CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost DSL usmjerivača

CCERT-PUBDOC-2008-06-231

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. UVOD 4

2. UVOD U DSL TEHNOLOGIJE 5

2.1. PRINCIP RADA DSL TEHNOLOGIJE 5

3. DSL USMJERIVAČ 6

3.1. KONFIGURIRANJE USMJERIVAČA 6

3.1.1. Konfiguriranje korištenjem web sučelja 7

3.1.2. Konfiguriranje usmjerivača preko CLI sučelja 8

3.1.3. Načini rada usmjerivača 8

3.1.4. Daljinsko spajanje na usmjerivač 9

4. POSTAVLJANJE PRISTUPNE LOZINKE 11

5. AUTENTIKACIJA, AUTORIZACIJA, OBRAČUN 13

5.1. RADIUS 13

5.2. TACACS+ 14

5.3. USPOREDBA PROTOKOLA RADIUS I TACACS+ 15

6. BEŽIČNI USMJERIVAČ 15

6.1. PRINCIP RADA 16

6.2. SIGURNOSNE PRIJETNJE 16

6.3. DODATNE FUNKCIJE USMJERIVAČA 17

6.3.1. Vatrozid 17

6.3.2. Filtriranje prometa prema sadržaju 17

6.3.3. Filtriranje prometa obzirom na MAC adresu 17

6.3.4. DMZ 18

6.3.5. NAT 18

6.3.6. Kvaliteta usluge 18

7. ZAKLJUČAK 20

8. REFERENCE 20

1. Uvod

DSL usmjerivači su mrežni uređaji koji se koriste za prosljeđivanje paketa između korisničkog računala (ili lokalne mreže) i Interneta pronalaženjem optimalnog mrežnog smjera na putu od izvorišta do odredišta. U svojim je počecima Internet bio siguran za korištenje, ali danas, sve više, predstavlja izvor brojnih opasnosti za računalne korisnike.

Da bi korištenje usmjerivača bilo zaštićeno od neovlaštenog upada zlonamjernih korisnika, vrlo je bitno na početku korištenja pravilno konfigurirati ovaj uređaj. Ako se lokalni ili daljinski napadač spoji na usmjerivač, on može mijenjati putanje paketa kroz mrežu, kao i onemogućiti pristup ostalim korisnicima.

U ovom je dokumentu dan pregled osnovnih pojmova vezanih uz konfiguriranje DSL usmjerivača, načine daljinskog pristupa, postavljanje pristupnih lozinki, enkripciju i autentikaciju podataka koji se izmjenjuju računalnom mrežom. Također, opisane su osnovne funkcionalnosti usmjerivača s implementiranom priključnom točkom (eng. access point) i postavke koje je potrebno postaviti kako bi se ovakvi uređaji zaštitili.

2. Uvod u DSL tehnologije

DSL (eng. Digital Subscriber Line) odnosno digitalna pretplatnička petlja naziv je tehnologije koja omogućava digitalni prijenos podataka preko bakrenih vodova (parica) do krajnjeg korisnika usluge. Prednosti DSL-a u odnosu na druge tehnologije su: širi iskoristivi frekvencijski pojas, stalna izravna veza, niska cijena implementacije, prilagodljiva brzina prijenosa kao i podrška za telefoniju.

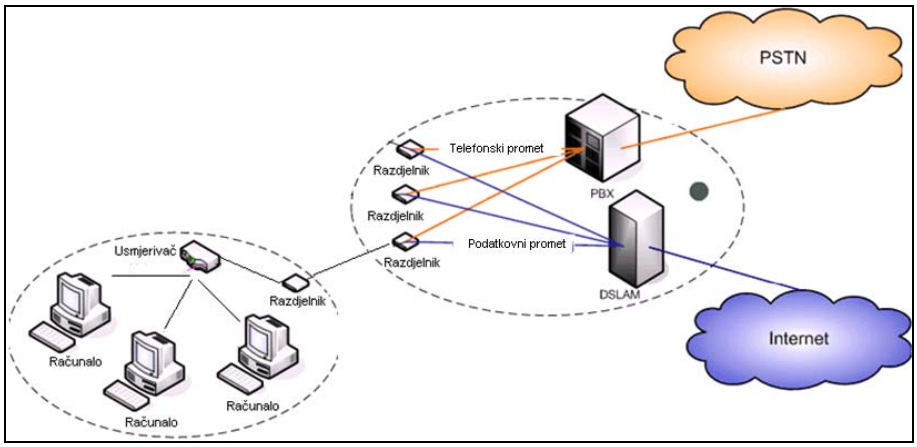
Postoji više podjela ove tehnologije koje zajednički imenujemo xDSL. Osnovnu podjelu moguće je načiniti u dvije odvojene skupine: asimetrične i simetrične DSL-tehnologije. Simetričnost se u ovom kontekstu odnosi na prijenosne brzine u dolaznom i odlaznom smjeru prijenosa podataka. Ako su te dvije brzine međusobno jednake, tada dotična DSL-tehnologija pripada skupini simetričnih DSL tehnologija. U suprotnom se radi o asimetričnoj DSL-tehnologiji.

DSL tehnologija	Max. brzina slanja (eng. upload)	Max. prijemna brzina (eng. download)	Domet (m)	Podrška za telefoniju
ADSL	1 Mbps	8 Mbps	5,500	Da
HDSL	1, 54 Mbps	1, 54 Mbps	3,650	Ne
IDSL	144 Kbps	144 Kbps	10,700	Ne
MSDSL	2 Mbps	2 Mbps	8,800	Ne
RADSL	1 Mbps	7 Mbps	5,500	Da
SDSL	2,3 Mbps	2,3 Mbps	6,700	Ne
VDSL	16 Mbps	52 Mbps	1,200	Da

Tablica 1. Pregled DSL tehnologija obzirom na njihove karakteristike

2.1. Princip rada DSL tehnologije

Kako bi se DSL tehnologija mogla koristiti mora se osigurati odgovarajuća oprema. Na korisničkoj strani potrebno je imati osobno računalo i DSL uređaj, tj. primopredajnu jedinicu s implementiranim komutacijskim (eng. switching) ili usmjerivačkim (eng. routing) modulom. Na drugom kraju DSL poveznice tj. u lokalnoj centrali nalazi se glavni razdjelnik koji povezuje krajnje DSL korisnike izravno s pristupnim DSL-multipleksorom (DSLAM). DSLAM multipleksira DSL promet na brzu jezgrenu ATM mrežu posredstvom tzv. univerzalnog pristupnog koncentratora (engl. UAC). Pored samog DSL prometa UAC može koncentrirati i ostale vrste prometa. UAC odabire pružatelja mrežne usluge te zatim usmjerava ili komutira podatke prema glavnoj poveznici (engl. trunk) i prema odabranom pružatelju mrežnih usluga. Slika 1. prikazuje kako to izgleda u stvarnosti.



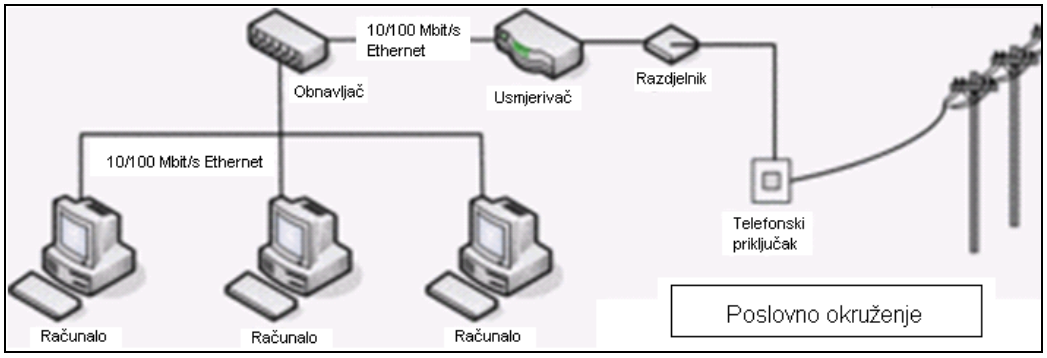
Slika 1. Struktura DSL mreže

3. DSL usmjerivač

Kao što je već spomenuto, da bi se korisnik mogao spajati na Internet njegovo računalo mora biti spojeno na DSL uređaj, odnosno DSL usmjerivač (eng. router). Usmjerivač je uređaj koji usmjerava pakete na njihovom putu kroz računalnu mrežu. Danas najčešće govorimo o usmjerivačima u IP mrežama, jer je njihova najveća primjena upravo za potrebe najveće računalne mreže danas - Interneta. Osnovne operacije koje svaki usmjerivač mora obavljati su prosljeđivanje paketa iz jedne u drugu mrežu te određivanje smjera prijenosa paketa kroz mrežu.

Iako je osnovna funkcionalnost usmjerivača prilično jednostavna u praksi je njihov zadatak prilično složen, te je zbog složene konstrukcije, specifičnog operativnog sustava i programa koje usmjerivači koriste njihova konstrukcija često kompleksna.

DSL usmjerivač (u daljnjem tekstu usmjerivač) je, dakle, uređaj koji spaja korisničko računalo na DSL liniju (Slika 2). Mogu biti izvedeni na različite načine pa tako, osim osnovnih funkcionalnosti usmjerivači, uglavnom, imaju ugrađen i preklopnik (eng. switch) čime se ostvaruje i funkcionalnost lokalne mreže.



Slika 2. Spajanje više računala na mrežu korištenjem usmjerivača

Većina korisnika, posebno u gradovima i prigradskim područjima s postavljenom paričnom infrastrukturom, koristi varijantu ADSL modema jer je standardiziran (prema standardu ADSL2+). Ujedno, prijenosna brzina u oba smjera je zadovoljavajuća za pristup Internetu, maksimalni domet čini ga atraktivnim čak i u malim gradovima i selima gdje je postavljena odgovarajuća kabelska infrastruktura, te podržava istovremeni prijenos POTS (eng. Plain Old Telephone Service) linija i ADSL podataka zajedničkom upredenom paricom.

U današnje vrijeme velik broj kućanstava, ali i tvrtki, koristi ovaj uređaj za potrebe spajanja na Internet. Kako bi ih se moglo bezbrižno koristiti potrebno je obratiti pažnju na sljedeće sigurnosne postavke kako ne bi postali meta udaljenih ili lokalnih napadača:

1. Fizička sigurnost usmjerivača
2. Sigurnost instaliranog operacijskog sustava na usmjerivaču
3. Ispravno konfiguriranje uređaja

3.1. Konfiguriranje usmjerivača

Postupak konfiguriranja usmjerivača može se izvesti na više načina:

1. Konfiguriranje korištenjem web sučelja
2. Konfiguriranje preko CLI sučelja
3. Daljinsko konfiguriranje

U daljnjem tekstu slijedi objašnjenje za svaki od navedenih načina zajedno s glavnim karakteristikama.

Međutim, bitno je spomenuti, da se početno konfiguriranje mora obaviti korištenjem web sučelja ili unosom naredbi preko CLI sučelja.

3.1.1. Konfiguriranje korištenjem web sučelja

Jedan od načina spajanja na usmjerivač je korištenjem web sučelja. Pritom je neophodno da računalo dobije adresu od usmjerivača koji ima DHCP server. Za pristup usmjerivaču potrebno je u web pregledniku Internet Explorer upisati njegovu adresu (uglavnom je to adresa 192.168.1.1.). Nakon upisivanja pristupne lozinke, koja je definirana od strane proizvođača uređaja, otvara se novi prozor iz kojeg je moguće upisivanje i/ili promjena postojeće konfiguracije. Ukoliko korisnik nije siguran je li 192.168.1.1. adresa na kojoj se nalazi usmjerivač, može to provjeriti tako da slijedi:

start run upiše cmd i klikne tipku "OK"

Zatim se otvara novi prozor gdje treba upisati naredbu ipconfig i na ekranu se ispisuju sljedeći podaci:

```
IP address           :192.168.1.101
Subnet Mask          :255.255.255.0
Default Gateway:     :192.168.1.1
(ovu je adresa koja se upisuje u
Internet Explorer)
```

Moguće je da se adrese, koje su dane u ovom primjeru ne podudaraju s onima kod korisnika, ali je bitno obratiti pažnju na adresu „Defaul Gateway-a“ budući da je to ona koju je potrebno upisati u web preglednik.

Ako korisnik nije siguran jesu li postavke njegovog usmjerivača ispravno podešene, može dozvoliti nekoj drugoj stručnoj osobi ulaz u usmjerivač na sljedeći način. Za Siemens SE515 usmjerivač to se radi na sljedeći način:

1. Potrebno je spojiti se na usmjerivač preko web sučelja i kliknuti na Advanced Setup Administration Management
2. Postaviti parametre:

```
Remote Management:          Enabled
Authorised Host Address     0.0.0.0
(omogućuje se pristup sa svih javnih i
privatnih IP adresa)
Web Server Port on WAN:     80
```

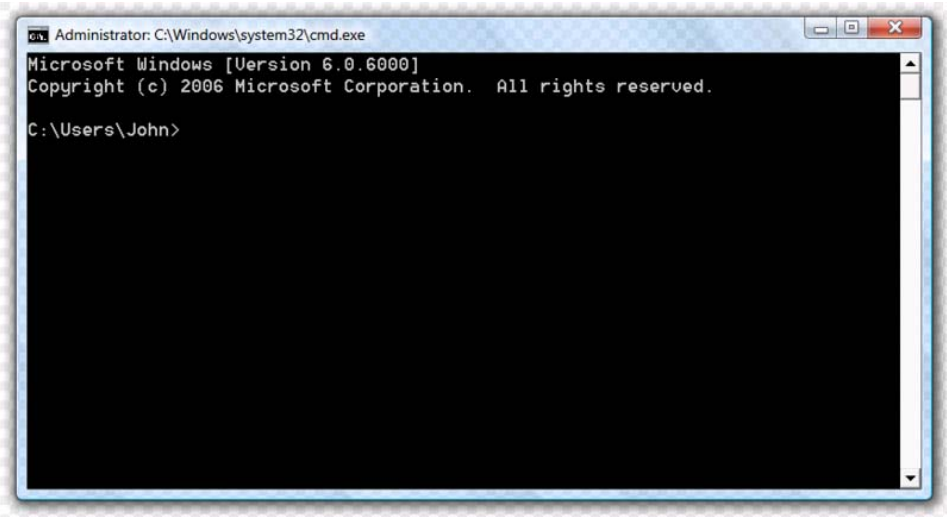
Po završetku ovakvog konfiguriranja potrebno je ponovno izmijeniti postavke kako bi se drugim neovlaštenim korisnicima onemogućio pristup:

1. Spojiti se na usmjerivač preko web sučelja i kliknuti na Advanced Setup Administration Management
2. Postaviti parametre:

```
Remote Management:          Enabled
Authorised Host Address:    127.0.0.1
Web Server Port on WAN:     8080
```

3.1.2. Konfiguriranje usmjerivača preko CLI sučelja

CLI (eng. Command Line Interface) sučelje se koristi za upravljanje uređajima isključivo preko teksta i komandne linije, a podržavaju ga gotovo svi operativni sustavi. Slika 3. prikazuje izgled CLI sučelja kod operativnog sustava Windows Vista.



Slika 3. CLI sučelje operativnog sustava Windows Vista

Usmjerivač je moguće konfigurirati serijskom vezom tako da se računalo kabelom spoji na konzolni priključak usmjerivača. Zatim se pomoću programa npr. Hyper Terminal pristupa CLI sučelju preko kojeg se dalje obavlja konfiguriranje. Da bi usmjerivač minimalno bio funkcionalan potrebno je postaviti određene parametre na njemu. Neki od njih su:

- Pristupna lozinka
- IP adresa sučelja
- Enkripcija

3.1.3. Načini rada usmjerivača

Konfiguriranje usmjerivača korištenjem CLI sučelja je definirano s nekoliko različitih načina rada (i ovisno je o tipu usmjerivača). Postoje brojne kategorije, a međusobno se razlikuju obzirom na to koje je postavke usmjerivača potrebno konfigurirati (tj. koje se naredbe mogu izvršavati). Kod Cisco uređaja ti su načini rada definirani ovako:

1. Korisnički način rada (eng. user mode) – omogućen je uvid u neke postavke usmjerivača, ali konfiguriranje nije moguće. Mogu se koristiti naredbe kao što su ping, telnet , rlogin ili naredbe za dobivanje osnovnih informacija o uređaju. Odziv ima oblik:

```
Router>
```

2. Privilegirani način rada (eng. privileged mode) – dostupne su sve postavke usmjerivača i sve statistike. Ovaj se način rada najčešće osigurava pristupnom lozinkom. Odziv ima oblik:

```
Router#
```

3. Globalni konfiguracijski način rada (eng. global configuration mode): iz privilegiranog načina rada može se ući u ovaj način rada, i kroz njega se obavlja konfiguracija usmjerivača. Odziv je:

```
Router(config)#
```

4. Specifični konfiguracijski načini rada(eng. specific configurations modes): iz globalnog konfiguracijskog načina rada može se ulaziti u pojedine specifične načine rada iz kojih se konfiguriraju sučelja, podsučelja, usmjerivački protokoli, itd. Svaki je način rada definiran podacima koji se nalaze u zagradi pored imena usmjerivača:

```
Router> Unprivileged mode
Router# Privileged mode
Router(config)# Global configuration mode
Router(config-if)# Interface mode
Router(config-subif)# Subinterface mode
Router(config-line)# Line mode
Router(config-router)# Router configuration mode
```

3.1.4. Daljinsko spajanje na usmjerivač

Ukoliko je usmjerivač, koji je spojen na mrežu već konfiguriran i ima barem jedan aktivni priključak s definiranom IP adresom, uređaju se može pristupiti daljinski. Osnovni razlog za korištenje ove metode je veća brzina izvođenja zadanih naredbi.

Daljinsko spajanje na usmjerivač može se obavljati korištenjem različitih programa, ali treba uzeti u obzir kako usmjerivač treba imati definiranu mogućnost za takvu vrstu spajanja.

U nastavku je dan opis ovakvih programa te kako ih se konfigurira.

1. Telnet

Telnet (eng. TELetype NETwork) je mrežni protokol unutar IP grupe protokola na Internetu ili u lokalnim mrežama koji korisniku omogućava da se sa svog računala, pomoću istoimenog interaktivnog klijentskog programa, spoji na fizički udaljeni poslužitelj i na njemu izvršava neke operacije. Taj poslužitelj uglavnom radi pomoću nekog od UNIX operacijskih sustava. Za pristup udaljenom računalu korisnik mora na njemu imati otvoren korisnički račun. Kada se korisnik pomoću specijaliziranog programa za Telnet spoji na udaljeni poslužitelj, njegovo lokalno računalo služi za unos naredbi koje se izvršavaju na udaljenom računalu. Telnet je tekstualna usluga bez ikakvih grafičkih elemenata, a podržavaju ga svi poznatiji operacijski sustavi kao što su, primjerice, Windows, UNIX/Linux, itd.

Danas usluge Telneta koriste uglavnom administratori računala kako bi pristupili funkcijama za konfiguriranje i održavanje poslužitelja.

Uspostava Telnet veze na Cisco usmjerivačima se postavlja naredbom:

```
Router(config)#interface Serial BROJ
Router(config-if)#ip address ADRESA
Router(config-if)#no shut
```

Osim toga, da bi se pristupilo usmjerivaču pomoću Telneta potrebno je postaviti *vty* (eng. virtual terminal) lozinku. U suprotnom će svaki pokušaj za uspostavu veze završiti bezuspješno.

Pristup mrežnim uređajima je jednostavan, a podaci koji se pritom izmjenjuju prenose se mrežom kao običan tekst. Napadač može iskoristiti ovu situaciju kako bi saznao sve bitne informacije o usmjerivaču (kao što su korisničko ime i pristupna lozinka) te ih iskoristiti za pristup uređaju kao korisnik s administratorskim ovlastima.

Metode zaštite odnose se na postavljanje lozinki i upotrebu ACL (eng. Access Control List) listi. Upotrebom ACL liste na usmjerivaču moguće je zabraniti pristup pojedinoj IP adresi računala (ili grupi IP adresa).

2. SSH

SSH (eng. Secure Shell) je sljedeći protokol za daljinsko spajanje i upravljanje konfiguracijskim postavkama usmjerivača. U svom radu primjenjuje enkripciju podataka kao i digitalne certifikate (eng. digital certificates) pa ga je iz tog razloga preporučljivije koristiti nego Telnet.

Postoje dvije inačice programa: SSH1 i SSH2 koja su dva različita protokola za prijenos podataka. SSH1 koristi DES (eng. Data Encryption Standard) ILI 3DES IPSec enkripciju, a SSH2 koristi 3DES. Važno je napomenuti da SSH2 koristi veći stupanj zaštite.

U sljedećem je primjeru opisano kako konfigurirati SSH pristup na Cisco usmjerivaču te koje je sve postavke potrebno postaviti kako bi što više zaštitili ovaj mrežni uređaj.

```
Router(config)#hostname TR
TR(config)#
TR(config)#ip domain-name Tech.com
The name for the keys will be: TR.Tech.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Key. Choosing a key modulus greater than 512 may take few
minutes.
How many bits in the modulus: 768
% Generating 768 bit RSA key …[OK]
TR(config)#
Mar 1 00:17:13:337: %SSH-5-ENABLED: SSH 1.5 has been enabled
TR(config)#
```

Nakon što se generira ključ na ekranu je vidljiva poruka koja kaže da je omogućen SSH1.5 na usmjerivaču. SSH 1.5 je ekvivalent SSH1, a SSH1.99 je ustvari SSH2.

Moguće je definirati dodatne postavke za SSH kao što su definiranje SSH „time-out" intervala (vrijeme prije nego što se prekine neaktivna sjednica), postavljanje sučelja za odredišnu adresu u SSH vezi, broj priključka za spajanje itd. Kako bi se pregledale sve postavke potrebno je upisati naredbu *show ip ssh* za pregled postavki ili *show ssh* za pregled SSH veza.

3. FTP

FTP (eng. File Transfer Protocol) je protokol za razmjenjivanje podataka, definiran u RFC 959. FTP protokol koristi dvije odvojene istovremene TCP veze, jednu za upravljanje (priključni broj usluge 21), a drugu za prijenos podataka (20).

Upravljačka veza se koristi za prijenos naredbi i odgovora na naredbe. Podaci se prenose samo preko podatkovne veze. Pri prijenosu podataka mora se voditi računa o formatu podataka. Za prijenos tekstualnih podataka definira se ASCII način prijenosa (prilikom uspostave veze), odnosno binarni - za prijenos binarnih podataka.

Međutim, budući da podaci koji se prenose kroz mrežu nisu kriptirani zlonamjerni korisnik može vrlo lako iskoristiti ovaj propust za izvođenje napada na ranjivi sustav.

4. SFTP

Budući da se pomoću FTP protokola podaci prenose mrežom u tekstualnom obliku, razvijen je protokol SFTP (eng. Secure File Transfer Protocol). SFTP je program koji dolazi u paketu s *openssh* programskim paketom, a omogućuje sigurnije korištenje FTP protokola pomoću SSH protokola. Korištenje SFTP programa preporučuje se svim korisnicima kao sigurnija zamjena za tradicionalni FTP servis.

Rad SFTP-a zasniva se na postupku preusmjeravanja portova (poznato i kao „tuneliranje"). To je mehanizam koji korisniku omogućuje preusmjeravanje inače nesigurnog FTP prometa preko sigurnog SSH komunikacijskog kanala.

Korištenje programa je vrlo jednostavno, budući da su sve naredbe naslijeđene od običnog FTP protokola.

4. Postavljanje pristupne lozinke

Postavljanje pristupnih lozinki, kako bi se osigurao ili onemogućio pristup usmjerivaču, jedno je od osnovnih stvari koje je potrebno konfigurirati za kasniji siguran rad uređaja. Zaštita lozinkom je samo jedan od načina kako zaštititi usmjerivač od neovlaštenog lokalnog ili udaljenog napadača. Druge se metode odnose na implementaciju vatrozida, implementaciju ACL (eng. access-list) lista, itd.

Postoje tri osnovne vrste pristupnih lozinki koje štite usmjerivač od neovlaštenog upada, a u nastavku je opisano kako ih konfigurirati na Cisco usmjerivačima.

1. Osnovna lozinka
   Tipovi ove lozinke su različiti, a njihovo postavljanje ovisi o tome za koju se pristupnu točku žele koristiti. U nastavku su navedeni ovi tipovi te kako se za svaki od njih postavlja lozinka.

   - Konzolna – koristi se kada usmjerivač nije spojen na mrežu nego se računalo spaja direktno na konzolni priključak usmjerivača.

```
Router(config)#line con 0
Router(config)#password LOZINKA
Router(config)#login
```

   - Aux – lozinka koja se koristi ako se korisnik direktnom fizičkom vezom spaja na pomoćni priključak usmjerivača

```
Router(config)#line aux 0
Router(config-line)#password LOZINKA
Router(config-line)#login
```

- VTY – "virtualna tty" lozinka koja se koristi kada kod daljinskog spajanja na usmjerivač

```
Router(config)#line vty 0 4
Router(config-line)#password LOZINKA
Router(config-line)#login
```

Brojevi koji su navedeni u prvom redu 0-4 ovise o broju linija. Noviji usmjerivači uglavnom imaju broj linija od 0-15)

- Async – koristi se ukoliko se u usmjerivač ugradi posebna kartica koja omogućava spajanje dodatnih uređaja

```
Router(config)#line x
Router(config-line)#password LOZINKA
Router(config-line)#login
```

Sve se spomenute lozinke postavljaju korištenjem naredbi *password* i *login*. Naredbom *password* određuje se koja će biti lozinka, a naredbom *login* se definira da usmjerivač počne primjenjivati spomenutu pristupnu lozinku. Preporučuje se korisnicima da, nakon što postave lozinke, provjere jesu li sve promjene upisane u usmjerivač. To se radi upisivanjem naredbe *show running-config* u neprivilegiranom načinu rada usmjerivača.

Moguće je, također, definirati vrijeme nakon kojeg je potrebno ponovno upisivati lozinku ako se neko vrijeme ne obavljaju nikakve radnje na usmjerivaču.

2. Pristupna lozinka za ulaz u privilegirani način rada
   Kako bi se postavila ova lozinka potrebno je unijeti sljedeće naredbe:
   - *enable password* – ova se naredba uglavnom ne koristi jer ne omogućuje enkripciju

```
Router(config)#enable password LOZINKA
```

   - *enable secret* – omogućava automatsku enkripciju lozinke korištenjem posebnih enkripcijskih mehanizama

```
Router(config)#enable secret LOZINKA
```

3. Korisnička lozinka
   Moguće je koristiti jednu ili više korisničkih lozinki ovisno o tome koliko se korisnika spaja na usmjerivač. Ovo je dodatna lozinka koja se može ili ne mora postavljati, a koristi se za povećanje sigurnosti prilikom pristupanja usmjerivaču. Također, na ovaj je način moguće definirati ovlasti za svakog korisnika obzirom na postavke koje smije vidjeti i/ili mijenjati.

```
Router(config)#username IME privilege STUPANJ password LOZINKA
Router(config-line)#login local
```

Kako te informacije ne bi bile dostupne svima, administratorima se preporuča enkripcija ovih podataka naredbom:

```
Router (config)# service password-encryption
```

U svrhu zaštite svi bi usmjerivači trebali imati postavljene pristupne lozinke. Dakle, svaki bi korisnik DSL usmjerivača trebao postaviti, minimalno, osnovnu lozinku te isprobati jesu li lozinke ispravno postavljene i funkcionalne.

Bitno je napomenuti kako se navedene pristupne lozinke odnose na kompleksnije usmjerivače, dok mali korisnici mogu postaviti samo lozinke za pristup preko web sučelja ili za daljinsko spajanje. Preporuka je koristiti tzv. „jake" lozinke (korištenje brojeva, slova i znakova u kombinaciji i postavljanje duljine lozinke veće od 6 znakova).

5. Autentikacija, autorizacija, obračun

U većim je mrežama prilično teško uspostaviti i održati sigurnost obzirom na pristup pojedinim mrežnim uređajima kao što su usmjerivači. Zato se, osim enkripcije podataka, dodatno koriste i druge metode naziva AAA autentikacija (eng. authentication, authorization and accounting).

- **Autentikacija** – ovim se postupkom određuje tko ima pristup mreži, obavlja se potvrđivanje identiteta korisnika (koji je zatražio pojedinu mrežnu uslugu) te utvrđuje prava pristupa korisnika zatraženoj usluzi
- **Autorizacija** – definira se ograničenje pristupa pojedinim uslugama za različite korisnike tj. predstavlja odobravanje određenih vrsta usluga korisniku na temelju rezultata prethodno provedene autentikacije, zatražene usluge i trenutnog stanja poslužitelja
- **Obračun** - odnosi se na praćenje potrošnje mrežnih resursa od strane pojedinih korisnika. Osim toga, koristi se i za praćenje uspostave „sumnjivih" veza na računalnu mrežu

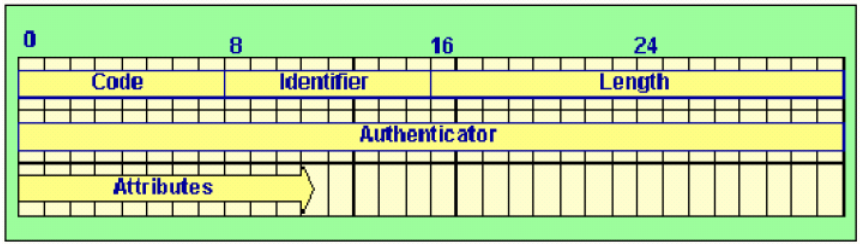
Na taj se način, osim što se unose dodatne mjere sigurnosti protiv neovlaštenog upada, omogućuje definiranje centralnog servera koji vodi računa da se na svakom usmjerivaču provodi adekvatna autentikacija, autorizacija i obračun.

U nastavku spomenuti samo najvažnije programske pakete koji koriste ovu metodu, a to su RADIUS i TACACS+.

5.1. RADIUS

RADIUS (eng. Remote Authentication Dial-in User Service) je centralizirani AAA protokol. Prvotno je bio namijenjen modemskom pristupu udaljenim mrežama, ali danas je njegova upotreba proširena na bežične pristupne točke, preklopnike, DSL poslužitelje i sl.

Protokol se bazira na klijent-poslužitelj modelu i koristi UDP mrežni protokol. Na strani klijenta koristi se Network Access Server (NAS) programski paket, koji obavlja zadatke vezane uz prosljeđivanja korisničkih parametara RADIUS poslužitelju kao i obradu primljenih odgovora. S druge strane, RADIUS poslužitelji su zaduženi za prihvaćanje upita, provjeru primljenih paketa, te vraćanja potrebnih konfiguracijskih parametara, koji će klijentu omogućiti pružanje adekvatne usluge korisniku. Slika 4. prikazuje format RADIUS podatkovnog paketa koji se izmjenjuje preko mreže kako bi se osigurala komunikacija između korisnika i poslužitelja.



Slika 4. Format RADIUS podatkovnog paketa

Korištenjem ovog protokola olakšava se i centralizira administracija korisnika, pruža se određeni stupanj zaštite protiv napada neovlaštenih korisnika, a i kompatibilan je s opremom različitih proizvođača mrežne opreme.

Spomenuti protokol sadrži određene sigurnosne propuste koji su posljedica propusta u implementaciji samog protokola ili neispravne i nepotpune implementacije programske podrške. Najbitniji među propustima odnose se na mogućnost odgonetanja tajnog ključa, uspješno nagađanje korisničke zaporke i neodgovarajuće mehanizme za generiranje slučajnih brojeva. Protokol se može poboljšati odabirom simetričnog algoritma za enkripciju zaporke, uvođenjem novog „User-Password" atributa s alternativnim algoritmom za enkripciju i pažljivim odabirom ključa za enkripciju zaporke.

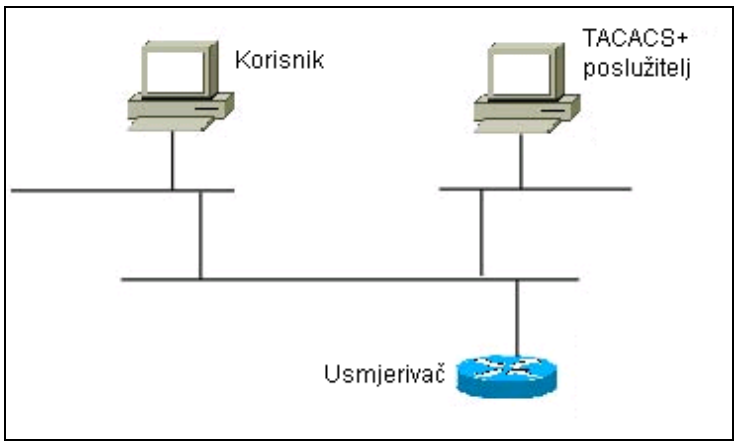
5.2. TACACS+

TACACS+ (eng. Terminal Access Controller Access Control System) je autentikacijski protokol, definiran RFC 1492 standardom.

Osigurava kontrolu pristupa usmjerivačima, mrežni pristup poslužitelja i ostalih mrežnih uređaja preko jednog ili više centraliziranih poslužitelja. U svom radu koristi mrežni protokol TCP.

Ovaj protokol omogućava odvojenu autentikaciju i autorizaciju. Princip rada temelji se na klijent-poslužitelj modelu i u svom radu vrlo je sličan protokolu RADIUS.

Slika 5. prikazuje topologiju mreže koja koristi protokol TACACS+.



Slika 5 . Topologija mreže koja koristi TACACS+

Za provođenje AAA procedure korištenjem programa TACACS+ najprije je potrebno na poslužitelju definirati listu korisnika te odrediti za svakog od njih pristupne ovlasti.

U nastavku je prikazano kako se na Cisco usmjerivačima konfigurira ovaj protokol.

```
router#configure terminal
router(config)#aaa new-model
router(config)#aaa authentication login my-auth-list tacacs+
router(config)#aaa authentication my-auth-list tacacs+ if-authenticated
router(config)#tacacs-server host 192.168.1.101
router(config)#tacacs-server key letmeinrouter(config-line)
router(config)#login authentication my-auth-list
```

5.3. Usporedba protokola RADIUS i TACACS+

Svaki od navedenih protokola imaju svojih prednosti i mana, a izbor koji protokol je bolje koristiti ponajprije ovisi o samim potrebama krajnjih korisnika.

U tablici 2 dan je usporedni prikaz protokola RADIUS i TACACS+.

	RADIUS	TACACS+
TCP ili UDP	Koristi UDP pakete. Uspostava veze korištenjem UDP paketa traje kraće	Koristi TCP pakete. Protokol je konekcijski orijentiran i koristi potvrdu prijema
Enkripcija	Enkriptira se samo pristupna lozinka	Enkriptira se cijeli paket
Autentikacija, autorizacija	Udružuje autentikaciju i autorizaciju što otežava njihovo moguće razdvajanje	Odvojeno se izvode postupci autentikacije i autorizacije
Upravljivost	Pojedini korisnici ne mogu upravljati usmjerivačem odnosno naredbama koje se izvršavaju	Omogućuje dva načina upravljanja: određuje dozvoljene naredbe i dodjeljuje autorizacijske razine

Tablica 2. Usporedni prikaz protokola RADIUS i TACACS+

6. Bežični usmjerivač

Bežični usmjerivač je mrežni uređaj koji obavlja sve funkcije običnog usmjerivača, ali mu je funkcionalnost dodatno proširena i na bežične mreže. Ovi su usmjerivači kombinacija ugrađenog DSL modema s Wi-Fi priključnom točkom (eng. AP–Access Point) i omogućuju lokalno bežično umrežavanje računala i pristup Internetu. AP povezuje više klijenata u zajedničku grupu i služi za povezivanje sa žičanom mrežom ili sa drugim bežičnim mrežama.

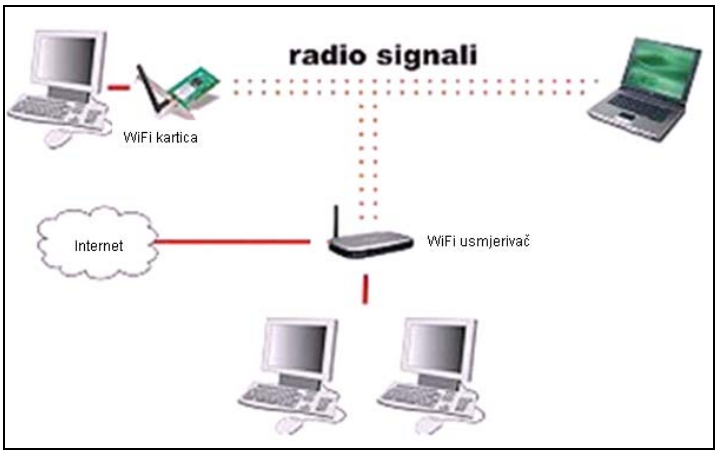
Bežični usmjerivači u Hrvatskoj koriste skupinu standarda bežične komunikacije 802.11b ili 802.11g i razvijeni su od strane međunarodnog tijela IEEE.

802.11b i 802.11g dijele područje frekvencija u 14 međusobno preklopljenih kanala koji su široki po 22 MHz. Kanali 1, 6 i 11 (a u nekim zemljama i 14) međusobno se ne preklapaju i te je kanale moguće koristiti tako da više mreža može raditi jedna blizu druge, a da se ne ometaju. Domet im je obično 30 metara u zatvorenom prostoru ili do 90 metara na otvorenom (što se može povećati korištenjem antena).

6.1. Princip rada

Bežične mreže koriste radiovalove za prijenos podataka i time uvelike povećavaju fleksibilnost rada jer korisnik više ne ovisi o kvaliteti i smještaju mrežnih kabela, nego je dovoljno da se povezana računala nalaze unutar područja pokrivenog mrežom. Ova tehnologija ne zahtijeva izravnu optičku vidljivost, kao npr. infracrveni prijenos podataka (IrDA). Kod bežičnih mreža pristupna točka odašilje radiovalove u području od 30 do 300 metara koji prolaze kroz tanje zidove i druge nemetalne prepreke. Pomoću dodatnih komponenti taj se domet može i povećati.

Bežična mreža sastoji se od dva osnovna elementa: klijenta i pristupne točke. Na slici 6. dan je primjer bežične mreže koja koristi bežični usmjerivač, osobno i prijenosno računalo.



Slika 6. Primjer jednostavne bežične LAN mreže s izlazom na Internet

6.2. Sigurnosne prijetnje

Iako su, u standardima koji definiraju bežične računalne mreže, navedeni razni elementi sigurnosti pokazuje se da ti elementi u većini slučajevi ostaju neiskorišteni što je, dakako, velik sigurnosni problem.

No i kada se aktiviraju svi sigurnosni elementi to ne znači nužno da je postignuta odgovarajuća razina sigurnosti. Razlog tomu su mnogi nedostaci samog standarda koji su naknadno uočeni i koji omogućavaju zlonamjernoj osobi da bez većih poteškoća pristupi i koristi mrežne resurse bez dozvole i znanja vlasnika ili administratora mreže. Neke od sigurnosnih mjera protiv neovlaštenog upada su korištenje enkripcije i onemogućavanje emitiranja SSID naziva bežične mreže.

1. Bežična mreža definira se tako da se svim komponentama dodijeli identifikator skupa usluga (eng. SSID - Service Set ID), odnosno ime koje jednoznačno identificira bežičnu mrežu. SSID se prilikom razmjene podataka na mreži izmjenjuje između klijenta i poslužitelja. U tom će slučaju svako računalo koje se nalazi u dometu bežične mreže moći automatski dobiti pristup mreži. Zaštita protiv toga je isključivanje opcije odašiljanja SSID podataka.

2. Sljedeći način osiguravanja bežičnih mreža je osigurati pouzdanu autentikaciju i autorizaciju korisnika te na taj način zaštititi privatnost. To se postiže korištenjem određenih protokola.

    - Najčešće korišten standard je WEP (eng. Wired Equivalent Privacy) protokol. WEP se koristi na podatkovnom sloju OSI modela kako bi zaštitio podatke tijekom prijenosa. WEP se oslanja na tajnosti ključa (koji se koristi između pristupne točke i klijenta). Ovaj protokol omogućuje visoku, ali ipak ne

apsolutnu sigurnost od neželjenih pristupa mreži. Napadači mogu koristiti brojne besplatne programe kao što su primjerice AirSnort ili Aircrack za otkrivanje tajnog ključa. Ovi programi rade na principu osluškivanja prometa i provjere paketa na mreži na temelju koje jednostavnim algoritmima određuju WEP ključ.

- S ciljem dodatnog povećanja sigurnosti 2003. godine razvijen je novi protokol za sigurniju bežičnu komunikaciju: WPA (eng. Wi-Fi Protected Access). WPA znatno povećava sigurnost korištenjem naprednih postupaka autentikacije, metodama za razmjenu ključa (dinamički ključ) i uvođenjem dodatne kontrole vezane za integritet podataka. Kao nadogradnja na ovaj, razvijen je i WPA2 standard.

Budući da usmjerivači koje korisnici kupuju nemaju uključene gotovo nikakve sigurnosne postavke, važno je da zaštite svoje usmjerivače kako bi se osigurali od neovlaštenih upada.

6.3. Dodatne funkcije usmjerivača

Većina današnjih usmjerivača koristi dodatne, napredne funkcionalnosti za povećanje sigurnosti. Neke od najvažnijih spomenut ćemo u ovom poglavlju.

6.3.1. Vatrozid

Vatrozid (eng. firewall) je u osnovi program koji se implementira na usmjerivaču, a osnovna mu je namjena filtriranje mrežnog prometa. Smještaju se na ulazu tj. izlazu mreže te na taj način predstavljaju sponu lokalne mreže i drugih neprovjerenih mreža kao što je npr. Internet (ili druga lokalna mreža). Na tim pozicijama vatrozidi imaju zadatak provjeravati sve mrežne pakete koji ulaze ili izlaze iz mreže po različitim kriterijima i pravilima.

Pri tome oni mogu pojedine pakete propuštati ili blokirati na njihovom putu, zavisno o postavljenim pravilima.

Napredni vatrozidi osiguravaju spajanje unutrašnje i vanjske mreže na svim programskim slojevima, od podatkovnog sve do aplikacijskog.

6.3.2. Filtriranje prometa prema sadržaju

Radi se o specijaliziranom programu namijenjenom, uglavnom, roditeljima koji žele zabraniti prikazivanje određenih sadržaja prilikom pretraživanja Interneta. Filtar se postavlja obzirom na riječi koje se koriste na stranicama, domene, URL adrese, itd. Aplikaciju je moguće zaštititi lozinkom kako ne bi došlo do zlouporabe iste. Program također omogućuje definiranje vremena u kojem se dozvoljava pristup Internetu.

6.3.3. Filtriranje prometa obzirom na MAC adresu

MAC (eng. Media Access Control) adresa je jedinstvena oznaka karakteristična za svaki mrežni uređaj. Definirana je s 12 znakova (npr. 00-18-DE-DD-E1-49), od čega prvih šest znakova određuju proizvođača opreme, a preostali znakovi identificiraju sam uređaj. Pristup usmjerivaču moguće je odrediti prema MAC adresi računala koja se spajaju na njega. U tom je slučaju potrebno kreirati listu dozvoljenih MAC adresa. Za sve ostale će, u tom slučaju, promet biti blokiran.

6.3.4. DMZ

DMZ (eng. Demilitarized Zone) je program koji se koristi kako bi se na usmjerivaču definirao prikaz samo nekolicine IP adrese (računala koje je spojeno na usmjerivač) koja će biti javno dostupna preko Interneta. Neki programi, koji rade preko TCP/IP protokola zahtijevaju da na računalu bude otvoreno više priključaka (eng. port). Međutim, računalo s javno prikazanom adresom više nije zaštićeno vatrozidom i kao takvo može biti podložno napadima zlonamjernih korisnika. Pritom je bitan i podatak da DMZ program omogućuje sigurnu komunikacija koja se odvija između spomenutog računala i ostalih računala iz lokane mreže.

6.3.5. NAT

NAT (eng. Network Address Translation) mehanizam prevodi višestruke IP adrese sa privatne mreže u jednu javnu adresu koja je vidljiva preko Interneta. Time se provodi dodatna sigurnosna mjera jer adrese računala spojenih na usmjerivač nisu javno vidljiva. Pritom usmjerivač ima funkcionalnost vatrozida jer blokira sav neželjen i neočekivan promet prema lokalnoj mreži.

6.3.6. Kvaliteta usluge

Računalne su mreže stvorene s ciljem spajanja računala tako da ona mogu razmjenjivati i dijeliti podatke. U početku, većina tih podataka je bila u tekstualnom obliku, ali je danas sve veća potreba za prijenosom multimedijskih sadržaja (npr. video konferencije, Internet televizija itd.). Prilikom slanja takvih podataka treba ostvariti sljedeće:

1. Ostvariti potrebnu širinu frekvencijskog pojasa
2. Smanjiti kašnjenje (prijenos u stvarnom vremenu)
3. Optimizirati opterećenje mreže

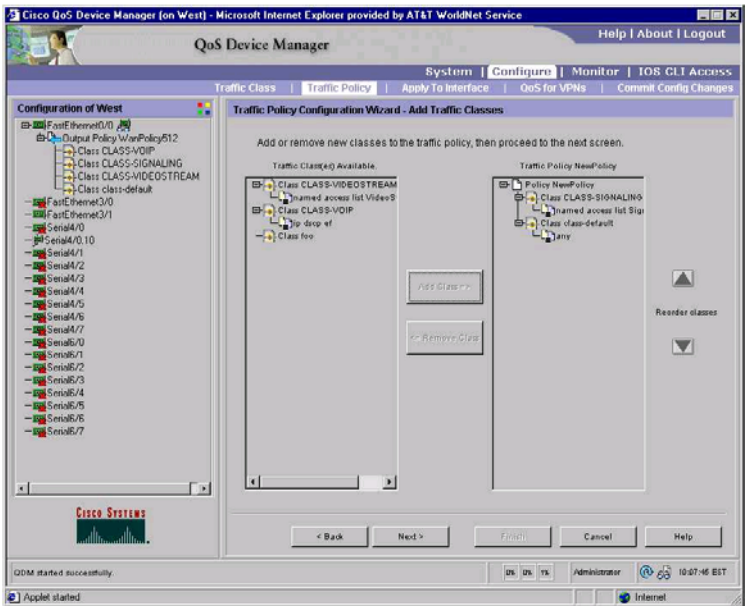
Iz tog se razloga definira kvaliteta usluge (eng.Quality of Service - QoS). Definicija kvalitete usluge, u najširem smislu, bila bi „stupanj zadovoljstva korisnika usluge“ (prema ITU-T E.800).

QoS omogućuje postavljanje različitih razina prioriteta za različite programe, korisnike ili tokove podataka. Na taj se način označavaju razine jamčene brzine veze prema drugom računalu u mreži, ali i nekih dodatni parametri u komunikaciji (načini usmjeravanja paketa kroz mrežu, jamčeno kašnjenje itd.).

Kod usmjerivača QoS se koristi za definiranje širine pojasa i prioriteta za određenu vrstu prometa na mreži. QoS se definira tako da se najprije odredi koji promet ima najveću važnost, a zatim se odredi širina pojasa za taj promet. Važno je spomenuti da bitan promet ne može zauzeti čitavi pojas i onemogućiti sav ostali promet koji se odvija preko usmjerivača.

Praćenjem QoS-a moguće je detektirati anomalije na mreži ili uređaju, što može predstavljati opravdanu sumnju na pokušaj provaljivanja u mrežu.

QoS je moguće implementirati samo na nekim usmjerivačima i potrebno ga je konfigurirati . Tako je npr. Cisco razvio QoS Device Manager aplikaciju, prikazanu na slici 7.



Slika 7. Implementiranje QoS usluge

Uz to što omogućava definiranje koje aplikacije i koja računala imaju veći prioritet, tj. kojima će se dodijeliti više resursa (brzine prijenosa) alat omogućava pregled opterećenosti i način korištenja pojedine veze. Praćenjem tih aktivnosti, administrator može na vrijeme uočiti i spriječiti bilo kakav pokušaj provale u sustav.

7. Zaključak

U današnje vrijeme kada je Internet potreban i važan resurs u svim organizacijama veoma je bitno posvetiti određenu pažnju računalnoj sigurnosti. Većina malih korisnika i tvrtki, za potrebe spajanja na Internet koristi upravo DSL usmjerivače.

Usmjerivači, koje je moguće nabaviti na tržištu, dolaze kod korisnika s nekim unaprijed definiranim postavkama. Sve dodatne funkcije je preporučljivo da korisnik sam konfigurira. Te se postavke u velikoj mjeri odnose na implementiranje sigurnosnih pravila kako bi se izbjegli napadi zlonamjernih korisnika. Zato je bitno postaviti sigurnosne lozinke kako se ne bi bilo tko mogao spojiti na mrežne uređaje, osigurati da podaci koji se razmjenjuju između mreža budu kriptirani te ispravno odabrati postavke usmjerivača s implementiranim sigurnosnim mehanizmima kako bi se rizik od sigurnosnog incidenta smanjio na najmanju moguću razinu.

8. Reference

[1] Router Security Configuration Guide, http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf, prosinac 2005.

[2] Ivan Pudar: Kontrola udaljenog pristupa, http://spvp.zesoi.fer.hr/seminari/2006/PudarIvan_KontrolaUdaljenogPristupa.pdf, lipanj 2006.

[3] How to create MAC Filter List on a Home Router, http://www.wikihow.com/Create-Machine-Address-Filter-List-on-a-Home-Router, studeni 2007.

[4] Parental Control Software Reviews, http://www.consumersearch.com/www/software/parental-control-software/, srpanj 2007.

[5] John Ward: Windows Remote Desktop Connection, http://teamtutorials.com/windows-tutorials/windows-remote-desktop-connection, ožujak 2008.

[6] Router, http://en.wikipedia.org/wiki/Router, svibanj 2008.