1 Konfigurace menší podnikové sítě

Cíl: Seznámit se s typickou sadou služeb používaných v podnikových sítích a s konfigurací těchto služeb na zařízení MikroTik použitém jako centrální bod.

Vybavení pracoviště: Zařízení MikroTik RB751G-2HnD propojené s vysílačem HP V-M200, dvěma virtuálními servery a dvěma studentskými počítači. Obě klientské stanice obsahují virtuální systém Windows 7 Professional s připojenými USB Wi-Fi adaptéry AirLive. Naintalovaný software: *Winbox.exe*, *FileZilla Client*, *Wireshark*, *putty.exe*, *The Dude server a client.*

Úkoly

1. Seznámit se s nástrojem WinBox a základním nastavením
2. Konfigurace lokální sítě a přístupu do internetu
3. Bezdrátové připojení do vnější sítě - Hotspot
4. Bezdrátové připojení do vniřní sítě - Radius server
5. Nastavení přistup přes VPN
6. Nastavení připojení k serverům z vnější sítě
7. Nastavení připojení k serverům z lokální sítě
8. Konfigurace firewallu
9. Monitoring sítě
10. Uvedení laboratorní úlohy do původního stavu

1.1 Teoretický úvod

Počítačové sítě obecně slouží ke sdílení informací a uživatelské komunikaci. V dnešní době pokročilých síťových služeb a velice výkonných zařízeních lze poměrně snadno vytvářet efektivní síťové struktury. Toho lze s výhodou využít pro potřeby menších či větších podniků.

Na trhu lze nalézt nepřeberné množství jednotlivých síťových prvků, počínaje těmi méně kvalitními, až po výrobky renomovaných společností Cisco System, Avaya a mnohých dalších. V našem případě se zaměříme především na síťové prvky řady RouterBoard od společnosti MikroTik.

Samotná podniková počítačová síť by měla zjednodušovat a urychlovat tok informací, ochranu citlivých dat, zefektivnit výrobní procesy a pomoci snížit finanční nároky spojené s běžným provozem podniku.

1.1.1 Síťové služby

Samotná počítačová síť z pohledu fyzické struktury by nebyla příliš využitelná bez fungujících síťových služeb. Základní doménou počítačových sítí jsou právě informační systémy podniků, ve kterých počítače a počítačové sítě už tradičně plní funkci komunikačního a zpracovatelského subsystému.

1.1.2 Základní požadavky síťových služeb

Následující elementární služby popisují základní funkce, které plní:

- Lan sítě umožňují lepší správu zdrojů - síťové tiskárny, síťově licencovaný software.
- Sítě pomáhají udržovat spolehlivé aktuální informace.
- Sítě pomáhají zrychlit sdílení dat.
- Sítě zlepšují komunikaci mezi pracovními skupinami. Elektronickou poštu a zasílání zpráv umožňuje většina síťových systémů, včetně systému monitorování a plánování projektů a pořádání konferencí v reálném čase.
- Sítě zefektivňují obchodní služby svým klientům. Vzdálený přístup k centrálním datům umožňuje klientům komunikovat přímo se svými dodavateli.
- Monitorování a vzdálené řízení (Remote Control) jiných stanic a prvků sítě.
- Hlasová a obrazová komunikace v síti, umožňující off-line komunikaci mezi uživateli sítě prostřednictvím hlasových a obrazových sekvencí přenášených v síti.

1.1.3 DHCP

Tento protokol z rodiny TCP/IP se používá pro automatickou konfiguraci zařízení připojených do sítě. Názvem DHCP server (Dynamic Host Configuration Protocol) označujeme takový prvek či službu v síti, která jednotlivým hostitelům přiděluje IP adresu, masku sítě, implicitní bránu a téměř vždy i adresu DNS serveru.

1.1.4 DNS

Všechny aplikace, které v Internetu zajišťují komunikaci mezi počítači, používají k identifikaci komunikujících uzlů IP adresu. Pro člověka, jako uživatele, jsou však IP adresy těžko zapamatovatelné. Adresy IPv6 už jsou naprosto nezapamatovatelné. Proto se používá místo IP adresy síťového rozhraní název síťového rozhraní. Pro každou IP adresu máme zavedeno jméno síťového rozhraní (počítače), přesněji řečeno doménové jméno.

1.1.5 VPN

V případě sítí VPN (Virtual Private Network) panuje určitá nejasnost ohledně toho, co je vlastně na síti VPN *virtuální* – je to ono soukromí (privátnost), anebo síť? Následující dva body podávají definici virtuální privátní sítě:

- Topologie virtuální privátní sítě VPN je provozována převážně nad *sdílenou* síťovou infrastrukturou, obvykle nad běžným, veřejným Internetem, přičemž v každém z koncových bodů se nachází alespoň jeden privátní segment sítě LAN.
- Relace sítě VPN běží nad šifrovaným spojením.

Aby mohly síťové segmenty na jednotlivých koncích sítě VPN správně pracovat nad šifrovaným spojením po veřejném Internetu, musí podléhat administrativní kontrole stejného podniku, jenž danou virtuální síť provozuje. Prakticky vzato to znamená, že koncové směrovače sítě VPN musí podléhat společné bezpečnostní a provozní správě; tyto směrovače v koncových bodech virtuální sítě VPN musí především pracovat s jedním společným schématem šifrování.

1.1.6 QoS

Internetové sítě neměly hned ze začátku obrovská, široce otevřená a přitom laciná datová potrubí, kterými by kdokoli kdykoli mohl okamžitě přenášet jakákoli data. Nástrojem QoS (Quality of Service) uplatníme v případě, kdy chceme upřednostnit jeden typ síťového provozu proti jinému, nebo zajistit určité aplikaci jasné kvalitativní parametry přenosu.

Běžná aplikace, například internetový prohlížeč, je poměrně odolná vůči výpadku či změně pořadí jednoho nebo i několika paketů. Protokol TCP, který pracuje nad IP protokolem, zajistí opětovné odeslání takto ztracených paketů, případně zajistí jejich správné pořadí.

Existují však aplikace, pro které kvalitativní parametry přenosu jsou důležité, nebo enormně důležité. Typickými aplikacemi, pro které jsou kvalitativní parametry přenosu podstatné, jsou hlasové přenosy, přenosy videa a podobné. K nim v poslední době přibývají i klíčové podnikové aplikace.

1.1.7 Firewall

Firewall je bránou, která selektivně rozhoduje, co smí a nesmí do privátní sítě vstoupit, nebo ji naopak opustit. Aby mohl firewall tuto úlohu naplňovat, musí být jedinou branou mezi chráněnou privátní sítí a vnějším světem. Firewall tedy řídí komunikaci z vnitřní sítě směrem ven, komunikaci soustřeďuje do jednoho uzlu, odfiltrovává nebezpečné služby, blokuje nepřátelské monitorování sítě apod. V roli firewallu může sloužit i normální směrovač; pouze musí být pro tuto činnost zvlášť nakonfigurován.

Veškerá komunikace síťových služeb probíhá skrze tzv. porty. Port se dá představit jako přepínač v telefonní ústředně. Jelikož ale při připojení PC do sítě je potřeba využívat více síťových služeb než jen jednu, máme k dispozici celkem 65535 portů, což znamená, že současně můžeme využívat služby http, ftp, ssh, smtp, pop... a pořád nám zbývá k dispozici mnoho a mnoho volných portů. A právě přes tyto porty je možné vést útok.

Při budovaní firewallu je potřeba si ujasnit míru zabezpečení a především se dohodnout na použitém řešení. Ve většině firem je k dispozici dokument, jenž řeší bezpečnostní politiku a tudíž při připojení do Internetu je potřeba, aby parametry připojení a použité ochrany tomuto dokumentu bezesporu vyhovovaly.

V dnešní době již firewall neplní jen základní funkci ochrany před únikem dat či napadením lokální sítě. Dnešní moderní firewall přináší komplexní řešení v oblastech napojení do Internetu a lokální sítě. Tyto komplexní služby dokáží plnit funkce antivirové ochrany, optimalizace připojení, problémy s IP, zabezpečené komunikace, sdílení přístupu k internetu apod.

1.1.8 VLAN

Virtuální sítí (VLAN) – má namysli transparentní propojení dvou nebo více lokálních sítí (LAN) na úrovni druhé síťové vrstvy. Lokální sítě mohou být přitom od sebe fyzicky vzdáleny a na jejich propojení přitom může být použita i jiná technologie, než je použita v samotných LAN. Vzájemná komunikace členských hostitelů sítě VLAN probíhá stejně, jako by byly připojeny ke stejnému síťovému vodiči, přestože mohou být ve skutečnosti umístěny v libovolném počtu různých fyzických sítí LAN. Virtuální sítě VLAN tvoří navíc domény nesměrového vysílání, a proto mohou jejich členové využívat konektivitu, sdílené služby a zabezpečené spojení s fyzickými sítěmi LAN.

1.1.9 WLAN

Zkratka WLAN znamená přesně to, co naznačuje – jedná se o síť LAN, ke které můžeme přistupovat i bez fyzického připojení k serveru, přepínači, rozbočovači, či jinému síťovému zařízení. Bezdrátové sítě WLAN vysílají a přijímají data vzduchem, prostřednictvím přenosu rádiových vln, a nevyžadují tak ke své činnosti klasická připojení s běžnými vodiči. Sítě WLAN získávají stále větší oblibu v řadě specializovaných oblastí, jako je například péče o zdraví, maloobchod, výrobní sféra, skladové hospodářství nebo akademická sféra. Ve všech těchto oblastech lidské činnosti vede vysílání a příjem informací v reálném čase mezi chytrými mobilními zařízeními a notebooky na jedné straně a centralizovanou sítí na druhé straně ke zvýšení produktivity práce. Proto je uznávané také jako obecné řešení síťového připojení pro široké spektrum uživatelů z podnikatelské sféry.

Základem technologie pro komunikaci bezdrátových sítí WLAN je standard IEEE 802.11; pracovní skupina IEEE 802.11 byla založena začátkem devadesátých let a jejím úkolem byl vývoj globálního standardu pro bezdrátové sítě LAN, pracující v nelicencovaném frekvenčním pásmu 2,4 GHz a 5 GHz.

1.1.10 NAT

Překlad adres (Network Adress Translation) poskytuje metodu překladu adres počítačů protokolu IPv4 (Internet Protocol version 4) v jedné síti na adresy IPv4 počítačů v jiné síti. Směrovač IP s povoleným překladem adres (NAT) nasazený na hranici setkání privátní sítě (například podniková síť) s veřejnou sítí (například Internet) umožňuje pomocí této služby překladu přístup počítačů v privátní síti k počítačům ve veřejné síti.

1.1.11 Radius server

RADIUS - Remote Authentication Dial-In User Service - je název síťového protokolu, který umožňuje ověření vzdálených uživatelů a jejich připojení k místní síti. Protokol RADIUS je nasazen ve formě serverů RADIUS, které mohou nabývat podob malých serverů v síti malé (domácí) kanceláře pro pár uživatelů, až po velké podnikové servery obsluhující tisíce uživatelských připojení.

Protokol RADIUS často používají také systémy VoIP, kdy se vzdálení klienti, jako např. broadbandové telefony, připojí k serveru VoIP pomocí bezpečné technologie. Příkladem může být protokol SIP (Session Initiation Protocol) připojující se k serveru SIP.

1.1.12 RouterOS

Jejím hlavním produktem je routerový operační systém, založený na platformě Linux v3.3.5, pojmenovaný RouterOS. Systém se vyznačuje především poměrně snadnou konfigurací, robustností a možností implementace na široké spektrum zařízení. Router OS nabízí velkou paletu služeb – firewall, routing, forwarding, VPN, bezdrátové sítě, hotspot, QoS a mnoho dalších nástrojů určených ke správě sítě. Podpora API je výhodou především pro nasazení v rozlehlých podnikových sítích pro možnost vytvářet své vlastní nástroje.

Existuje více způsobů, jakými lze systém konfigurovat. Počínaje lokálním přístupem přímo na instalovaném zařízení a serialovou konzolí. Samozřejmostí je podpora vzdálené správy pomocí protokolu Telnet a bezpečnějšího SSH. Pro přehlednější úpravy lze použít webové rozhraní a především aplikaci Winbox.

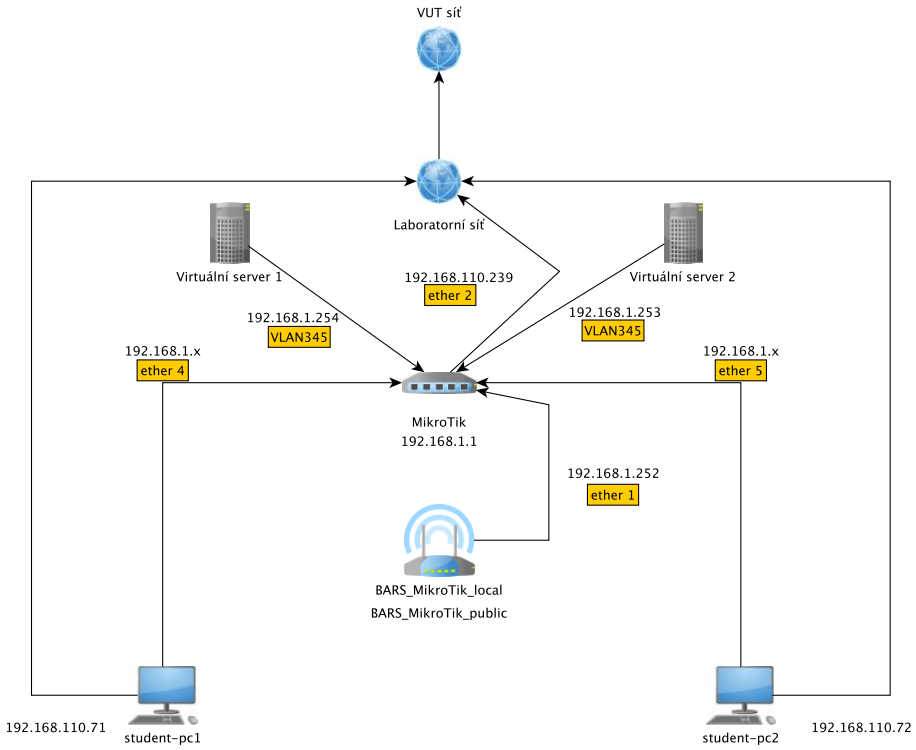

Figure 1: Příklad struktury reálné sítě

1.2 Postup řešení

1.3 Úkol č.1: Seznámení se s nástrojem WinBox a základní nastavení routeru

1. Spusťte virtualizační prostředí *Oracle VM VirtualBox*.
2. U virtuálního systému *WIN7* zkontrolujte nastavení síťové karty: Oranžové ozubené kolečko *Settings* → záložka *Network* a nastavte dle obrázku níže. (Pro PC21 volte VLAN344 a pro PC22 volte VLAN345).

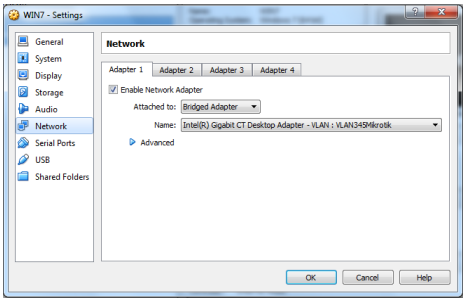

Figure 2: Nastavení virtuální síťové karty

3. Přihlašte se do virtuálního systému Windows 7 (heslo: ***student***) a spusťte aplikaci *winbox.exe*. Pokud není aplikace na ploše, stáhněte ji z http://www.mikrotik.com/download.
4. V záložce *Neighbors* klikněte na MAC adresu routeru, do políčka *login* zadejte ***admin***. Políčko *password* ponechte prázdné a přihlašte se pomocí tlačítka *Connect*.
5. Po přihlášení uveďte router do továrního nastavení následujícím postupem: *System* → *Reset Configuration* → *No Default Configuration* → *Reset Configuration*.
6. Po opětovném přihlášení pro lepší přehlednost nastavte jméno zařízení: *System* → *Identity* a zvolte libovolný název.
7. Zabezpečte zařízení heslem: *System* → *Password*.

Nyní jste schopni svůj router rozpoznat i v případě více zapojených zařízení MikroTik do sítě a zároveň je chráněn heslem proti nedovolnému přístupu.

1.4 Úkol č. 2: Konfigurace lokální sítě a přístupu do internetu

1. Vytvořte bridge: *Bridge* → *"+"*, poté do pole *Name* vložte vhodný název a potvrďte tlačítkem *OK*.

2. Oba porty do kterých jsou připojeny klientské stanice je nutné přidat do bridge: *Bridge* → záložka *Ports* → *"+"*, poté v poli *Interface* zvolte jednotlivě konkrétní porty (dle schématu v teoretickém úvodu) a v poli *Bridge* vyberte vámi vytvořený bridge a potvrďte *OK*.

3. Nyní je potřeba vytvořenému bridge přiřadit IP adresu a rozsah: *IP* → *Addresses* → *"+"*, poté do pole *Address* vepište ***192.168.1.1/24*** a v poli *Interface* vyberte příslušný bridge a potvrďte *OK*. Síť si zařízení dopočítá samo.

4. Přejdeme k nastavení DHCP serveru: *IP* → *DHCP Server* → *DHCP Setup* → v zobrazeném okně vyberte vytvořený bridge a pokračujte *Next*. V dalším okně se zobrazí adresový rozsah - nechte beze změny, stejně jako následujícím okně gateway. V dalším okně vzhledem ke staticky nakonfigurovaným zařízením v síti nastavte rozdávané adresy na ***192.168.1.2 - 192.168.1.200***. V následujícím okně nastavte DNS servery na ***8.8.8.8*** a ***8.8.4.4***. Pole *Lease Time* v následujícím okně změnte na ***00:00:10***.

5. Pro rychlejší získání IP adresy z DHCP serveru zadejte postupně následující příkazy v příkazové řádce virtuálního systému: ***ipconfig /release*** a ***ipconfig /renew***.

6. Nyní ověřte dostupnost routeru a počítačů mezi sebou pomocí nástroje ping.

7. Pro přístup do vnější sítě (nativní laboratorní síť) musíme získat adresu z vnější sítě: *IP* → *DHCP Client* → *"+"* v okně *Interface* zvolíme příslušný port dle schématu v teoretickém úvodu a potvrdíme *OK*.

8. Pro spojení lokální a vnější sítě použijeme NAT: *IP* → *Firewall* → *NAT* → *"+"* v záložce *General* v poli *Chain* zvolíme ***srcnat*** a v poli *Out. Interface* zvolíme ***ether2***. Přepneme na záložku *Action* a v poli *Action* vybereme hodnotu ***masquerade***, potvrdíme *OK*. Nyní by měla měl být z obou počítačů přístupná jak nativní laboratorní síť tak připojení k internetu.

9. Ověřte dostupnost nástrojem ping na vnější adresu routeru, adresu nativních počítačů a rychlost připojení k internetu na adrese http://www.speedtest.net.

1.5 Úkol č. 3: Bezdrátové připojení do vnější sítě - Hotspot

1. Vzhledem k tomu že Access Point (HP V-M200) již vysílá pod SSID: *BARS_MikroTik_public*, které je přednastaveno na VLAN10, tak nyní tuto VLAN musíme vytvořit v routeru: *Interfaces* → *VLAN* → *"+"*, poté v poli *Name* vyplňte vhodný název a v poli *VLAN ID* vyplňte ***10***. Nakonec v poli *Interface* vyberte port na který je dle schématu připojeno AP.

2. Nyní na tuto VLAN vytvoříme Hotspot: *IP* → *Hotspot* → záložka *Servers* → *Hotspot Setup* v poli *HotSpot Interface* vyberte vámi vytvořenou vlan.

V dalším okně ponechte IP adresu beze změny stejně tak v následujícím okně rozsah rozdávaných adres. V okně s importem certifikátu vyberte možnost ***none***. IP adresu SMTP serveru ponechte na hodnotě ***0.0.0.0***. Do pole *DNS Servers* v následujícím okně vyplňte ***8.8.8.8*** a ***8.8.4.4***. Pole *DNS Name* ponechte prázdné. V posledním okně vyplňte libovolné heslo pro správce hotpostu v poli *Password for the User*.

3. Pro přístup návštěvníků pouze do sítě internet je vhodné použít profil *Trial*: *IP* → *Hotspot* → záložka *Server Profiles* zde vyberte automaticky vytvořený profil *hsprof1* → záložka *Login* → v sekci *Login By* zatrhněte *Trial* a potvrďte *OK*.

4. Nyní povolíme sdílení účtu *Trial* pro více klientů: *IP* → *Hotspot* → záložka *User Profiles* zde vyberte automaticky vytvořený profil *default* → záložka *General*, v poli *Shared Users* vyplníme číslo ***5*** a potvrdíme *OK*.

5. Do obou klientských stanic připojte USB Wi-Fi adaptéry připravené na stole. Adaptéry lze pohodlně připojit z levé strany LCD.

6. Ověřte zda virtuální systém úspěšně namapoval USB adaptér AirLive: *START* → *Ovládací panely* → *Centrum síťových připojení a sdílení* → *Změnit nastavení adaptéru*.

7. Pro jednodušší obsluhu zakažte kabelové připojení: Pravým tlačítkem myši na *Připojení k místní síti* → *Zakázat*.

8. Připojte se k síti *BARS_MikroTik_public*, spusťte webový prohlížeč a otevřete libovolnou webovou stránku. Budete přesměrováni na přihlašovací stránku vámi vytvořeného hotspotu. Pro využití omezeného přístupu do sítě internet, klikněte na odkaz v horní části *click here*.

9. Ověřte dostupnost počítačů mezi sebou pomocí nástroje ping.

10. Ověřte dostupnost některého ze světových serverů pomocí nástroje ping.

11. Ověřte dostupnost privátní sítě.

12. Obvykle nechceme aby volně příchozí lidé měli přístup do privátní sítě, proto je nutné vytvořit ve firewall následující pravidlo: *IP* → *Firewall* → záložka *Filter Rules* → "+" → záložka *General* v poli *Chain* vyberte ***forward***, v poli *Src. Address* vyplňte ***10.5.50.0/24*** (rozsah adres který jste použili pro hotospot), do pole *Dst. Address* ***192.168.1.0/24*** (rozsah lokální sítě). Přepneme na záložku *Action*, v poli *Action* vybereme ***reject*** a nakonec v poli *Reject With* vybereme ***icmp admin prohibited***.

13. Nyní ověřte funkčnost pravidla pomocí nástroje ping na adresu ***192.168.253*** (lokální FTP server).

14. Abychom omezili přístup na router (bránu) vytvoříme nové pravidlo s tím rozdílem, že v poli *Chain* vybereme ***input*** a zbytek nastavíme jako v předchozím pravidle.

15. Nyní ověřte funkčnost pravidla pomocí nástroje ping a otevřením webového rozhraní MikroTiku pomocí webového prohlížeče na adrese ***192.168.1.1***.

16. Né vždy je vhodné návštěvníkům povolit plnou dostupnost linky a proto vytvoříme omezení: *IP* → *Hotspot* → záložka *User Profiles* → položka *default* a v poli *Rate Limit (rx/tx)* nastavte vhodnou hodnotu např.: ***4M/4M*** a potvrďte *OK*.

17. Nyní ověřte pomocí http://www.speedtest.net zda omezení funguje.

1.6 Úkol č. 4: Bezdrátové připojení do vniřní sítě - Radius server

1. Na jednom z virtuálních strojů opět povolíme kabelové připojení a odpojíme bezdrátovou síť *BARS_MikroTik_public*.

2. Analogicky jako v předešlém úkolu přiřadíme VLAN na Wi-Fi vysílání, konkrétně na *BARS_MikroTik_local* namapujeme VLAN20 s tím rozdílem, že v poli *VLAN ID* vyplníte ***20***.

3. Jako v předchozím úkolu vytvořte hotspot na VLAN pomocí průvodce s tím rozdílem, že v v poli *HotSpot Interface* vyberete nově vytvořenou vlan a v poli *Local Address of Network* vyplňte adresu ***10.5.51.1/24***, vše ostatní ponechte beze změny.

4. Jelikož pro ověřování uživatelů budeme používat lokální Radius server, musíme si jej vytvořit: *Radius* → *"+"* → v poli *Service* vybereme položku ***hotspot***, v poli *Address* vyplníme IP adresu ***192.168.1.1***, v poli *Secret* vyplníme libovolné heslo a potvrdíme *OK*.

5. Pro správu databáze uživatelů a jednotlivých nástroju Radius serveru použijeme *MikroTik User Manager* dostupný na ***192.168.1.1/userman***. Příhlásíme se pomocí defaultně nastavených údajů ***admin/bez hesla***.

6. Nyní přiřadíme databázi uživatelů konkrétní server/router: Záložka *Routers* → *Add* → v poli *Name* zvolíme vhodný název, v poli *IP address* vyplníme ***192.168.1.1*** a v poli *Shared secret* vyplňte heslo zadané při vytváření Radius serveru.

7. Pro přehlednější správu více uživatelů vytvořte profil: Záložka *Profiles* → *"+"* a do pole *Name* vepište vhodný název (např. studenti) a potvrdíme *Create*.

8. Nyní lze vytvořit uživatele: Záložka *Users* → *Add* → *One* → do polí *Username Password* vepište ***student1*** a v poli *Assign profile* vyberte vámi vytvořený profil. Přidejte tlačítkem *Add*.

9. Nyní povolíme hotspot serveru ověřování pomocí Radius serveru: *IP* → *Hotspot* → záložka *Server Profiles* → vybereme profil *hsprof2* → záložka *RADIUS*, zatrhneme checkbox u *Use RADIUS* a potvrdíme *OK*.

10. Na druhém počítači se připojte se k síti *BARS_MikroTik_local*, spusťte webový prohlížeč a otevřete libovolnou webovou stránku. Budete přesměrováni na přihlašovací stránku vámi vytvořeného hotspotu.

11. Přihlašte se pomocí účtu vytvořeného v User Manageru.

12. Ověřte dostupnost některého ze světových serverů pomocí nástroje ping.

13. Ověřte dostupnost privátní sítě.

1.7 Úkol č. 5: Konfigurace vzdáleného přístupu - VPN

1. Abychom snadno určili kdo je připojen přes VPN a mohli lépe spravovat jednotlivé uživatele, vytvoříme nový IP Pool: *IP* → *Pool* → *"+"* do pole *Name* vepište ***VPN_pool***, do pole *Addresses* vepište rozsah IP adres ***192.168.1.201-192.168.1.220***.

2. Nyní vytvoříme profil který definuje jednotlivé parametry pro připojení: *PPP* → záložka *Profiles* → *"+"*. V poli *Name* vyplníme ***PPTP_profile***, do pole *Local Address* vepíšeme vnitřní adresu routeru ***192.168.1.1***, v poli *Remote Address* vybereme námi nakonfigurovaný pool ***VPN_pool***. Dále vyplňte IP adresu ***8.8.8.8*** DNS serveru v poli *DNS Server*. V záložce *Protocols* → sekce *Use Encryption* vyberte ***yes*** a potvrdíme *OK*.

3. Nezbytnou součástí je vytvoření profilu pro jednotlivé uživatele: *PPP* → záložka *Secrets* → *"+"*. Do polí *Name* a *Password* vyplníme vhodné jméno (např.***student2***). V poli *Service* vybereme ***pptp***, v poli *Profile* vybereme námi vytvořený ***PPTP_profile*** a potvrdíme *OK*.

4. Nastal čas abychom zapnuli samotný PPTP server: *PPP* → záložka *Interface* → *PPTP Server* → zatrhneme checkbox *Enabled* a v poli *Default Profile* vybereme námi vytvořený ***PPTP_profile***, nakonec potvrdíme *OK*. Server běží na "pozadí", proto nečekej žádnou potvrzovací hlášku nebo řádek s jeho aktivitou.

5. Aby byla přes VPN dostupná celá síť a ne pouze router je nutné změnit na lokálním rozhraní následující: *Bridge* → námi vytvořený bridge → záložka *General* → v poli *ARP* vyberte ***proxy-arp***.

6. Na jednom z virtuálním systému upravíte nastavení síťové karty podobně jako na začátku úlohy: Oranžové ozubené kolečko *Settings* → záložka *Network* v poli *Name* změňte na ***VLAN:LAN*** a potvrďte *OK*. Tímto nasimulujeme přístup z vnější sítě (nativní laboratorní). Zároveň odpojíme počítač od bezdrátové sítě.

7. Nyní ve virtuálním Windows 7 nastavíme VPN připojení: *START* → *Ovládací panely* → *Centrum síťových připojení a sdílení* → *Nastavit nové připojení nebo síť* → *Připojit k firemní síti* → *Použít moje připojení k Internetu (VPN)*, do pole *Internetová adresa* vepište vnější IP adresu routeru (brány) ***192.168.110.239***. Do pole *Název cíle* vyplňte vhodný popis vytvářeného spojení. Ostatní nastavení ponechte bez změny a pokračujte tlačítkem *Další*.

8. Nyní vyplňte údaje k přihlášení uživatele: Do polí *Uživatelské jméno* a *Heslo* vyplňte ***student2*** nebo vámi volitelně zadané při konfiguraci uživatele a vyzkoušejte tlačítkem *Připojit*.

9. Pomocí nástroje *ipconfig* zkontrolujte zda jste dostali IP adresu ze správného rozsahu.

10. Ověřte dostupnost některého ze světových serverů pomocí nástroje ping.

11. Ověřte dostupnost privátní sítě.

1.8 Úkol č. 6: Nastavení připojení k serverům z vnější sítě

Dle schématu v teoretickém úvodu vidíme v síti předpřipravené dva virtuální servery. Jeden z nich, konkrétně ***192.168.1.254*** nastavíme tak, aby byl dostupný z vnější sítě.

1. Jelikož aplikace pro FTP spuštěná na serveru číslo 1. naslouchá na portu 20 a 21, přesměrujeme nyní tyto porty z při dotazu z vnější sítě do vnitřní: *IP* → *Firewall* → záložka *NAT* → *"+"* → záložka *General*, v poli *Chain* vybereme ***dstnat***, do pole *Dst. Address* vepíšeme adresu brány z vnější sítě ***192.168.110.239***, v poli *Protocol* vybereme ***6 (tcp)*** a jako *Dst. Port* vepíšeme ***20-21***. Dále v záložce *Action* v poli *Action* vybereme ***dst-nat***, do pole *To Addresses* vepíšeme adresu požadovaného serveru, tedy ***192.168.1.254***, do pole *To Ports* port na kterém kterém server naslouchá, tedy ***20-21*** a potvrdíme *OK*.

2. Otevřete aplikaci *FileZilla Client* umístěnou na ploše a vyzkoušíme přípojení k ftp serveru. U daného počítače mějte nastavenou virtuální síťovou kartu stejně jako při testování VPN.

3. Spusťte také aplikaci *Wireshark* pro zachytávání síťového provozu. Nastavte zachytávání na virtuálním ethernetu: Šedivé ozubené kolečko v horní liště, vyberte *Připojení k místní síti* a spusťte tlačítkem *Start*.

4. Zároveň si vyfiltrujte pouze ftp (příkazy): Kliknutí do řádku *Apply a display filter* a vepsaní ***ftp*** a potvrzením modrou šipkou vpravo.

5. Nyní zkuste navázat spojení se serverem pomocí *FileZilla* a zadáním přednastaveného účtu do kolonek *Hostitel* - ***192.168.110.239***, *Uživatelské*

jméno - ***student1***, *Heslo* - ***student1***. Pole port ponechte prázdné a připojte se tlačítkem *Rychlé připojení*.

6. V aplikaci Wireshark si prohlédněte jak probíhá komunikace mezi klientem a serverem při ověřování uživatele. Zjistěte uvítací zprávu poslanou serverem.

7. V aplikaci Wireshark změňte filtr na ***ftp-data***.

8. Z ftp serveru stáhněte zip soubor *bars_prednasky.zip* do počítače přetažením. Sledujte rychlost přenosu a průběh komunikace a přenosu dat ve Wireshark.

9. Ne vždy je žádoucí vytěžování konektivity jedním klientem, nebo stahování objemných souborů plnou rychlostí, vyzkoušíme si nastavení omezení: *Queues* → záložka *Simple Queues* → "+" do pole *Name* vyplňte ***FTP***, do pole *Target* vepište ***0.0.0.0/24***, v poli *Dst.* vyplňte ***192.168.1.254***. Tím jsme nastavili zdrojové a cílové IP adresy a název omezení.

10. Nyní nastavíme samotné parametry omezení: *Max Limit* u *Target Upload* i u *Target Download* nastavíme na ***1M***. V obou polích pro *Burst Limit* nastavíme ***50M***. *Burst Threshold* ponecháme beze změny. U obou polí *Burst Time* nastavíme ***1000*** a potvrďte tlačítkem *Apply* a přepněte se do záložky *Traffic*. Tím jsme nastavili že pokud parametry překročí po stanovený čas hodnotu 50MB, bude linka "ořezána" na 1MB.

11. Nyní zkuste znovu přenést data z FTP serveru na virtuální počítač a sledujte jak v se mění rychlost stahování na grafu generovaném MikroTikem a na hodnotách zobrazovaných FileZilla klientem.

12. Nakonec si obdobně jako při přesměrování portů pro FTP server zkuste vytvořit pravidlo pro přesměrování na webový server na adrese ***192.168.1.254*** a naslouchajícím na portu ***80***.

13. Nyní ve webovém prohlížeči počítače na kterém jste testovali FTP, zkuste zadat adresu ***192.168.110.239*** a vyzkoušet tak funkčnost přesměrování.

1.9 Úkol č. 7: Nastavení připojení k serverům z lokální sítě

Nyní si zkusíme připojení z lokální sítě na lokální FTP server. Virtuální síťová karta musí být nastavena na (VLAN344 nebo VLAN345) aby dostala adresu z privátního rozsahu.

1. Otevřete aplikaci *FileZilla Client* a připojete se obdobně jako v předešlém úkolu na FTP server **192.168.1.253** se přihlašovacími údaji ***student1/student1***.

2. Analogicky jako v předešlém úkolu stáhněte soubor *bars_prednasky.zip* do virtuálního počítače a porovnejte čas stahování souboru z lokální a z veřejné (laboratorní nativní) sítě. Diskutujte důvod rozdílu.

3. Na MikroTiku lze pomocí grafů sledovat vytíženost jednotlivých fyzických i virtuálních rozhraní nebo CPU a RAM samotného zařízení. Je však koncipováno do průměru po 5. minutách, což není pro působnost v laboratorní úloze mnoho. Vegenerování grafu si však zkusíme na *queues FTP* které jsme předtím vytvořili: *Tools* → *Graphing* → záložka *Queue Rules* → *"+"*. Zde v poli *Simple Queue* vybereme námi vytvořenou ***FTP***, ostatní ponecháme beze změny a potvrdíme *OK*.

4. Graf si můžete zobrazit po zadaní URL ***192.168.1.1/graph*** v internetovém prohlížeči a kliknutím na hypertextový odkaz *FTP*.

5. Nyní si zkuste upravit defaultně zobrazovaný soubor webovým serverem *index.html*, který je dostupný na ftp serveru (domovský adresář FTP serveru je napamován na zdrojový adresář webového serveru).

6. Soubor si stáhněte na virtuální počítač, otevřete pomocí *Poznámkového bloku* a upravte tak, aby se zobrazoval vámi vhodně vložený krátký text (nadpis). Zároveň vložte graf generovaný MikroTikem jako obrázek, který se bude automaticky obnovovat při načtení stránky. (Potřebnou pomoc najdte např. na: http://www.jakpsatweb.cz/obrazky.html.

7. Nyní vámi upravený *index.html* nahrajte zpět na FTP server a ověřte funkčnost pomocí webového prohlížeče.

1.10 Úkol č. 8: Firewall

Nyní si zkusíme nastavit jednoduchý firewall. Poměrně bezpečnou a v menších sítích používanou metodou je "povol co znám, ostatní zakaž".

1. Povolíme nyní porty které jsme přidali do *NAT*, konkrétně ***20, 21, 80***: *IP* → *Firewall* → záložka *Filter Rules* → *"+"*, v poli *Chain* vybereme ***input***, do pole *Dst. Address* vepíšeme IP adresu brány z vnější sítě ***192.168.110.239***, v poli *Protocol* vybereme ***6 (tcp)***, v poli *Dst. Port* vyplníme ***80***, v záložce *Action* v poli *Action* vybereme ***accept*** a potvrdíme *OK*.

2. Analogicky proveďte pro porty ***20,21***

3. Ověřte nyní funkčnost portu 23 - telnet. Spusťte aplikaci na ploše *putty.exe*, v sekci *Connection type* vyberte ***Telnet***, do pole *Host Name* vepište již dobře známou IP adresu ***192.168.110.239*** a zkuste se připojit tlačítkem *Open*.

4. Přihlašte se pomocí login:***admin*** a vámi zvoleného hesla k administraci routeru. Po úspěšném přihlášení jste schopni MikroTik konfigurovat pomocí konzole.

5. Nyní zakážeme všechny porty, vyjma těch, které jsme výše povolili: *IP* → *Firewall* → záložka *Filter Rules* → *"+"*, v poli *Chain* vybereme ***input***, do pole *Dst. Address* vepíšeme IP adresu brány z vnější sítě ***192.168.110.239***, v záložce *Action* v poli *Action* vybereme ***reject*** a potvrdíme *OK*.

6. Ukončete a znovu spusťe aplikaci *putty.exe* a zkuste se pomocí telnet příhlásit na router. Připojení by se nemělo povést. Zkontrolovat můžete i počet bytů a packetů u vytvořeného pravidla ve firewallu, které narůstají s pokusy o připojení.

1.11 Úkol č. 9: Monitoring

Důležitou součástí správy počítačové sitě je monitoring. Je vždy lepší problémům předcházet, než řešit akutní problémy. Jedním z monitorovacích nástrojů je The Dude od společnosti MikroTik. Vyzkoušíte si základní konfiguraci v tomto prostředí.

1. Vzhledem k tomu že v aktuální verzi RouterOS není možné nainstalovat server The Dude, je nutné pustit lokální server na virtuálním sytému pomocí ikony na ploše *The Dude*.

2. Dvojím kliknutím na ikonu blesku vlevo nahoře se Vám zobrazí okno s definicí připojení k serveru. V poli *Režim* zvolte ***místní***, v poli *Uživatelské jméno* ponechte ***admin***, pole *Heslo* ponechte prázdné.

3. Nyní dvojklikem otevřete záložku *Network Maps* → *"+"* → v záložce *Obecné* vyplňte pole *Název* a potvrďte *OK*.

4. Otevřete vámi vytvořenou mapu sítě.

5. Pravým tlačítkem myši na volnou plochu můžete přidávat jednotlivé části sítě. Nyní přidejte router: *Přidat zařízení*, v poli *Adresa* vyplňte ***192.168.1.1***, v poli *Uživatelské jméno* vyplňte **admin**, v poli *Heslo* vyplňte vámi zvolené heslo k administraci routeru. Zatrhněte checkbox *RouterOS* a pokračujte tlačítkem *Další*. V dalším okně použijte tlačíko *Detekce*, vyberte všechny nabízené služby a potvrďte *OK*.

6. Obdobně jako v předešlém úkolu přidejte i další zařízení v sítí a zkuste tak napodobit schéma uvedené v teoretickém úvodu.

7. Spojte jednotlivá zařízení pomocí *Přidat spojení* a tahem mezi dvěma konkrétními zařízeními.

8. Najetím kurzorem myši nad jednotlivá zařízení zobrazíte grafy sledovaných služeb. Detailněji je lze zobrazit ve vlastnostech konkrétního zařízení.

9. Po sestavení monitorované sítě zkuste znovu přenos souborů z/na FTP server a sledujte tok dat, popřípadě vytížení jednotlivých prvků v síti.

1.12 Úkol č. 10: Uvedení laboratorní úlohy do původního stavu

1. Smažte nastavené VPN spojení z virtuálních systémů.
2. Zkontrolujte zda na FTP serverech jsou testovací soubory.
3. Smažte stáhnuté testovací soubory z virtuálních systémů.
4. Na lokální webový server nahrajte původní soubor *index.html*, popřípadě vytvořte nový pouze s jednoduchým vzkazem ve formátu nadpisu.
5. V zařízení MikroTik smažte databázi uživatelů RADIUS serveru: *Files* a pomocí tlačítka *"-"* smažte složku *user-manager* včetně souborů v ní uložených.
6. V sekci *Queues* smažte vámi vytvořená omezení.
7. Stejně jako na začátku úlohy uveďte MikroTik do továrního nastavení včetně smazání defaultní konfigurace.

Kontrolní otázky

- Uveďte kde jinde by jste vhodně využili VLAN.
- Na jakém portu naslouchá služba HTTPS?
- Jaké výhody má použití Hotspotu a jaká nastavení ve firewallu jsou automaticky provedena?
- Jaké následky by mělo přesměrování pouze portu číslo 21 u služby FTP?

Seznam zkratek

- DHCP – Dynamic Host Configuration Protocol
- DNS – Domain Name System
- FTP – File Transfer Protocol
- IS – Informační systém
- LAN – Local Area Network
- NAT – Network Address Translation
- RADIUS – Remote Authentication Dial-In User Service
- VLAN – Virtual Local Area Network
- VPN – Virtual Private Network

Literatura

- STEPHEN R. W. DISCHER – *RouterOS by example: understanding MikroTik RouterOS through real life applications* – College Station, Texas: MicroTik, 2011. ISBN 9780615547046.
- PETR KRČMÁŘ – *Proč není NAT totéž co firewall.* ROOT.cz. [online]. 13. 6. 2007 [cit. 2015-12-13]. Dostupné z: <`http://www.root.cz/clanky/proc-neni-nat-totez-co-firewall/`>
- KOTLAŘÍK – *Protokol DHCP* [online]. [cit. 2015-12-07]. Dostupné z: <`http://ucitel.spsbv.cz/kotlarik/index_soubory/POS/Protokol_DHCP.pdf`>
- MARTIN KUCHAŘ – *Firewall - obrňte své počítače.* Pctuning [online]. 2005-02-02 [cit. 2015-12-09]. Dostupné z: <`http://pctuning.tyden.cz/software/ochrana-pocitace/4296-firewall-obrnte_sve_pocitace`>