Marinko Smiljanić,
student stariji vodnik,
Vojna akademija,
Beograd
mr Boban Pavlović,
kapetan, dipl. inž.
Vojna akademija,
Beograd

VIRTUELNE PRIVATNE MREŽE – MOGUĆE REŠENJE POUZDANIH KOMUNIKACIJA

UDC: 004.728
004.738.5.057.4

Rezime:

U radu su prikazane osnovne karakteristike virtuelnih privatnih mreža (VPN – Virtual Private Networks). Analizirane su VPN mreže na drugom i trećem sloju sistema otvorenog za povezivanje (OSI – Open System Interconnnection). Objašnjena je realizacija internet protokola (IP – Internet Protocol) VPN mreže i VPN mreže u okruženju višestruke komutacije labela (MPLS – Multi-Protocol Label Switching). Posebna pažnja posvećena je sigurnosti MPLS VPN mreža, naročito sa stanovišta upotrebe u funkcionalnim sistemima veza, kao što je sistem veza Vojske.

Ključne reči: VPN, VPN na drugom sloju, VPN na trećem sloju, IP, MPLS, zaštita.

VIRTUAL PRIVATE NETWORKS – POSSIBLE SOLUTION OF RELIABLE COMMUNICATIONS

Summary:

In this paper the basic characteristics of the VPN networks are presented. The VPN networks on the second and the third level of the OSI reference model are analyzed. The realization of the IP VPN and VPN networks within MPLS environment is presented as well. Security in MPLS networks is one of the most important characteristics, especially in military communication systems, which is shown in the second part of this paper.

Key words: IP, Virtual Private Networks, 2L VPN, 3L VPN, protection, MPLS.

Uvod

Da bi se jedna organizaciona celina vojske povezala sa komandom, u jedinstvenu širokopojasnu mrežu (WAN – Wide Area Network), do pre deset godina bilo je potrebno popisati adrese svih lokacija i iznajmiti telefonske linije od svake lokacije ponaosob do komandne zgrade. Pri tome je mreža mogla da bude realizovana na dva načina. Prvi način podrazumeva da se svaka jedinica poveže sa komandom posebnom linijom, što je efikasno ako je udaljenost između jedinica velika. Drugi, efikasniji i jeftiniji način podrazumeva hijerarhijsku strukturu, u kojoj se jedinice grupišu u lokalna mrežna čvorišta, koja se povezuju na centralno čvorište. I jedno i drugo rešenje zahteva zakup linija – cena tog zakupa u lokalnoj mreži nije mnogo velika, ali je korišćenje međumesnih, a pogotovo međunarodnih linija veoma skupo.

Internet je danas prisutan u svakom mestu, a lokalna mreža povezana sa internetom biće „vidljiva“ sa svih drugih lokacija na globalnoj mreži, pa i sa lokalne mreže u drugoj organizacionoj jedinici, koja je, takođe, povezana sa internetom. Na primer, ako se želi povezati komanda jedinice u Beogradu sa organizacionim celinama u Valjevu i Smederevu,

dovoljno je da se na sve tri lokacije zakupi linija do najbližeg internet provajdera. Na taj način formira se sopstvena mreža.

Na ovaj način samo prividno je uspostavljena izolovana mreža – virtuelna privatna mreža. Mnogi proizvođači su, u potrazi za kratkim i upečatljivim imenom, konceptu dodelili ime „ekstranet", dakle pojam suprotan pojmu „intraneta", mreže koja može da bude fizički potpuno nezavisna od interneta.

VPN – osnovni pojmovi

Virtuelna privatna mreža omogućava povezivanje dve ili više udaljenih lokacija u jedinstvenu lokalnu računarsku mrežu [1]. Za realizaciju ove veze koriste se posebni protokoli koji omogućavaju šifrovanje (enkripciju) podataka, čime se obezbeđuje bezbedna razmena podataka između korisnika unutar VPN sistema. Ovakve mreže su privatne, jer resurse ovih konekcija mogu koristiti samo organizacije koje su njihov vlasnik. Privatne su i sa aspekta rutiranja i adresnog plana, odnosno algoritmi rutiranja i adresni plan su potpuno nezavisni od drugih mreža. Mreža je virtuelna, jer se konekcije formiraju korišćenjem samo jednog dela instaliranih resursa javne mreže za prenos podataka. Istorijski gledano, X.25 je prvi WAN protokol koji je omogućio izgradnju VPN mreža na javnim mrežama za prenos podataka. Prevashodna uloga ovako izgrađenih mreža je smanjenje telekomunikacionih troškova efikasnijim korišćenjem infrastrukture uz istovremeno očuvanje sigurnosti i integriteta podataka.

Tendencija je da se sve privatne poslovne WAN mreže u budućnosti zamene VPN baziranim WAN poslovnim mrežama. Osnovni razlozi za to su:

– znatno manja cena izgradnje mreže, u odnosu na tradicionalne privatne mreže;

– omogućavanje elektronskog poslovanja i internet ekonomije. VPN je znatno fleksibilnija i skalabilnija arhitektura mreže u odnosu na klasične privatne WAN mreže. Skalabilnost predstavlja mogućnost jednostavnih izmena u mreži, kako bi se omogućio rad sa novijim tehnologijama i platformama. Kada je mreža skalabilna znači da odgovara zahtevima koji mogu biti promenljivi i koji se mogu menjati s obzirom na konkretnu namenu mreže. One omogućavaju vrlo brzo i jeftino povećanje broja udaljenih internacionalnih lokacija, mobilnih korisnika u romingu i slično. Bez dodatnih ulaganja koriste sve raspoložive ulaze davaoca internet usluga (ISP – Internet Service Provider);

– znatno manji troškovi i napori u održavanju vlastite mreže, jer se veći deo poslova održavanja odvija u okviru mreže provajdera koji nudi ovu uslugu;

– jednostavnija mrežna topologija. Upotrebom IP jezgra (backbone) eliminišu se permanentna kola (PVC – Permanent Virtual Channel) koja su se ostvarivala putem mreža zasnovanih na prenosu okvira (Frame Relay) ili asinhronom prenosnom modu (ATM – Asynchronous Transfer Mode) i time uzrokovali punu mrežnu strukturu privatne WAN mreže, što je, pored kompleksnosti, znatno povećavalo i cenu realizacije ovakve mreže;

– mreža može da bude potpuno ili delimično izolovana od interneta. Postoje dva

tipa praktične realizacije mreže preko koje mogu da se ostvare VPN. To su nadređeni i ravnopravni model VPN mreže.

Nadređeni (Overlay) model VPN mreže i danas je prisutan i predrazumeva da se na svakoj lokaciji korisnika nalazi jedan ili više rutera, koji su sa ruterima na drugim udaljenim lokacijama povezani vezama tačka-tačka, iznajmljenim linijama, ATM ili Frame Relay vezama (sl. 1). Ovaj model efikasno funkcioniše, ali postoji značajan problem skalabilnosti i zahteva koji se postavljaju korisnicima da sami upravljaju ruterima koji održavaju vezu između udaljenih lokacija, kao i problemi promene konfiguracije pri svakom dodavanju novih elemenata.

Ravnopravni (Peer) model VPN mreže treba da omogući isporučiocima servisa opsluživanje veoma velikog broja korisnika i ujedno preuzimanje funkcije administriranja njihovih mreža, tako da oni mogu da se posvete samo svom primarnom poslovanju, ne upuštajući se u pravila IP rutiranja (sl. 2). Model se sastoji od četiri komponente:

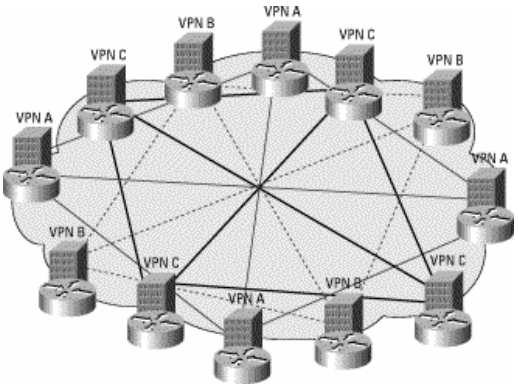
1) ograničene distribucije informacije o rutama,

2) upotreba višestrukih tabela rutiranja,

3) korišćenje novog tipa adresa (VPN – IP adrese), i

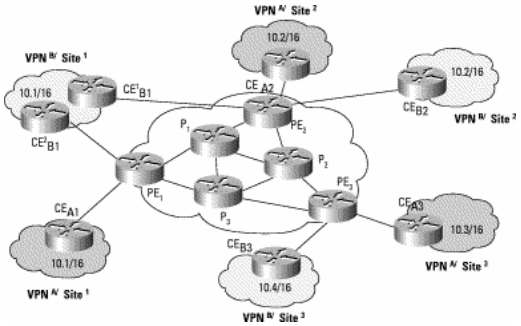
4) upotreba protokola zasnovanog na komutaciji korišćenjem labela – MPLS.

Ravnopravni model će najverovatnije u budućnosti potisnuti nadređeni model. Iako su VPN rešenja zasnovana na ovom drugom modelu prisutna, ovi tipovi rešenja imaju nekoliko velikih problema koji ograničavaju dalji razvoj VPN servisa. Overlay model se zasniva na kreiranju veza, a ne mreža. Svako mesto (čvor) poseduje ruter koji je povezan linkovima tačka-tačka do rutera na drugim mestima unutar VPN. To komplikuje, odnosno povećava broj potrebnih izmena u konfiguraciji pri dodavanju novog čvora u postojeću mrežu. Kod VPN, gde se zahteva potpuna povezanost čvorova u mreži, to uključuje promene u konfiguraciji na svim postojećim čvorovima, zbog toga što je svakom od njih potrebna dodatna veza tačka-tačka do tog novog mesta. Kod VPN izgrađenih na konektivnim mrežama – mrežama sa prenosom okvira ili ATM, bez potpuno izvedenih konekcija između korisnika, skaliranje jednostavno ne daje dobre rezultate.



Sl. 1 – VPN „nadređeni" model

Zbog toga VPN koriste ravnopravni model i nekonektivnu arhitekturu na sloju 3. Ravnopravni model zahteva da korisnički čvor „gleda" na samo jedan ivični ruter (PE – Provider Edge), nasuprot svim drugim korisničkim ruterima (CPE – Customer Premises Equipment) ili krajnjim korisničkim ruterima u istoj VPN. Nekonektivna arhitektura dozvoljava kreiranje VPN na sloju 3, eliminišući potrebu za tunelima, kao što je prikazano na slici 2.



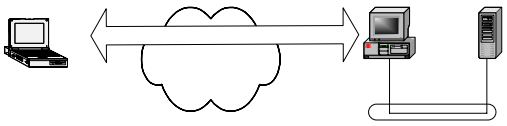
Sl. 2 – VPN „ravnopravni" model

U VPN vezi može da se pojavi sledeći niz događaja, kako je prikazano na slici 3:

1. Dva krajnja korisnika najpre se međusobno autorizuju.

2. VPN server može da odredi kojim uslugama radna stanica ima dozvolu da pristupi i može u saglasnosti sa tim da upravlja saobraćajem koji sledi. Ovaj korak se zove autorizacija.

3. Jednom kada je tunel stvoren, njegove krajnje tačke dodaju posebna zaglavlja paketima koji su adresirani za suprotnu stranu tunela, šifruju originalni paket i zaglavlje i prepakuju sve te informacije u nove IP pakete. Interna zaglavlja obezbeđuju informacije o autorizaciji na nivou paketa i obezbeđuju da se otkrije svako falsifikovanje podataka.



Sl. 3 – Siguran tunel virtuelne privatne mreže

Tunelovanje je najvažnija komponenta tehnologije virtuelnih privatnih mreža i predstavlja prenos paketa podataka namenjenih privatnoj mreži preko javne mreže. Ruteri jedne javne mreže nisu svesni da prenose pakete koji pripadaju privatnoj mreži i VPN pakete kao normalan sadržaj.

Tunelovanje i prepakivanje je metod pri kojem se koristi infrastruktura jednog protokola za prenos paketa drugog protokola. Umesto da se šalju originalni paketi, oni su prepakovani dodatnim zaglavljem. Dodatno zaglavlje sadrži informacije potrebne za rutiranje, odnosno usmeravanje paketa kroz mrežu, tako da novodobijeni paket može slobodno putovati transportnom mrežom.

Tunel predstavlja logičku putanju paketa kojom se on rutira preko mreže. Prepakovani podaci su rutirani transportnom mrežom sa jednog kraja tunela na drugi. Pojam tunel se uvodi jer su podaci koji putuju tunelom razumljivi samo onima koji se nalaze na njegovom izvorištu i odredištu. Ovi paketi se na mreži rutiraju kao svi ostali paketi.

Početak i kraj tunela nalaze se u VPN mrežama. Kada prepakovani paket stigne na odredište vrši se raspakivanje i prosleđivanje na konačno odredište. Ceo proces prepakivanja, transporta i raspakivanja paketa naziva se tunelovanje.

Opcije veze

Kada se koristi prenosni računar postoji nekoliko načina za korišćenje prednosti VPN tehnologije da bi se ostvarila veza sa mrežom u svojoj jedinici:

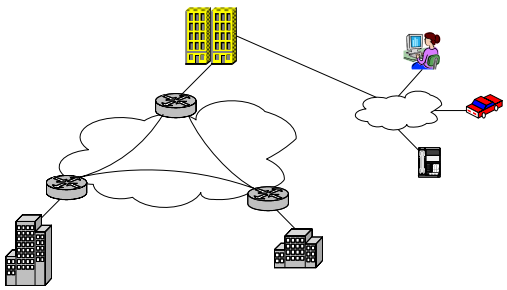
– modemska veza sa lokalnim posrednikom internet usluga. Upotreba PC modemske kartice radi ostvarivanja veze postojećim zemaljskim linijama do lokalnog posrednika internet usluga, uspostavljavanje dogovora po sistemu od tačke do tačke (PPP – Point-to-Point Protocol) i uspostavljanje VPN veze preko interneta;

– celularna komutirana veza sa lokalnim posrednikom internet usluga. Ovaj pristup je gotovo isti kao kada se koristi veza preko zemaljskih linija, izuzev što je ostvarena preko analogne veze ili veze na bazi komutacije kola;

– celularna komutirana veza direktno na internet. Povezivanje na internet preko direktne digitalne veze, a ne preko modemskog pristupa. Ovakve usluge tek predstoje.

Mreže VPN na drugom sloju (Frame Relay, ATM)

Mreže VPN na drugom sloju (u daljem tekstu 2L VPN) obuhvataju mreže realizovane korišćenjem resursa Frame Relay i ATM mreža, što se može videti na slici 4.



Sl. 4 –VPN mreže na drugom sloju

Javne mreže, kao što su FR ili ATM, mogu prenositi multimedijalne poruke uključujući glas, video i podatke. Ovaj tip VPN koristi usluge javne komutirane mreže za prenos podataka, PVC ili obilaženje virtuelnih prekidača (SVC – Switched Virtual Circuit) za razdvajanje saobraćaja razlilčitih korisnika. Paketi podataka ne moraju biti IP, niti moraju biti šifrovani. Opciono se mogu koristiti autentifikacija i šifrovanje, pri čemu identitet korisnika i integritet podataka ostaje zagarantovan. VPN bazirani na javnim komutiranim mrežama za prenos podataka pružaju potpunu kontrolu usluga. U većini slučajeva su raspložive i dodatne usluge, kao što je opcija kvalitet servisa (QoS – Quality of Service). Ovaj tip VPN naročito je popularan u Evropi, gde su javne komutirane mreže za prenos podataka široko dostupne, a poslovno korišćenje interneta je manje razvijeno.

Frame Relay je protokol od kraja-do-kraja koji može raditi preko različitih pristupnih tehnologija, kao što je digitalni servis integrisanih mreža (ISDN – Integrated Services Digital Network), linija sa digitalnom pretplatničkom vezom (DSL – Digital Subscriber Line) ili običan stari telefonski servis sa povećanim brojem linija (POTS – Plain Old Telephone Service) dial-up linije. Nove pristupne metode, kao što su SVC ili ISDN pristup, govore da je FR sada pouzdanije i isplativije rešenje za globalne VPN usluge.

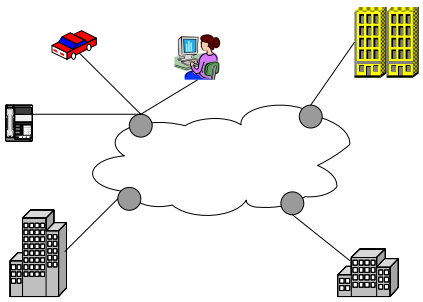
Mreže VPN na trećem sloju (IP VPN mreže)

Nagli globalni razvoj interneta otvorio je mogućnost izgradnje VPN mreža realizovanih direktno na bazi IP protokola sa trećeg sloja OSI modela (u daljem tekstu 3L VPN). Osnovna prednost ovakvih VPN mreža nad 2L VPN mrežama je posledica globalnog karaktera interneta (internet je prisutan svuda za razliku od Frame Relay i ATM mreža), a donosi i dodatnu redukciju troškova. Mreže se grade šifrovanim tunelima koji imaju istu funkciju koju su imali i virtuelna kola u 2L VPN mrežama.

RAS
server

Rad od

Mreže 3L VPN dele se na: internet VPN i IP VPN mreže.



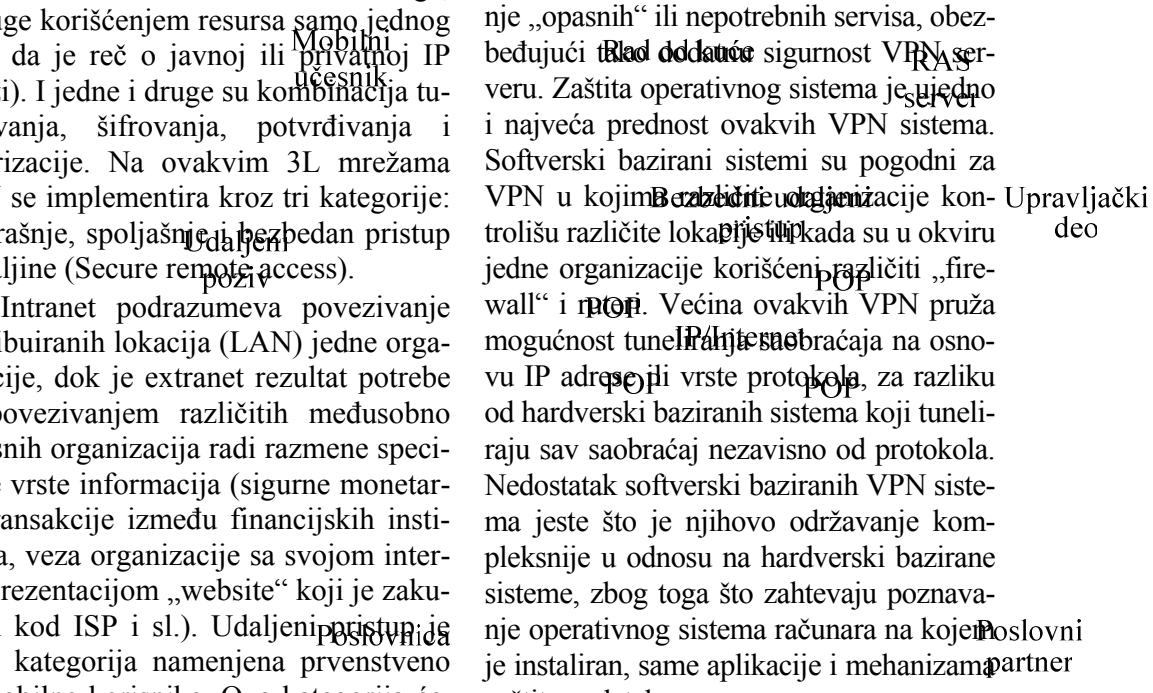
Sl. 5 – IP/Internet VPN mreže

Prve su realizovane korišćenjem infrastrukture dva ili više davalaca usluge, a druge korišćenjem resursa samo jednog (bilo da je reč o javnoj ili privatnoj IP mreži). I jedne i druge su kombinacija tunelovanja, šifrovanja, potvrđivanja i autorizacije. Na ovakvim 3L mrežama VPN se implementira kroz tri kategorije: unutrašnje, spoljašnje i bezbedan pristup sa daljine (Secure remote access).

Intranet podrazumeva povezivanje distribuiranih lokacija (LAN) jedne organizacije, dok je extranet rezultat potrebe za povezivanjem različitih međusobno zavisnih organizacija radi razmene specifične vrste informacija (sigurne monetarne transakcije između financijskih institucija, veza organizacije sa svojom internet prezentacijom „website“ koji je zakupljen kod ISP i sl.). Udaljeni pristup je treća kategorija namenjena prvenstveno za mobilne korisnike. Ova kategorija će, dugoročno gledano, zameniti široko rasprostranjene servise za daljinski pristup (RAS – Remote Access Service), prvenstveno zbog znatnog smanjenja troškova telefonskih poziva s obzirom na to da su svi pozivi lokalni, odnosno pozivi do najbliže tačke pristupa davaoca usluge (PoP – Point of Presence), održavanje servera je prepušteno davaocu usluge (sl. 5).

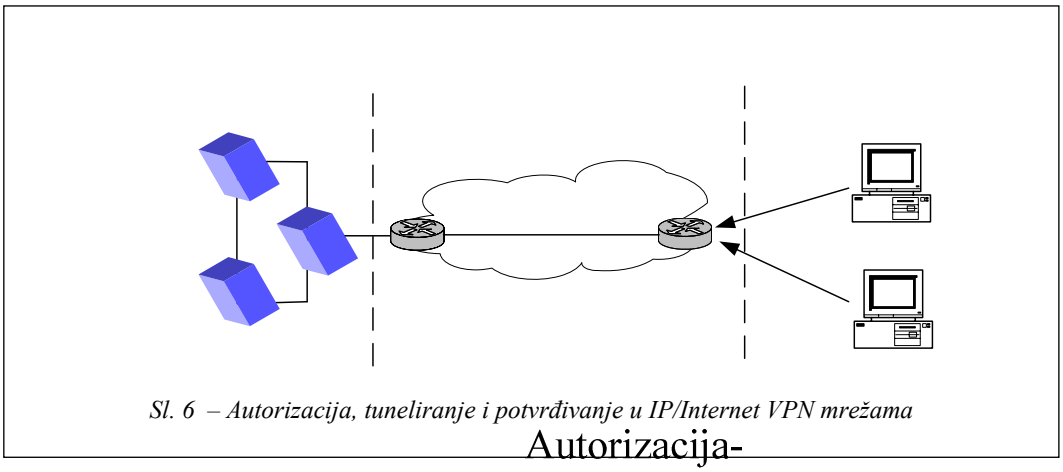
Prema konkretnoj realizaciji 3L VPN se dele na: hardverski bazirane, softverski bazirane i bazirane na principu otvoreno – zatvoreno (Firewall) i VPN aplikacione pakete.

Većina hardverski baziranih sistema realizovana je pomoću rutera koji kriptuju podatke. Oni su sigurni i laki za implementaciju i obezbeđuju najveći mrežni transfer podataka od svih VPN sistema. „Firewall“ bazirani sistemi koriste prednosti ovog mehanizma, kao što su: restrikcije pristupa u intranet, translacije adresa i onemogućavanje „opasnih“ ili nepotrebnih servisa, obezbeđujući tako dodatnu sigurnost VPN serveru. Zaštita operativnog sistema je ujedno i najveća prednost ovakvih VPN sistema. Softverski bazirani sistemi su pogodni za VPN u kojima se zahteva da svaka od organizacije kontrolišu različite lokacije ili kada su u okviru jedne organizacije korišćeni različiti „firewall“ i router. Većina ovakvih VPN pruža mogućnost tuneliranja saobraćaja na osnovu IP adrese ili vrste protokola, za razliku od hardverski baziranih sistema koji tuneliraju sav saobraćaj nezavisno od protokola. Nedostatak softverski baziranih VPN sistema jeste što je njihovo održavanje kompleksnije u odnosu na hardverski bazirane sisteme, zbog toga što zahtevaju poznavanje operativnog sistema računara na kojem je instaliran, same aplikacije i mehanizama zaštite podataka.



Realizacija IP VPN mreža

Mreže IP VPN mogu se posmatrati kao skup tuneliranja, šifrovanja, potvrđivanja i autorizacije, kao što je prikazano na slici 6.



Sl. 6 – Autorizacija, tuneliranje i potvrđivanje u IP/Internet VPN mrežama

Integritet 3L VPN mreža obezbeđuje se izgradnjom „sigurnih tunela“ kroz javne IP komunikacione kanale korišćenjem L2TP (2L Tunneling Protocol), L2F (2L Forwarding), PPTP (Point to Point Tunneling Protocol) ili IPSec (Internet Protocol Security) protokola.

Za razliku od prva tri protokola koji uspostavljaju konekciju na drugom nivou i od kojih ni jedan ne uključuje šifrovanje korisničkih podataka, IPSec je skup protokola i procedura za uspostavu, održavanje i završavanje zaštićenih komunikacionih kanala kroz javnu IP mrežu uz potvrđivanje i servise za šifrovanje na IP mrežnom nivou, tako da kroz IP tunele prolaze kriptovani podaci [2]. Definisana su četiri različita načina transmisije podataka kroz IP/Internet mreže (slika 7):

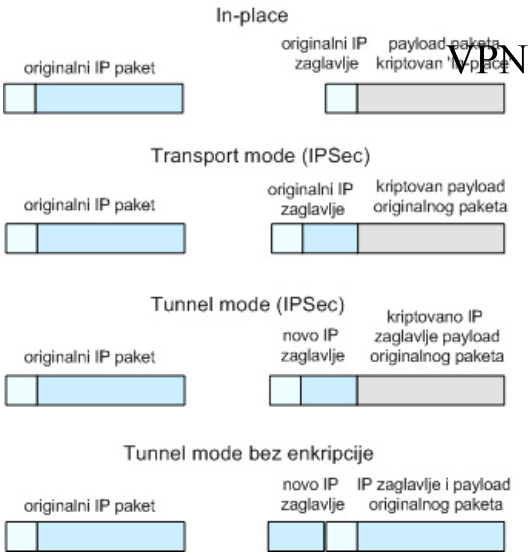
– bez promene – rešenje koje je specifično za različite proizvođače, a kriptuju se samo podaci i nema promene veličine paketa,

– prenosni mod – kriptuju se samo podaci, ali se povećava veličina paketa,

– šifrovani tunel mod – IP zaglavlje se kriptuje zajedno sa podacima, a paketu se dodaje novo IP zaglavlje koje kao odredišnu adresu nosi adresu izlaznog VPN uređaja. To je najbolje rešenje koje daje najbolju zaštitu korisničkih podataka,

– otvoreni tunel mod – ništa se ne kriptuje, ali se dodaje novo IP zaglavlje.

Ukoliko se ne vrši šifrovanje podataka u IP/Internet VPN mrežama adekvatnije je koristiti termin Virtual Network (VN), jer je „privatnost“ u ovakvim mrežama pod znakom pitanja.



Sl. 7 – Obrada originalnog IP paketa u 3L VPN mrežama

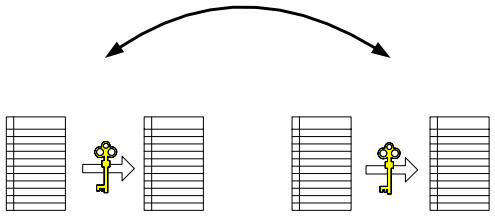
Transmisija nekriptovanog teksta kroz internet može biti veoma opasna. Podaci mogu biti pročitani pomoću neke od „sniffing“ tehnologija. Razvijeni su alati kao što su „protokol analyzer“ ili mrežni dijagnostički alati ugrađeni u današnje operativne sisteme koji lako mogu pročitati nekriptovane podatke. Proces šifrovanja, dešifrovanja i učesnici u njemu (pošiljalac i primalac) čine kriptosistem. Postoje dva tipa kriptosistema: privatni sa simetričnim ključem (private (symmetric) key) i javni sa asimetričnim ključem (public (asymmetric) key).

Simetrični algoritmi su najčešći u kriptografiji. Koriste složene algoritme i isti ključ za šifrovanje i dešifrovanje. Operišu nad blokovima kodiranog otvorenog teksta određene dužine. Svoju sigurnost uglavnom baziraju na kvalitetu i dovoljnoj dužini ključa. Šifruju sve digitalne podatke, uključujući i e-mail, telnet konekcije, zvuk i sliku.

Neki od tih algoritama poznati su javnosti u celini ili delimično, i time su izloženi sveobuhvatnom i dugotrajnom ispitivanju. Drugi se čuvaju u tajnosti i tako izbegavaju javnu ocenu svoje sigurnosti. Danas postoji mnogo simetričnih algoritama različitih po brzini, veličini bloka, dužini ključa, patentnim i licencnim pravima. Neki od poznatijih su DES (Data Encryption Standard), podvrsta Triple DES (3DES), RC4–40, CAST–40, DES–40 i drugi.

Kao i kod svih konvencionalnih sistema i kod simetričnih algoritama ključ za šifrovanje i ključ za dešifrovanje su isti i njime blagovremeno, sigurnim kanalom iz jednog izvora, moraju biti snabdeveni i pošiljalac i primalac. Na putu prenosa informacije, protivničkom kriptoanalitičaru – prisluškivaču – dostupna je samo zaštićena poruka, a njena sigurnost kod ovakvih sistema gotovo isključivo zavisi od ključa.

Na slici 8 prikazan je jednostavan primer putanje podatka u simetričnom algoritmu kriptosistema. U ovom primeru, pošiljalac šifruje poruku „abc“ koristeći tajni ključ, i pretvara ovu poruku u „!&#“. Svako ko ima isti tajni ključ može dešifrovati poruku „!&#“ nazad u originalnu poruku „abc“.



Sl. 8 – Primer simetričnog algoritma

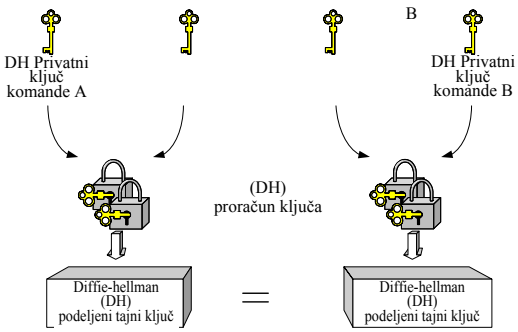
Najveći problemi ovih kriptosistema su u distribuciji ključeva šifrovanja, koji su osnova konvencionalnih sistema, i u utvrđivanju verodostojnosti poruke. Kriptosistemi javnih ključeva rešavaju upravo ove probleme.

Asimetrični algoritmi, tj. algoritmi sa javnim ključevima, za šifrovanje i dešifrovanje koriste različite ključeve, vezane izvesnim transformacijama, ali tako da se jedan iz drugog ne mogu dobiti bez poznavanja specijalne informacije. Kod ovih sistema i pošiljalac i primalac, svaki za sebe, generišu po par odgovarajućih ključeva, ključ za šifrovanje (javni) i ključ za dešifrovanje (tajni, lični). Prima-

lac sada šalje svoj ključ za šifrovanje pošiljaocu, slobodno, nezaštićenim kanalom, a ovaj mu njime šifruje poruku. Niko sem primaoca nema ključ za dešifrovanje i jedino on može da je dešifruje. Javni ključ je dostupan svima, ali je računski neostvarivo da se iz njega dobije tajni ključ.

Ipak, postoji mogućnost da se neko lažno predstavi i pošalje poruku umesto nekog drugog. Takođe je moguće da neko presretne javni ključ i umesto njega podmetne svoj, pa će na taj način moći da pročita poruku. I za takve slučajeve kriptosistem javnih ključeva ima rešenje. Ako osoba koja komunicira ovim sistemom želi i verifikaciju, tj. proveru autentičnosti poruke, ona može od drugog korisnika da zahteva da svoju poruku, koju je šifrovao javnim ključem primaoca, šifruje i svojim tajnim ključem. Pri prijemu, on proverava autentičnost dešifrući poruku javnim ključem drugog korisnika, a onda je otvara dešifrući svojim tajnim ključem.

Dva javna ključa kriptosistema koja se obično koriste sa virtuelnim privatnim mrežama danas su Diffie-Hellman (DH) i Rivest Shamir Adlemen (RSA). Na slici 9 prikazan je jedan ovakav sistem.



Sl. 9 – Primer javnog ključa (asimetričnog) algoritma

Takođe je važno da se obezbedi da su korisnici baš oni za koje se predstavljaju. Internet Protocol Security (IPSec) okosnica je otvorenog standarda, koji je razvio IETF (Internet Engineering Task Force) da osigura privatnost podataka, potvrđivanje podataka i korisnika na javnoj mreži.

Razvijena su dva vida potvrđivanja: potvrđivanje korisnika i podataka. Potvrđivanje podataka je ređe prisutno u primenjenim sistemima i podrazumeva identifikaciju VPN uređaja koji šalje podatke kao i potvrdu da oni nisu menjani pri prenosu. Potvrđivanje korisnika koji koristi VPN mrežu je češće korišćen metod. Najčešće se koriste sistemi koji podržavaju RADIUS, TACACS/TACACS+ ili LDAP autentifikacioni servis.

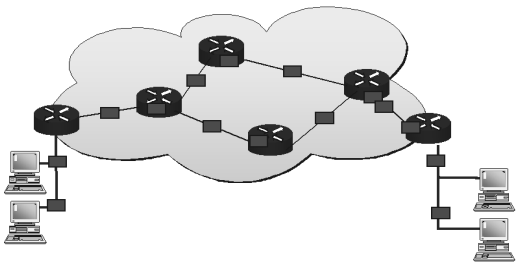
Nakon potvrđivanja identiteta osobe koja koristi VPN, njegov ranije definisan profil određuje servise i aplikacije koje može koristiti, tako da mu se omogućava korišćenje samo onih resursa VPN za koje je autorizovan. Autorizacija koja se radi u odnosu na servis podržava: internet servise (Web browser, mail, FTP (File Transfer Protocol), Telnet i sl.)), kompletnu TCP (Transmission Control Protocol) familiju, zatim RPC (Remote Procedure Call) ili UDP (User Datagram Protocol) bazirane aplikacije.

Ono što svaki korisnik očekuje od vlastite mreže je određeni nivo kvaliteta, sigurnost i raspoloživost. Ukoliko je kvalitet i raspoloživost internet konekcija i bio diskutabilan poslednjih godina, stanje se značajno menja iz dana u dan, stalnim proširivanjem internet jezgra i novim servisima, kao što su diferencijalni servis (DiffServ – Differentiated Service) koji kvalitativno menjaju celu sliku. Sa ova-

kvim alatima IP davaoci usluge sada su u mogućnosti da garantuju određeni nivo kvaliteta definisan kroz ugovoreni nivo usluga, SLA (Service Level Agreement), što je do skoro bila osnovna prednost 2L mreža. I uz sve alate koji treba da obezbede sigurnost podataka u IP/Internet VPN mrežama, to i dalje ostaje osnovni problem ovako realizovanih mreža, što je posledica arhitekture samog interneta koji je osmišljen kao mreža u kojoj podaci treba da budu dostupni svima.

Mreže VPN u MPLS

Komutacija polja podataka (labela) višestrukim protokolom, MPLS, predstavlja arhitekturu u okviru IETF standarda koja omogućava upravljanje saobraćajem i QoS podršku koji postoje kod ATM mreža, čijom primenom se ubrzava prosleđivanje paketa. Prosleđivanje paketa vrši se na osnovu polja podataka (etiketa) kratke dužine koje se smeštaju između zaglavlja sloja linka podataka i sloja mreže. Rezultat je formiranje mreže prosleđivanja bazirane na internet protokolu, sa kraćim vremenom konekcije, s obzirom na to da se rutiranje vrši duž označenih („etiketiranih“) putanja. Na slici 10 prikazana je jedna tipična IP mreža sa saobraćajem bez specificiranih ruta.



Sl. 10 – Izgled klasične IP mreže

MPLS predstavlja način za suočavanje sa problemima upravljanja kapacitetom i zahtevima servisa sledeće generacije mreža internet jezgra baziranih na IP, problem TE (Traffic engineering). Primena MPLS povezana je sa sposobnošću nivelisanja podataka (scalability), odnosno mogućnošću jednostavnih izmena u mreži, kako bi se omogućio rad sa novijim tehnologijama i platformama, i rutiranjem (zasnovane na QoS i metrici kvaliteta servisa) i može egzistirati preko postojećih ATM i FR. Pored toga, MPLS smanjuje potrebno procesiranje po paketu koje je potrebno kod svakog rutera u mreži sa IP, povećavajući još više performanse rutera. Još značajnije, MPLS omogućava nov kvalitet u četiri oblasti koje obezbeđuju njegovu popularnost: QoS podrška, upravljanje saobraćajem, mogućnost realizacije VPN i multiprotokolska podrška. Univerzalna priroda MPLS najviše odgovara korisnicima koji poseduju kombinovane mrežne tehnologije, traže način za optimiziranjem resursa i mogućnosti proširenja QoS podrške. To je moguće ako se poznaje činjenica da se MPLS može primeniti na mnogobrojnim mrežnim tehnologijama, kao i da MPLS osposobljeni ruteri mogu da „komuniciraju“ sa običnim IP ruterima, a isto važi i za komutatore koji se mogu prekonfigurisati radi podrške datog protokola.

MPLS obavlja sledeće funkcije:

– definiše mehanizme upravljanja saobraćajnim tokovima različite prirode, kao što su tokovi između različitog hardvera ili između različitih aplikacija;

– ostaje nezavisan od protokola na slojevima 2 i 3;

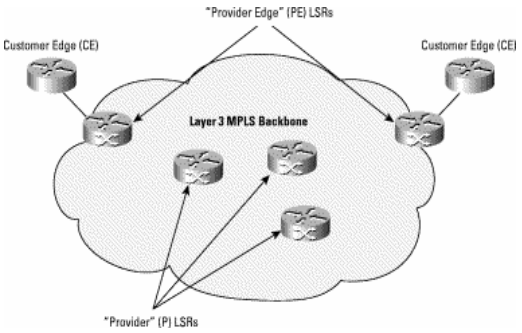
– omogućava mapiranje IP adresa u jednostavne labele fiksne dužine koje se koriste od strane različitih tehnologija prosleđivanja i komutacije paketa;

– podržava IP, ATM, i protokole za prenos okvira na sloju 2.

MPLS obezbeđuje efikasan mehanizam za podržavanje VPN. Sa VPN saobraćaj određene grupe korisnika prolazi transparentno kroz mrežu na način koji ga uspešno razvrstava od ostalih paketa u mreži, pružajući garancije u pogledu performansi i sigurnosti.

Ove mreže moraju da budu skalabilne, ekonomične i sposobne da izađu u susret širokom opsegu zahteva korisnika, gde spadaju pouzdanost i sigurnost, kvalitet servisa i mogućnost povezivanja svakog sa svakim. One moraju da ponude kompletno pružanje multimedijalnih servisa kako bi privukle nove korisnike. MPLS se javlja kao ključna tehnologija za mreže nove generacije, posebno u optičkim mrežama. VPN bazirane na MPLS obezbeđuju fleksibilnu povezanost i skalabilnost, što su odlike mreža sa IP, kao i tajnost i QoS kao odlike ATM i mreža sa štafetnim prenosom okvira (FR).

S obzirom na to da MPLS bazirane VPN umanjuju kompleksnost i cenu mreže, one dozvoljavaju davaocima servisa da svoje usluge pružaju mnogo raznovrsnijoj bazi malih i srednjih organizacija i ustanova. Za realizaciju MPLS VPN mreža dovoljna je samo jedna konekcija od njihovog rutera do krajnjeg rutera provajdera. Krajnji ruter stavlja labele na pakete i prenosi ih kroz MPLS jezgro sve do krajnjeg rutera najbližeg odredištu. Sa ovom tehnologijom, davaoci servisa sada mogu ponuditi korisnicima VPN sa QoS, omogućenim internetom, intranetom i ekstranetom, i paketskom telefonijom bez kompleksnosti koje su ove aplikacije prethodno zahtevale kako bi proširile servisne ponude i stvorile dodatne prihode.



Sl. 11 – VPN mreža bazirana na MPLS

Komponente koje sačinjavaju MPLS VPN mrežu prikazane su na slici 11. Na krajevima mreže nalaze se ruteri ka opremi korisnika (CE – Customer Edge). Ovi ruteri su deo korisničke mreže i nemaju saznanja o VPN. Ivični (PE – Provider Edge) ruteri dobijaju putanje od rutera korisnika i prenose ih do drugih PE rutera preko MPLS okosnice servisnog provajdera. U sredini mreže nalaze se ruteri provajdera (u daljem tekstu P ruteri), ili ruteri za komutaciju labela (LSR – Label Switched Routers), koji implementiraju MPLS transportni servis na trećem sloju. Važno je napomenuti da ruteri provajdera na okosnici „nemaju saznanja“ o VPN i zbog toga pružaju mnogo veću skalabilnost. Informacije u vezi sa VPN potrebne su samo za PE rutere, i mogu biti raspodeljene između PE rutera. PE ruteri moraju da znaju informacije vezane za VPN prosleđivanje samo za one VPN u kojima su direktne veze.

Između korisničkih tačaka u VPN ne mora nužno postojati veza jedan ka jednom. Dato korisničko mesto može biti član višestrukih VPN. Međutim, to mesto može biti u vezi samo sa jednim zahtevom za rutiranje/prosleđivanje (VRF – VPN routing/forwarding instances). Na nekom korisničkom mestu VRF sadrži sve putanje dostupne tom mestu u VPN čiji je član.

Sigurnost MPLS VPN mreža

Današnji poslovni korisnici zadovoljni su stepenom sigurnosti koje pružaju Frame Relay i ATM kao VPN tehnologije sa drugog sloja. Međutim, u poslednje vreme sve više se javlja interesovanje u vezi sa stepenom sigurnosti koje pružaju MPLS bazirane VPN [3], [4].

Poređenjem MPLS VPN baziranih rešenja sa tradicionalnim VPN rešenjima sa drugog sloja, kao što su Frame Relay i ATM postavlja se nekoliko ključnih sigurnosnih zahteva:

– neophodno je posedovati odvojeno adresiranje i usmeravanje,

– interna struktura jezgra mreže mora biti skrivena od spoljnog sveta kao što je u slučaju Frame Relay i ATM mrežnog jezgra i

– mreža mora biti otporna na napade tipa otkaza (DoS – Denial of Service) i napade tipa upada.

1) *Adresni prostor i odvojeno usmeravanje*

Odvojeno adresiranje implicira da dve nezavisne VPN mreže poseduju potpuno odvojene adresne prostore. Sa aspekta usmeravanja to znači da svaki krajnji sistem u VPN mreži ima jedinstvenu adresu, tako da se u istom VPN ne mogu pojaviti dve strane koje dele isti adresni prostor. ATM i Frame Relay nemaju problem sa implementacijom ovih svojstava s obzirom na to da nikad ne vrše proveru informacija na trećem sloju već se odluka o prosleđivanju donosi na osnovu kriterijuma sa drugog sloja, kao što su identifikatori konekcije linka podataka (DLCI – Data Link Connection Identifiers) i identifikatori virtuelne putanje/identifikatori virtuelnog kanala (VPI/VCI – Virtual Path Identifiers/Virtual Channel Identifiers).

MPLS uzima u obzir 3L deo paketa, ali istovremeno omogućava da nekoliko VPN koristi isti adresni prostor. MPLS VPN omogućava korišćenje javnog ili privatnog adresiranja. To je moguće ostvariti dodavanjem 64-bitnog identifikatora putanje, RD (Route Distinguisher) za svaku IPv4 putanju. Ova nova putanja, tzv. VPN IPv4 adresa, osigurava jedinstvenost VPN adrese i u MPLS jezgru. Jedini izuzetak predstavlja IP adresiranje PE ili CE linkova koji moraju biti jedinstveni ako se koriste protokoli za dinamičko usmeravanje.

MPLS obezbeđuje odvajanje putanja tako da svaki PE ruter održava posebnu tabelu usmeravanja za svaki povezani VPN. Ova tabela usmeravanja, tzv. VRF (Virtual Routing and Forwarding) instanca, sadrži putanje s jedne VPN koje su definisane statistički ili kroz dinamički protokol usmeravanja. Dodavanjem jedinstvenih VPN identifikatora kao što je RD, multiprotokolni BGP (Bridge Gateway Protocol) obezbedio je mogućnost

jedinstvenog identificiranja VPN putanja kroz jezgro mreže. PE ruteri međusobno razmenjuju informaciju i zatim je smeštaju u poseban VRF unutar VPN. Korišćenjem ovih svojstava moguće je ostvariti odvojeno usmeravanje kroz MPLS mrežu za svaki VPN.

2) *Sakrivanje jezgrenog dela mreže davaoca usluga*

Za davaoce usluga i korisnike nije poželjno da interna topologija mreže bude vidljiva iz spoljnog sveta. Bez poznavanja mrežne topologije napadač može jedino pretpostaviti IP adresu koju napada, što čini mrežu komplikovanijom za napad. U ovom trenutku pomenuto svojstvo poseduju 2L VPN mreže, kao što su Frame Relay i ATM. Između mreže davaoca usluga i korisničke mreže jedino se razmenjuje informacija o korisničkim virtuelnim kanalima, VC. To korisniku ograničava uvid u topologiju mreže davaoca usluga. Korisnik poznaje jezgreni deo mreže jedino na osnovu informacije koju prima na temelju VC.

Ista zamisao se prenosi i na korisničke mreže, kao i na MPLS jezgro. MPLS ne otkriva dodatne nepotrebne informacije čak ni korisničkim VPN. Kako je interfejs prema VPN BGP, nema potrebe odavati bilo kakvu informaciju o jezgrenom delu mreže. Jedina informacija neophodna u slučaju ruting protokola između PE i CE je adresa PE rutera. Ako to nije poželjno, može se konfigurisati statičko usmeravanje između PE i CE. Na taj način se MPLS jezgro može u potpunosti sakriti i adresirati korišćenjem javne ili čak privatne adrese.

3) *Otpornost na napade*

Bilo da je u pitanju 2L VPN ili MPLS VPN, mreža davaoca usluge treba da bude otporna na napade. Napadi unutar VPN trebalo bi da budu obuhvaćeni unutar istog VPN, bez uticaja na rad drugih VPN. Napadač ne bi trebalo da bude u mogućnosti da pristupi ostalim VPN ili mreži davaoca usluge. Otpornost na napade obuhvata napade tipa otkaza, pri čemu resursi postaju neraspoloživi ovlašćenim korisnicima, kao i napade tipa upada ili neovlašćenog pristupa. Kako je većina DoS napada bazirana na 3L svojstvima, Frame Relay i ATM nisu praktično osetljivi na ovaj tip napada. Ako bi se napad ipak počinio, to bi bila interna stvar VPN mreže, jer bi mreža jednostavno prosledila napadnute pakete bez provere DLCI ili VPI/VCI para.

Međutim, MPLS tehnologija dozvoljava tu vrstu napada, kao i napad na MPLS jezgro, pri čemu postoje dva osnovna načina napada MPLS jezgra mreže: direktni pokušaj napada PE rutera i pokušaj napada MPLS signalizacionim mehanizmima.

Direktni napad PE rutera

Da bi mogao da se izvrši direktni napad PE rutera neophodno je poznavati njegovu adresu. Moguće je sakriti adresnu strukturu MPLS jezgra mreže od spoljnog sveta, osim kada se koristi dinamički protokol usmeravanja.

Ako napadač ne poznaje IP adresu bilo kojeg rutera u jezgru, mora je pogoditi kako bi poslao pakete. Zbog odvojenog adresiranja, svaki ulazni paket tretira se kao da pripada korisničkom adresnom

prostoru. Zbog toga je vrlo teško pristupiti internom ruteru, čak i pri pogađanju IP adresa.

Ako napadač poznaje IP adresu rutera koji želi napasti, postoji veliki broj načina da se poremete servisi datog rutera. U praksi se pristup PE ruteru preko CE–PE interfejs može ograničiti na odgovarajući protokol rutiranja korišćenjem kontrolnih lista pristupa. To ograničava tačku napada na jedan protokol usmeravanja, na primer RIP (Routing Information Protocol) ili BGP. Potencijalni napad bi mogao biti poslat na veliki broj putanja ili se prosleđivati PE ruteru pri svakom ažuriranju putanja. I u jednom i u drugom slučaju to dovodi do DoS napada, ali ne i do napada tipa neovlašćenog pristupa. Da bi se ograničio ovaj pristup, neophodno je konfigurisati protokol usmeravanja na PE ruteru na što sigurniji način.

Generalno, nije moguće pristupiti iz jednog VPN drugom VPN. Teoretski je moguće iskoristiti ruting protokol za izvođenje DoS napada na PE ruterima koji mogu imati negativan uticaj na druge VPN. Međutim, ako PE ruteri vrše pravilno filtriranje, ne postoji mogućnost pretnji ove vrste. PE ruteri moraju biti posebno sigurni, naročito na interfejsima prema CE ruterima. Kontrolne pristupne liste bi trebalo da budu konfigurisane da ograniče pristup samo ka portovima ruting protokola i pristup sa CE rutera.

Ometanje MPLS labela

U jezgru MPLS mreže paketi se ne prosleđuju na bazi IP odredišne adrese, nego na temelju labela koje se dodeljuju na PE ruterima. Kao i kod IP spoofing napada u kojima napadač zamenjuje izvorišnu ili odredišnu IP adresu paketa, teoretski je moguće zameniti i labelu MPLS paketa.

U Frame Relay i ATM mrežama to bi bilo ekvivalentno umetanju DLCI ili VPI/VCI para. Međutim, ako ovi DLCI ili VPI/VCI parovi nisu konfigurisani na specifičnom portu dolazi do odbacivanja saobraćaja.

U MPLS interfejs između CE rutera i njegovog partnerskog PE rutera je IP interfejs, odnosno interfejs bez labela. CE ruter nije svestan MPLS jezgra i ponaša se kao da šalje IP pakete ka običnom ruteru. „Inteligencija“ je prisutna u PE uređaju gde se na temelju konfiguracije odabira i dodaje labela paketu. To je uobičajeno za sve PE rutere. Svi interfejsi ka MPLS okruženju zahtevaju samo IP pakete, bez labela. Iz sigurnosnih razloga PE ruter ne sme nikada da prihvati paket sa labelom od CE rutera. Implementacija „Cisco“ rutera je takva da se odbacuju labelirani paketi koji pristižu na bilo koji interfejs koji onemogućava komutaciju labela [5]. Na taj način nije moguće umetnuti „lažne“ labele, jer ni jedna labela neće biti prihvaćena.

Ostaje mogućnost zamene IP adrese paketa koji se šalje prema MPLS jezgru. Međutim, pošto postoji strogo odvajanje adresiranja unutar PE rutera i svaki VPN ima vlastiti VRF, jedino se može oštetiti VPN iz kojeg dolazi paket. Drugim rečima, VPN korisnik može napasti sam sebe. MPLS ne dodaje bilo kakav sigurnosni rizik, pošto mreža davaoca usluge nije ugrožena, tako da se neće uticati na uslugu prema ostalim VPN. Odgovornost ispravne zaštite CE rutera isključivo pripada korisniku.

Kako je nemoguće umetnuti „spoofed“ labelu u MPLS mrežu i tako pristupiti drugom VPN ili MPLS jezgru, MPLS bazirani VPN obezbeđuje isti nivo sigurnosti kao i Frame Relay ili ATM bazirani VPN.

Zaključak

Sa aspekta vojne primene treba naglasiti da savremeni načini ratovanja zahtevaju brz prenos informacija u realnom vremenu s obzirom na uslov da je podatak koristan samo ako je pravovremen i pouzdan. Razvojem informatičke podrške prenos govora je postao trivijalan, dok se u prvi plan stavljaju podaci i multimedija, što postojeći sistem veza Vojske ne može da zadovolji. Opremanje Vojske novim sredstvima postaje sve teže, a veliki broj tehnoloških koraka već je preskočen, što u velikoj meri otežava moguću kupovinu novih sistema.

Mreže zasnovane na IP tehnologiji sa uvođenjem komutacije predstavljaju budućnost modernih telekomunikacija i mogu u velikoj meri zadovoljiti potrebe prenosa različitih vrsta informacija u Vojsci. Stvaranje komutacione platforme u komandnim i informacionim sistemima otvara velike mogućnosti stvaranja pouzdane virtuelne privatne mreže za vojne potrebe (slika, podaci, multimedija, video konferencija, itd.). Posebnu pažnju u ovakvim sistemima treba posvetiti odgovarajućoj zaštiti, kako softverskoj, tako i hardverskoj, s obzirom na značaj podataka koji se ovim putem prenose. U mogućoj realizaciji jednog ovakvog komunikacionog sistema, a s obzirom na postojeće stanje u Vojsci, odgovarajuća podrška trebalo bi da se potraži među ostalim imaocima telekomunikacionih sredstava na našoj teritoriji. Činjenica je da su u ovom trenutku, u segmentima vezanim za ovu problematiku, mnogi od njih opremljeniji od Vojske, iako bi situacija trebalo da bude obrnuta. Na taj način sigurno bi se uštedela i velika materijalna sredstva, a mogao bi se dobiti jedan dobar i pouzdan komunikacioni sistem koji bi mogao da zadovolji sve veće potrebe savremene vojske.

Literatura:

[1] International Technical Support Organization, A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management, November 1999.
[2] Stallings, W.: Cryptography and Network Security, Prentice Hall, 1998.
[3] Rosen, E., Rekhter, Y.: BGP/MPLS IP Virtual Private Networks (VPNs), RFC 4364, February 2006.
[4] http://www.netcraftsmen.net/
[5] http://www.cisco.com/