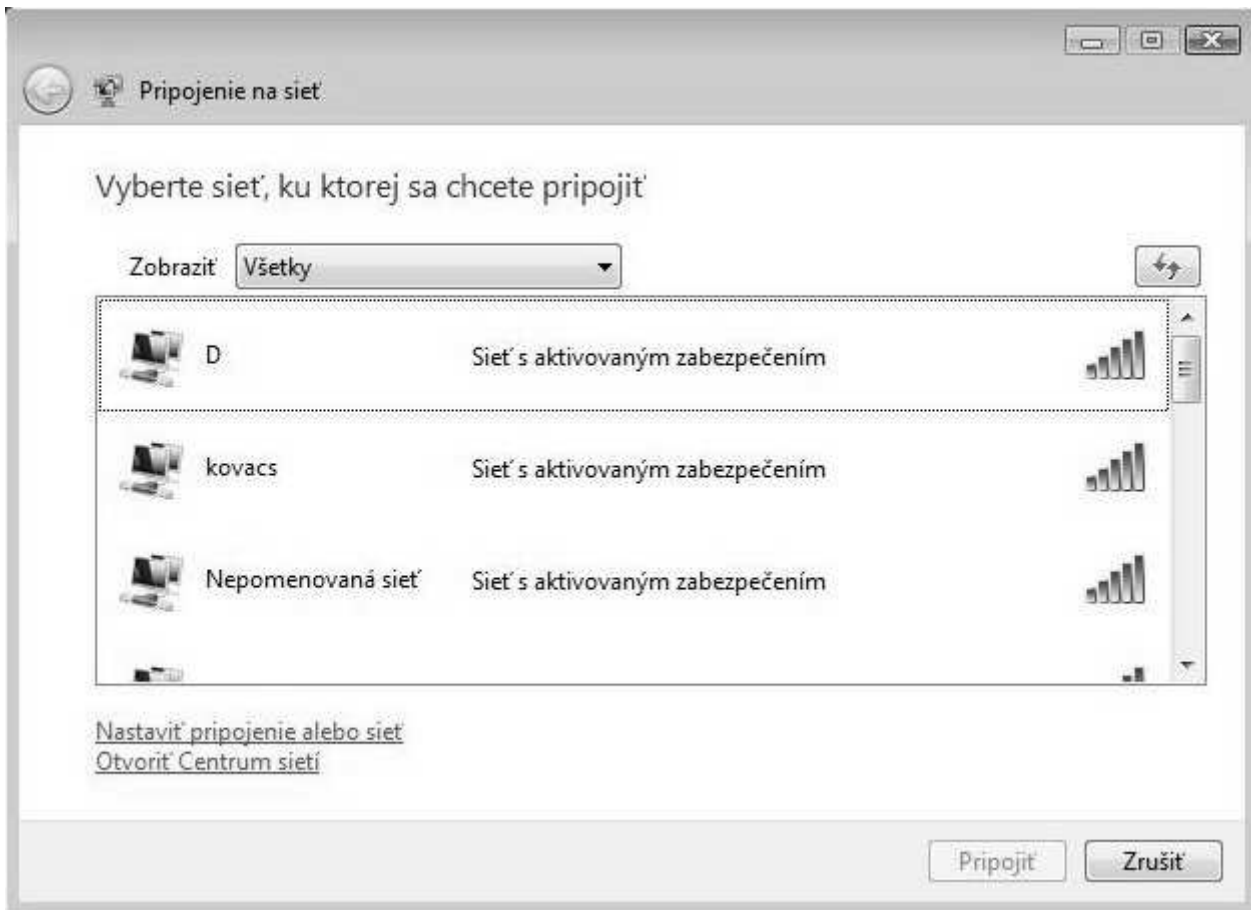


V tomto okienku zrušíme zaškrtnutie **Automaticky použiť moje prihlasovacie meno atď...**
Teda táto voľba zostane vypnutá a potvrdíme **OK**

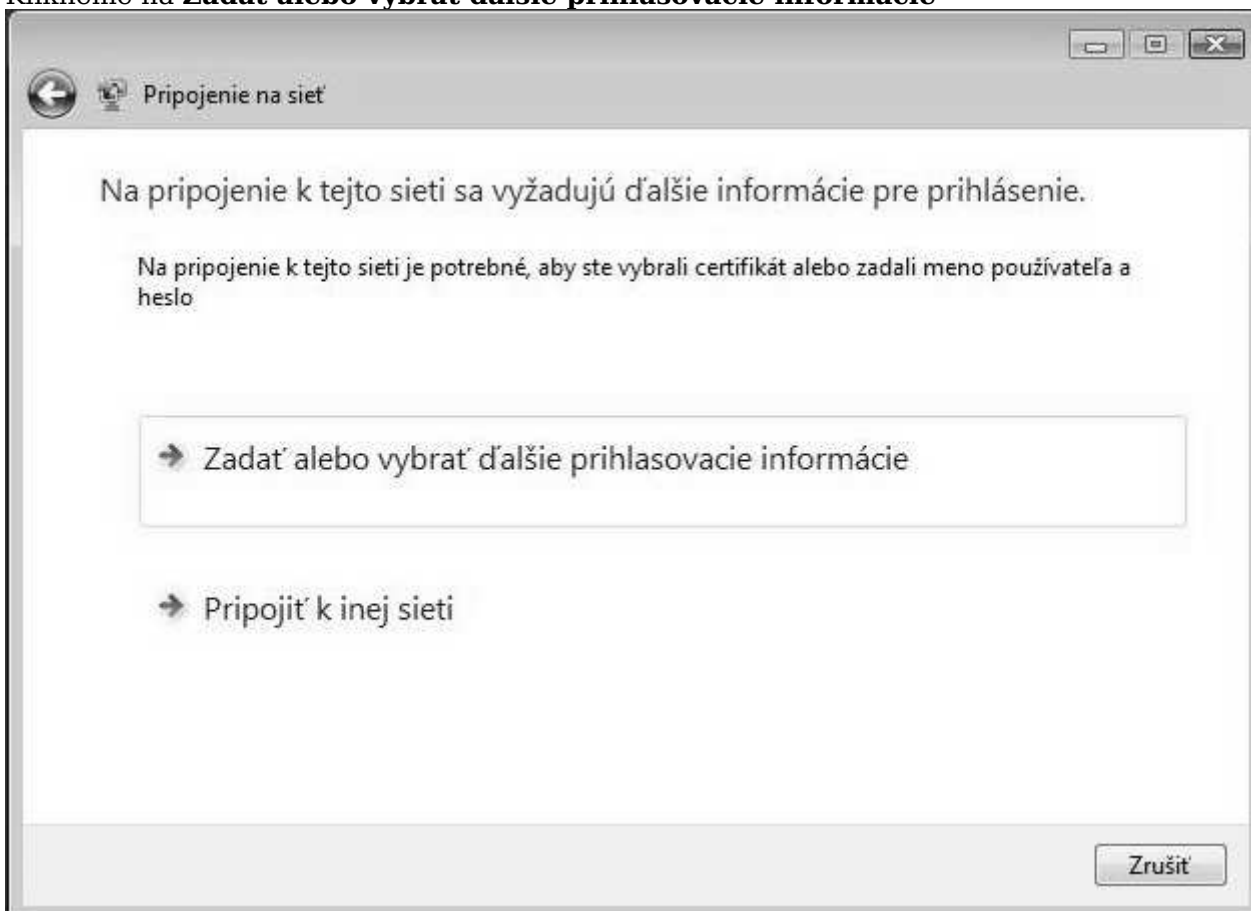


Odklikáme všetky otvorené okná **OK**

A môžeme vyskúšať pripojenie k bezdrôtovej sieti, kliknutím vpravo dole na ikonu bezdrôtových sietí.

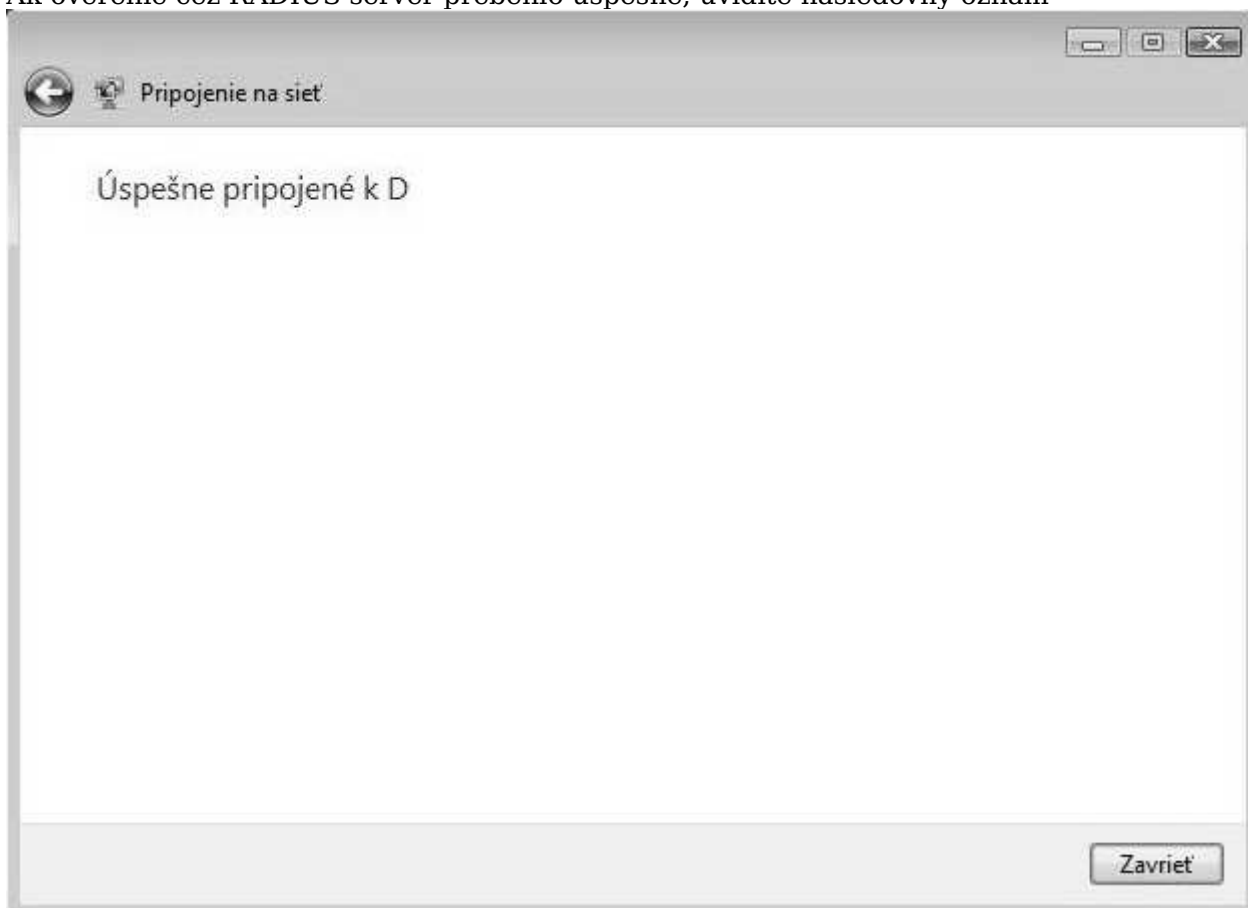


Klikneme na názov siete **SSID** a ak je všetko v poriadku, musíme ešte zadať meno a heslo, teda to isté meno a heslo, ktoré sme nastavili ako užívateľa na RADIUS serveri, v našom prípade **sergej** a jeho **heslo**. Klikneme na **Zadať alebo vybrať ďalšie prihlasovacie informácie**



Tu len zadáme **meno** a **heslo**, rovnaké ako na RADIUS serveri

Ak v tomto kroku vyskočí okno s požiadavkou na potvrdenie certifikátu, tak ho potvrdíme OK. Ak overenie cez RADIUS server prebehlo úspešne, uvidíte nasledovný oznam



Obmedzenie objemu prenesených dát

Nastavenie maximálneho objemu prenesených dát je možné cez menu vo webovom rozhraní ZeroShellu:

Po prihlásení, kliknúť vľavo na **RADIUS**, potom vpravo hore **Accounting**, zaškrtnúť **User Accounting**. Vpravo dole v sekcii **Accounting Classes** nadefinujeme pravidlá pridaním **Add**. Nové pravidlo nejako pomenujeme **Class Name**.

Nastavíme všetky obmedzenia **Traffic, Time, Bandwidth** teda množstvo prenesených dát, čas, max. rýchlosť pripojenia.

Potom pravidlo uložíme **Save**, potom znova vpravo hore **Save**.

Teraz vľavo klikneme na **Users**, potom na meno užívateľa a vľavo dole v sekcii **RADIUS Accounting** vyberíme **Account Class** z rozbalovacieho zoznamu to pravidlo obmedzenia, ktoré chceme prideliť tomuto užívateľovi. Nakoniec uložíme nastavenia pre užívateľa, vpravo hore **Submit**

Test RADIUS servera z počítača so systémom Windows

Ako otestovať funkčnosť RADIUS servera z počítača, ktorý je pripojený do LAN cez switch, ešte pred pripojením klientov cez WiFi?

Test uskutočníme pomocou jednoduchej voľne šíriteľnej utility **NTRadPing**.

Okrem spomínaného programu potrebujeme počítač so systémom Windows (NT, XP, Vista, 7), pripojený do tej istej LAN ako RADIUS server. Stiahneme si NTRadPing a rozbalíme, inštalácia nie je potrebná.

Potom sa prihlásime na RADIUS server a cez webové rozhranie pridáme nový Access Point AP, ktorého IP adresa

je zhodná s počítačom, z ktorého budeme testovať. Ako príklad som zvolil počítač s IP 192.168.1.30

Po prihlásení do webového rozhrania RADIUS servera, klikneme vľavo na **RADIUS** potom hore na

Access Points

a vyplníme jednotlivé políčka podľa obrázka a na koniec klikneme na **Add**.

https://192.168.1.4 - Access Point List - Mozilla Firefox

Access Point List

Access Point Name	IP or Subnet	Shared Secret	<input type="button" value="Add"/>	<input type="button" value="Change"/>	<input type="button" value="D"/>
WindowsXP	192.168.1.30 /	testing123			

	Access Point Name	IP or Subnet	Shared Secret
	WindowsXP	192.168.1.30	testing123

Teraz môžeme na počítači spustiť **NTRadPing** a vyplníme údaje podľa nasledovného obrázka.

Voľba **CHAP** musí byť **vypnutá**. Klikneme dole na tlačítko **Send**.

Ak sa v odpovedi RADIUS servera objaví **response: Access-Accept**, potom daný užívateľ bol úspešne autentifikovaný cez RADIUS server.

NTRadPing Test Utility

RADIUS Server/port: 192.168.1.4 1812

Reply timeout (sec.): 3 Retries: 6

RADIUS Secret key: testing123

User-Name: sergej

Password: ***** CHAP

Request type: Authentication Request 0

Additional RADIUS Attributes:

NTRadPing 1.5 - RADIUS Server Testing Tool
© 1999-2003 Master Soft SpA - Italy - All rights reserved
<http://www.dialways.com/>

ms MASTERSOFT® **DIALWAYS**

RADIUS Server reply:

```
Sending authentication request to server 192.168.1.4:1812
Transmitting packet, code=1 id=0 length=48
received response from the server in 32 milliseconds
reply packet code=2 id=0 length=20
response: Access-Accept
..... attribute dump .....
```

Test RADIUS servera z počítača so systémom linux

Rovnako ako pri testovaní zo systému Windows, aj pre testovanie z počítača so systémom linux je potrebné pridať

IP adresu linuxového počítača do RADIUS servera ako Access Point. Postup je rovnaký, ako už bolo

vyššie spomenuté.

Ak už teda máme linuxový počítač zaregistrovaný v RADIUS serveri ako Access Point, potom budeme potrebovať príkaz **radtest**.

Ak Váš linux neobsahuje príkaz **radtest** je to zrejme preto, že na ňom nemáte nainštalovaný balík **freeradius-utils**.

Pre Debian a Ubuntu stačí použiť príkaz: **apt-get install freeradius-utils**

Použitie príkazu **radtest** je jednoduché:

radtest meno heslo IP-RADIUS-servera port SharedSecret, potom konkrétny príkaz bude vyzeráť nasledovne:

radtest sergej heslo 192.168.1.4 1812 testing123

Ak po zadani príkazu bude výpis vyzeráť podobne, ako na obrázku, potom autentifikácia prebehla úspešne.

```
dolinsky@server:~$ radtest sergej heslo 192.168.1.4 1812 testing123
Sending Access-Request of id 184 to 192.168.1.4 port 1812
  User-Name = "sergej"
  User-Password = "heslo"
  NAS-IP-Address = 192.168.1.29
  NAS-Port = 1812
rad_recv: Access-Accept packet from host 192.168.1.4 port 1812, id=184, length=2
dolinsky@server:~$ █
```

Záver

RADIUS server opísaný v tomto článku je reálne nasadený do prevádzky na škole.

Zoznam WiFi routerov a Access Pointov, ktoré som testoval v spojení s RADIUS serverom:

- CANYON 802.11g Wireless Router CN-WF514
- CANYON CN-WFAP
- AirLive WL-1500R Wireless Router
- UniFi AP 802.11n MIMO
- TP-LINK TL-WR841ND

Na strane klientov mám overené nasledovné operačné systémy a mobilné zariadenia:

- Windows XP
- Windows Vista
- Windows 7
- Linux Ubuntu
- Apple iPhone (iOS)
- Apple iPad (iOS)
- Apple MacBook Air (MacOS X)
- Mobilné zariadenia s OS Android
- Mobilné telefóny s OS Symbian

Zatiaľ som nemal možnosť otestovať pripojenie zariadení s OS Windows Mobile, a BlackBerry.

Zdroje: [ZeroShell-WPA-Enterprise.pdf](#)

[ZeroShell WPA Enterprise](#)

[Wireless Authentication and Encryption with Zeroshell Linux](#)

[Set up Secure Wireless With Zeroshell Linux](#)

[Bezdrátová školní WiFi síť](#)

[WindowsXP-WPA-Enterprise.pdf](#)

[WindowsVista-WPA-Enterprise.pdf](#)

[Windows7-WPA-Enetrprise.pdf](#)

[Linux-WPA-Enterprise.pdf](#)

[Configuring 802.1X Authentication in Linux](#)

[MacOSX-WPA-Enterprise.pdf](#)

[Mac-WPA-Enterprise.pdf](#)

[iPad-WPA-Enterprise.pdf](#)

[iPhone-WPA-Enterprise.pdf](#)

[Android-WPA-Enterprise.pdf](#)

[WindowsMobile-WPA-Enterprise.pdf](#)

[Symbian-WPA-Enterprise.pdf](#)

[BlackBerry-WPA-Enterprise.pdf](#)

[MobileDevices-WPA-Enterprise.pdf](#)

[IAS\(RADIUS\) Server na platforme Windows 2003](#)

[Free RADIUS testing tools](#)