SVEUČILIŠTE U RIJECI

TEHNIČKI FAKULTET

Preddiplomski stručni studij elektrotehnike

Završni rad

PRIMJENA GRE TUNELA U RAČUNALNIM MREŽAMA

Josip Dobrić

0069049422

Rijeka, svibanj 2016.

SVEUČILIŠTE U RIJECI

TEHNIČKI FAKULTET

Preddiplomski stručni studij elektrotehnike

Završni rad

PRIMJENA GRE TUNELA U RAČUNALNIM MREŽAMA

Mentor: Doc. dr. sc Mladen Tomić

Josip Dobrić

0069049422

Rijeka, svibanj 2016.

TEHNIČKI FAKULET
Povjerenstvo za završne ispite
preddiplomskog stručnog studija elektrotehnike
Br.: 602-04/15-14/15
Rijeka, 06.03.2015.

ZADATAK
za završni rad

Pristupnik: Josip Dobrić

Matični broj: 0069049422
Lokalni matični broj: 11800022

Naziv zadatka: **PRIMJENA GRE TUNELA U RAČUNALNIM MREŽAMA**

Naziv zadatka na engleskom jeziku: **GRE TUNNEL APPLICATIONS IN COMPUTER NETWORKS**

Sadržaj zadatka:

Proučiti način rada GRE tunela. Analizirati i objasniti potrebu njegova korištenja i najčešće primjene. Objasniti probleme koji se rješavaju njegovom primjenom te usporediti s drugim rješenjima. Usporediti VPN mreže korištenjem IPSec tunela u odnosu na GRE over IPSec. Implementirati testni primjer na mrežnoj opremi.

Zadano: 17.03.2015.

Mentor:
Doc. dr. sc. Mladen Tomić

Predsjednica Povjerenstva:
Izv. prof. dr. sc. Vera Gradišnik

Zadatak preuzeo dana: 17.03.2015.
(potpis pristupnika)

Dostaviti:
- Predsjednica Povjerenstva
- Mentor
- Djelovođa Povjerenstva
- Evidencija studija
- Pristupnik
- Arhiva Zavoda

IZJAVA

Sukladno s člankom 9. Pravilnika o završnom radu, završnom ispitu i završetku preddiplomskih stručnih studija Tehničkog fakulteta u Rijeci, izjavljujem da sam samostalno izradio završni rad prema zadatku br. 602-04/15-14/15.

U Rijeci, 18.05.2016. Josip Dobrić

Sadržaj

1. Uvod

U naslovu teme se spominje termin “tunel“. Ovdje se radi o virtualnom tunelu koji spaja računalne mreže na dvije lokacije, npr. sjedište tvrtke i njenu udaljenu poslovnicu. GRE tunel je protokol koji omogućava povezivanje računalnih mreža dvije ili više lokacija koristeći javnu mrežu kao medij preko kojeg se rade virtualni tuneli, konkretnije virtualne računalne mreže ili VPN (*Virtual Private Networks*). Iako mnogi internet operateri ili ISP (*Internet Service Provider*) nude VPN usluge u svojim paketima usluga, implementacijom GRE tunela u svoje računalne mreže imamo veću kontrolu nad mrežom te nam omogućavaju da nakon kupnje opreme potrebne za ostvarivanje GRE tunela, nemamo dodatne troškove te ne plaćamo dodatne usluge operateru, jedino što nam je potrebno je internet usluga.

Također, GRE protokol je osmišljen i kao protokol unutar kojeg se može enkapsulirati bilo koji drugi protokol. Na taj način možemo na daljinu povezati različite aplikacije i usluge jer možemo putem javne ili privatne mreže slati protokole koji se ne bi mogli slati bez korištenja ove metode zbog toga što uređaji koji posreduju u prijenosu podataka ne podržavaju protokol koji mi želimo prenijeti.

Nedostatak GRE protokola je manjak sigurnosti. To je moguće rješiti uvođenjem IPsec protokola, tako da ćemo se i toga dotaknuti u ovom radu. On je također tunelski protokol, te kombinacijom IPsec-a i GRE-a dobivamo sigurni i zaštićeni virtualni tunel.

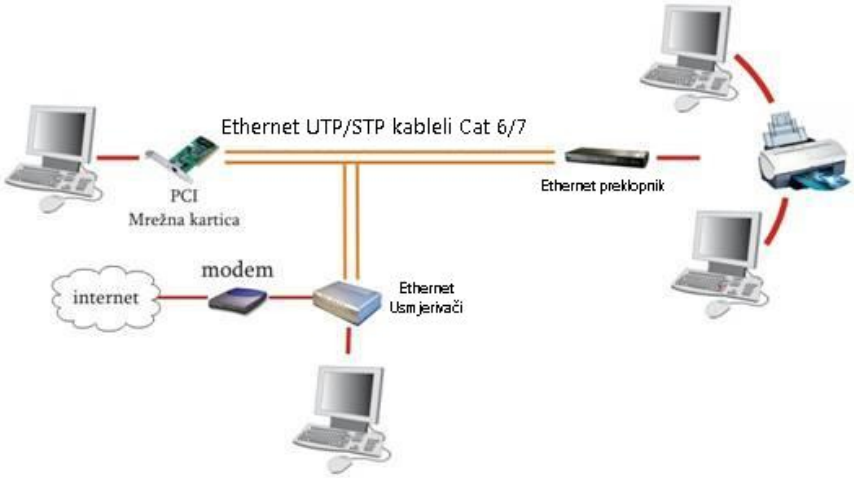
2. Osnovni pojmovi

2.1. Osnovna podjela računalnih mreža

Računalne mreže se djele na:

1. LAN (*Local Area Network*)
2. WAN (*Wide Area Network*)

LAN – Lokalna mreža je skupina računala i mrežnih uređaja koja se nalazi na maloj geografskoj udaljenosti, najčešće unutar jedne zgrade, ureda, kampusa i slično. Lokalna mreža se najčešće koristi kako bi se sva računala unutar lokalne mreže spajala na centralni server, dijelila mrežne printere, pohranjivala podatke na mrežnu pohranu, lakše razmjenjivala podatke i slično. Lokalnom mrežom administrira sam korisnik ili tvrtka koju je korisnik angažirao. U potpunosti je pod našom kontrolom tako da sami podešavamo i konfiguriramo ponašanje mreže tako da ostvarimo mogućnosti koje su nama potrebne.

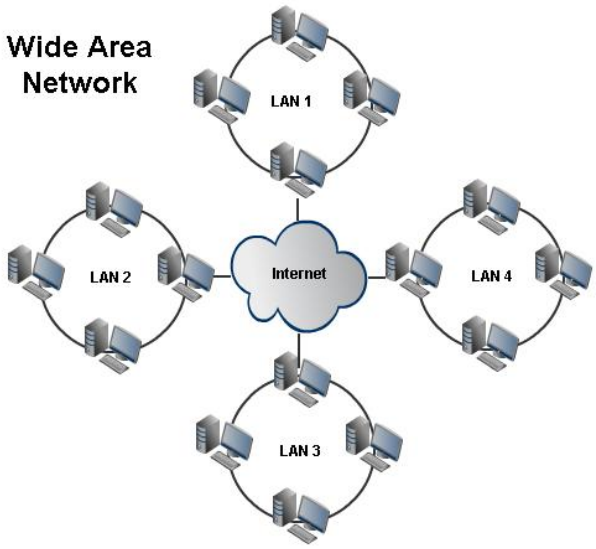


Slika 2.1.1. Primjer LAN mreže
Izvor: http://www.novointel.hr/images/WAN-LANSlika2.jpg

WAN – *Wide Area Network* je geografski raspršena telekomunikacijska mreža. Ovaj termin podrazumijeva širu komunikacijsku mrežu od LAN mreže. WAN mreža može biti privatna ili

unajmljena, ali najčešće se podrazumijeva da je to javna mreža, tj. mreža pod administracijom telekomunikacijskih operatera.

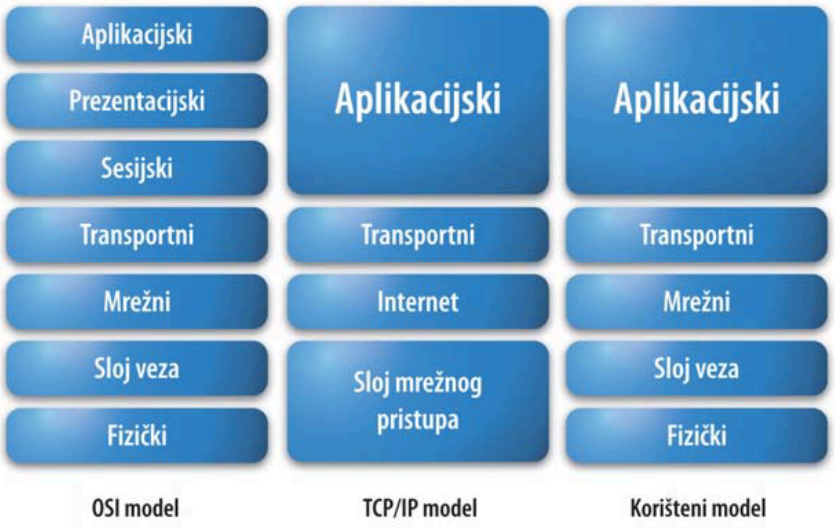
Kada tvrtka ima lokalne mreže koje su geografski odvojene, u pravilu moraju koristiti usluge pristupa Internetu ISP-a (*eng. Internet Service Provider*) kako bi se povezale. Veza između lokalnih mreža (LAN-ova) ostvaruje se preko zakupljenih telekomunikacijskih veza. Tu uslugu ISP naravno dodatno naplaćuje. Kako bi izbjegli plaćanje dodatne usluge, uvodimo tuneliranje (*eng. Tunneling*) u svoju računalnu mrežu. Na ovaj način možemo ostvariti Virtualnu Privatnu Mrežu, odnosno VPN (*eng. Virtual Private Network*). Konfiguracijom usmjernika unutar LAN mreža, možemo napraviti virtualne tunele koji koriste WAN mrežu, odnosno Internet, tako da se ostvari direktna veza dviju LAN mreža koje se tada ponašaju kao da su unutar iste mreže. Na taj način izbjegnemo dodatno plaćanje usluga ISP-u te je mreža u potpusnoti pod našom kontrolom.



Slika 2.1.2 Primjer WAN mreže
Izvor: http://www.computer-networking-success.com /images/what-is-wan.jpg

2.2. Mrežni slojevi

Da bi mogli razumijeti djelovanje tuneliranja, moramo se upoznati sa mrežnim slojevima. Postoje dvije varijante podjele mrežnih slojeva u računalnim mrežama: OSI model i TCP/IP model (slika 2.2.1).



Slika 2.2.1 Podjela mrežnih slojeva
Izvor: Dario Car, dipl. ing: "Uvod u računalne mreže", 2014.

2.2.1. OSI model

OSI (*Open System Interconnection*) je referentni model kojim na opisuje kako aplikacije komuniciraju preko mreže. OSI model je apstraktni model koji služi da bi proizvođači i programeri razvijali proizvode tako da mogu komunicirati sa konkurencijskim proizvodima. Iako se često koristi za opisivanje i demonstraciju, OSI model se jako rijetko zapravo koristi zato što jako malo mrežnih proizvoda ima u sebi komponente i sustave koji su točno razdijeljeni po OSI slojevima.

Razvijen je 1983. godine iz suradnje više većih proizvođača mrežne opreme. U početku je zamišljen kao detaljni model po kojem će se raditi sučelja u mrežnim uređajima, međutim odlučeno je da će se napraviti zajednički referentni model po kojem će proizvođači izrađivati sučelja, što na kraju postaju standardi. OSI je na posljetku prihvaćen kao međunarodni standard od strane ISO-a (*International Organization of Standards*).

Osnovna usloga OSI modela je da se proces komunikacije između dva uređaja može detaljno opisati po slojevima. Tako u svakoj razmjeni podataka, informacije teku niz OSI slojeve u jednom uređaju sa najvišeg na najniži, a zatim ih drugi uređaj čita tako da inforamacija putuje sa nižeg sloja prema višem.

OSI model se sastoji od sedam slojeva koji pojedinačno komuniciraju samo sa slojem iste razina u drugom uređaju.

Slojevi OSI modela:

1. Fizički sloj – zadaća mu je da prenosi bitove kroz mrežu kao električni, optički ili radio signal. Opisuje *hardware*-ski dio mrežne opreme koji sudjeluje u razmjeni podataka
2. Podatkovni sloj – uspostavlja vezu sa fizičkog sloja i tok bitova pakira u okvire. Ima dva podsloja, LLC (*Logical Link Control*) i MAC (*Media Access Control*).
3. Mrežni sloj – zadužen je za adresiranje i usmjeravanje podataka. Odabire najbolje putove za slanje podataka prema odredištu.
4. Transportni sloj – služi za pouzdanu dostavu paketa, što uključuje i provjere grešaka kod primanja paketa.
5. Sesijski sloj – uspostavlja, upravlja i prekida komunikaciju. Također, autentificira i ponovo uspostavlja vezu u slučaju prekida.
6. Prezentacijski sloj – ovaj sloj je dio operativnog sustava i pretvara dolazni i odlazni promet iz jednog tipa prezentacije u drugi, npr. iz čistog teksta u kriptirani na jednoj strani, i obratno na drugoj.
7. Aplikacijski sloj – opisuje protokole kojima aplikacije komuniciraju. Na ovom sloju se određuje točno kojoj aplikaciji je namjenjen upućeni paket

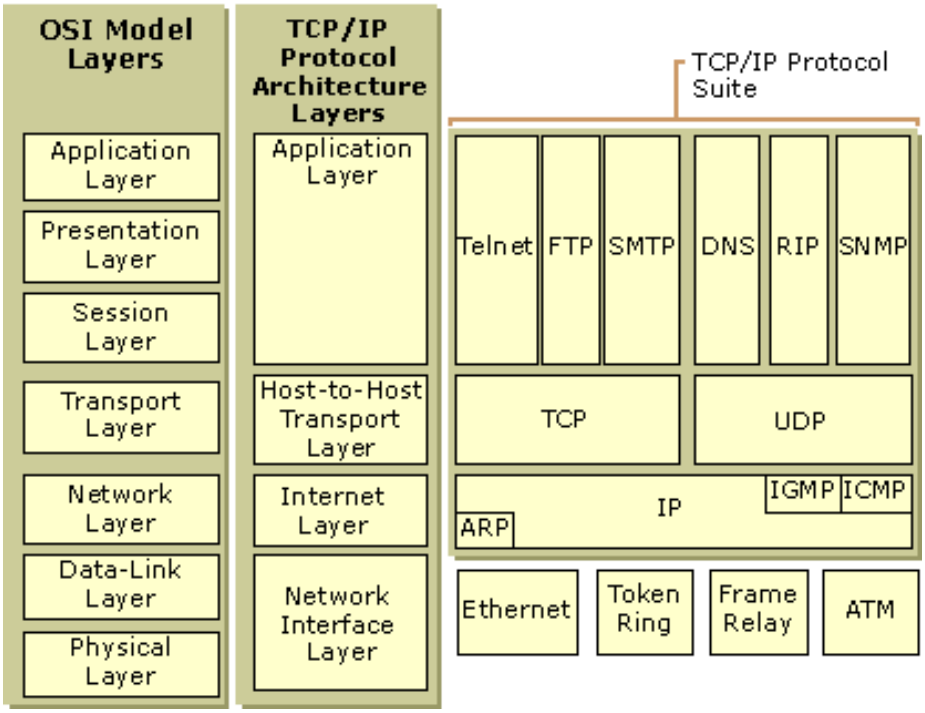
Protokoli po mrežnim slojevima (slika 2.2.2.):

1. Sloj podatkovne veze – Ethernet, Wi-Fi, Token ring, Frame delay…
2. Mrežni sloj – IP (IPv4, IPv6), ICMP, ARP, IGMP…
3. Transportni sloj – TCP, UDP
4. Aplikacijski sloj – DNS, DHCP, FTP, HTTP, FTP, POP3, IMAP, SSH, Telnet, TLS/SSL…

2.2.2. TCP/IP model

TCP/IP model je model koji nam opisuje način na koji funkcioira *Internet*. TCP (*Transmission Control Protocol*) i IP (*Internet Protocol*) su protokoli koji nam to opisuju. IP definira kako računala mogu poslati podatke međusobno putem usmjerenih, međusobno povezanih mreža. TCP definira kako aplikacije kreiraju pouzdane komunikacijske kanale putem takvih mreža. TCP/IP je ciljano razvijen za rješavanje određenih problema, tako da se ne koristiti za generalno opisivanje svih mreža kao što je slučaj s OSI modelom.TCP model je zapravo varijanta OSI modela te se sastoji od samo četiri sloja:

1. Sloj podatkovne veze – objedinjuje fizički sloj i podatkovni sloj OSI modela.
2. Mrežni sloj – ekvivalent mrežnom sloju kod OSI modela
3. Transportni sloj – ekvivalent transportnom sloju kod OSI modela
4. Aplikacijski sloj – objedinjuje sesijski, prezentacijski i aplikacijski sloj OSI modela



Slika 2.2.2 Protokoli po mrežnim slojevima [10]
Izvor: https://technet.microsoft.com/en-us/library/cc958821.aspx

2.3. IPv4

IP protokol vezija 4 (IPv4), nije se puno promijenio od kada je definiran 1981. Kroz dugogodišnje korištenje pokazao se kao robustan i prilagodljiv protokol za Internet. Nažalost, kreatori IPv4 protokola nisu predvidjeli tako brz rast i razvoj Interneta, kao i sve veći broj potrebnih IP adresa.

IPv4 koristi 32 bitne IP adrese, tako da je maksimalan broj IP adresa 2^{32} (4,294,967,296 adresa). Broj dostupnih IP adresa je istvari manji od teoretskog maksimuma je zbog *broadcast* adresa, tako da je IP adresa koje se mogu dodijeliti korisnicima nešto manji od 4 milijarde. Nažalost, u početku razvoja Interneta, IP adrese su se dosta neoprezno dodijeljivale. Tako se nekim korisnicima kao što su sveučilišta, vladine agencije ili određenim kompanijama dodijeljivane IP adrese klase A, tako da je recimo jedno sveučilište imalo dostupno 16,777,216 javnih IP adresa, za čim naravno niti jedno sveučilište neće nikada imati potrebe. Ne zna se točan broj "izgubljenih" IP adresa na taj način, ali pretpostavlja se da je realno dostupno oko 3,5 milijarde IP adresa.

Na prvi pogled, 3,5 milijarde IP adresa izgleda kao jako puno, međutim to i nije baš tako. Veći broj IP adresa je raspodijeljen između država koje su sudjelovale u razvoju Interneta tako da je većina adresa dodijeljena unutar Amerike i Europe. Države koje su se kasnije razvile, kao što su Kina i Indija, imaju puno potrebu za više IP adresa nego što ih je dostupno.

Također, u 21. stoljeću, računala nisu jedina koja zahtjevaju IP adresu. Danas koristimo mobitele, tablete, pa čak i vozila i kućanske aparate koji su svi dio interneta te imaju potebu za IP adresama. Tu dolazimo do spoznaje koliki je ustvari problem manjak IP adresa.

Jedno od rješenja za ovaj problem je i uvođenje NAT-a (*Network Address Translation*). NAT uređaj se nalazi između naše lokalne mreže i interneta. Na taj način odvaja našu lokalnu mrežu i "vanjsku" mrežu te nam omogućava da unutar svoje lokalne mreže koristimo IP adrese koje nisu dostupne nekome tko nije unutar naše lokalne mreže. Na ovaj način se srušio početni koncept Interneta koji je internet opisivao kao mreža računala gdje će svako računalo biti dostupno sa bilo kojeg drugog računala te će na taj način razmjena podataka biti vrlo jednostavna. Bez obzira na to, NAT je svejedno zaživio jer ipak u računalne mreže uvodi

mnoge pozitivne stvari. Prvo i najbitnije je da smanjuje potrebu za IP adresama. Dovoljno je da jedna tvrtka, kućanstvo ili sveučilište ima jednu javnu IP adresu, a ne da svako računalo ima svoju. NAT s jedne strane koristi tu javnu IP adresu za dohvaćanje podataka sa interneta, a s druge strane ima lokalnu mrežu unutar koje se nalaze privatne IP adrese koje mi možemo proizvoljno dodijeljivati svojim računalima, naravno uzimajući u obzir određene zakone računalnih mreža. Nije bitno da li negdje na internetu već postoji računalo sa IP adresom koje smo mi dodijelili svojem računalu jer ta dva računala se međusobno ne "vide" te dupliciranje IP adresa ne stvara problem. Na taj način se drastično smanjuje broj potrebnih javnih IP adresa.

Međutim, ovo je samo privremeno rješenje te se moralo krenuti naprijed i smisliti dugotrajnije rješenje koje će riješiti problem nedostatka IP adresa. Tu dolazimo do IPv6.

Slika 2.3.1 Zaglavlje IPv4 paketa
Izvor: https://osiprodeusodcspstoa01.blob.core.windows.net/hr-hr/media/c8a6a714-2784-4328-8297-2e62706f302d.png

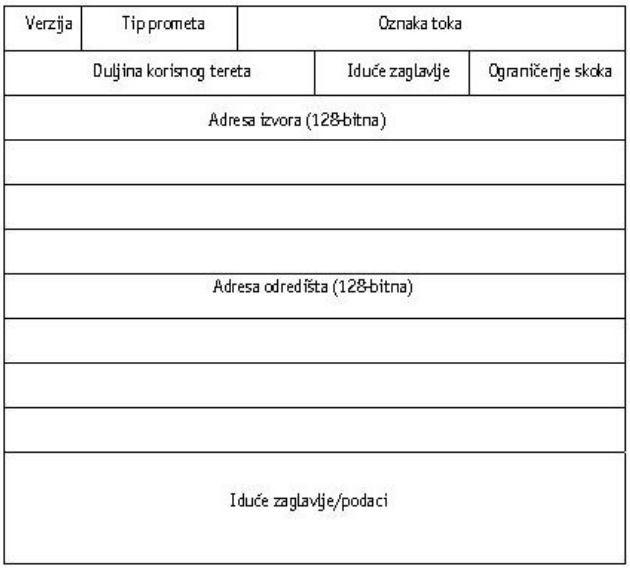
2.4. IPv6

Za razliku od IPv4 koji je koristio 32 bitne IP adresa, IPv6 koristi 128 bitne adrese. Korištenjem 128 bitova za adresiranje dolazimo do brojke od $3.4*10^{38}$ dostupnih javnih IP adresa.

Pri razvoju IPv6 IETF je nastojao zadržati pozitivne stvari IPv4, te unaprijediti novi protkol dodavanjem novih i naprednijih mogućnosti. Neke od tih mogućnosti su:

- Podržava izvorne (*source*) i odredišne (*destination*) adrese koje su duge 128 bitova.

- Ugrađena je podrška za Ipsec
- Koristi *Flow Label* polje koje usmjernik koristi za kontrolu protoka paketa za QoS (*Quality of service*)
- Ne zahtjeva ručnu konfiguraciju DHCP-a
- Podržava pakete veličine 1280 bajtova
- otvoreniji je poboljšanjima – vrlo je jednostavno implementirati poboljšanja protokolima zbog mogućnosti zaglavlja da se dodaju opcionalna polja u samo zaglavlje (slika 2.4.1.)



Slika 2.4.1. Osnovno IPv6 zaglavlje
Izvor: https://www.carnet.hr/tematski/ipv6/images/sl1.jpg

2.5. Usmjernik (*eng. Router*)

U mrežama koje razmjenjuju pakete, kao što je Internet, usmjernik (*Router,* slika 2.5.1.) je uređaj, ili aplikacija na računalu, koja nam određuje sljedeću točku u mreži kojoj ćemo proslijediti paket na njegovom putu prema krajnjem cilju. Usmjernik povezuje najmanje dvije mreže, te određuje kojim putem (*route*) će poslati koju informaciju uzimajući u obzir ono što on zna o trenutnom stanju mreže u kojoj se nalazi.

Usmjernik u sebi slaže tablicu dostupnih puteva i njihovih stanja i koristi te informacije zajedno sa algoritmom udaljenosti i troška da bi odredio najbolji put za svaki pojedini paket. Najčešće paket putuje preko više različitih mreža da bi stigao do svog cilja. Usmjerivanje (*routing*) je funkcija koje se nalazi na Mrežnom sloju OSI modela.

Slika 2.5.1. Cisco 2801 usmjernik
Izvor: https://supportforums.cisco.com/document/86786/how-add-wic-2t-card-router-2800

2.6. Preklopnik (*eng. Switch*)

Uvođenjem preklopnika (*Switch,* slika 2.6.1.) u računalne mreže, odustalo se od korištenja koncentratora (*Hub*). Za razliku od koncentratora, preklopnici analiziraju svaki paket te ga šalju na sučelje kojem je namjenjen, za razliku od koncentratora koji samo prosljeđuju svaki paket na sva sučelja. Preklopnik čita MAC adrese (*hardware-sku* adrese) pošiljatelja i primatelja iz zaglavlja paketa te ga uspoređuje s tablicom koju sprema u svoju memoriju gdje se nalaze MAC adrese uređaja spojenih na njegova sučelja.

Praktični su nam jer većina može sama zapamtiti MAC adrese uređaja, popunjavalući tablicu MAC adresa dok prosljeđuju pakete koje prolaze kroz njih. Također, moguće je spojiti mreže različitih brzina preko istog preklopnika ako ima odgovarajuća sučelja. Na taj način omogućavamo razmjenu podataka između uređaja koji mogu biti *Ethernet* (10 Mbit/s), *FastEthernet* (100Mbit/s), *GigabitEthernet* (1Gbit/s), itd.

Slika 2.6.1. Cisco SMB 500 preklopnik
Izvor: https://www.packet6.com/getting-started-with-ciscos-500-series-smb-switches/

2.7. Načini komunikacije u Ethernet mreži

U mrežama sa preklopnicima moguće su tri vrste komunikacije:

- *Unicast*
- *Multicast*
- *Broadcast*

Unicast komunikacija je kada samo jedan uređaj šalje podatke i samo jedan uređaj prima podatke. Primjeri takve komunikacije su HTTP, SMTP, Telnet i drugi protokoli.

Multicast komunikacija je kada uređaj šalje podatke, a grupa uređaja prima podatke. Primjer takve komunikacije je slanje slike i zvuka na više odredišta u mreži.

Broadcast komunikacija je kada jedan uređaj šalje podatke svim uređajima u mrežnom segmentu. Primjer *broadcast* komunikacije su ARP i DHCP protokoli.

3. GRE TUNEL

Zamislimo si situaciju u kojoj imamo sjedište tvrtke na jednoj lokaciji i poslovnice te iste tvrtke smještene na različitim lokacijama, u različitim državama. Primjer bi nam mogao biti ovlašteni automobilski servisi. Svaki servis mora poslati izvještaj što se radilo i na kojem autu u tvornicu, na njihov centralni server. U tom slučaju imamo stotine servisa razbacani po cijelom svijetu koji se moraju spojiti na isti centralni server u tvornici. Ovdje nam u pomoć dolaze virtualni tuneli koji nam služe da bi postigli ovu funkcionalnost.

Tuneliranje (eng. *Tunneling*) je protokol koji unutar neke WAN mreže, najčešće interneta, stvara virtualne tunele, tj. puteve kojima podaci putuju od izvora prema odredištu. Razlika između tuneliranja i klasičnog usmjeravanja paketa kroz mrežu je ta što pomoću tuneliranja možemo ostvariti virtualne privatne mreže (VPN) i možemo dodatno zaštiti podatke.

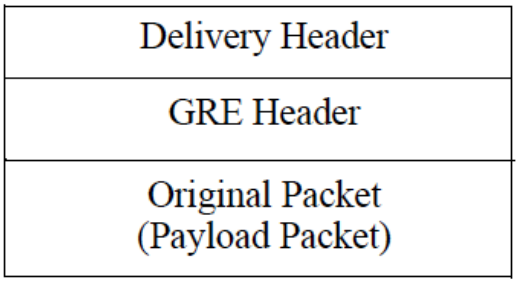
Jedan od tunelskih protokola je i GRE (eng. *Generic Routing Encapulsation*) tuneliranje. Konfiguriranjem GRE tunela između dva usmjernika postižemo to da se naše dvije udaljene lokacije ponašaju kao da su unutar istog LAN-a, tj. kao da su unutar iste mreže. Sa stajališta usmjernika, put između dva usmjernika među kojima je postigbut GRE tunel, ne postoji. Njima izgleda kao da su oni direktno spojeni jedan u drugi, iako vjerovatno prelaze preko stotina različitih usmjernika koji se nalaze na putu između njih dvoje. Ovo se također može postići i unajmljivanjem dediciranih vodova od strane ISP-a, međutim to je dodatna usluga koja se dodatno nadoplaćuje. Kod GRE tunela jedini trošak koji imamo je kupovina usmjernika i plaćanje mjesečne pristojbe za internet ISP-u, koju ionako plaćamo da bi imali pristup internet u svojoj tvrtci. Također, velika prednost GRE tunela u odnosu na zakupljene vodove je ta što nam je mreža u potpunosti pod našim nadozorom tako da je administracija i otklanjanje kvarova u potpunosti nama u rukama i ne ovisimo o ISP-u, tj. telekomunikacijskom operateru i njihovoj korisničkoj podršci.

GRE tuneliranje je vrlo fleksibilan i generički protokol, tako da unutar njega možemo enkaspulirati jako puno drugih protokola kao što su *Unicast IP, Multicast IP, Apple talk, IPX, Appletalk,* itd. Na taj način postižemo to da preko mreže koja možda i ne podržava određeni protokol, enkapsulacijom nepodržanog protokola unutar GRE tunela, možemo ostvariti potpunu funkcionalnost onoga što nam je potrebno.

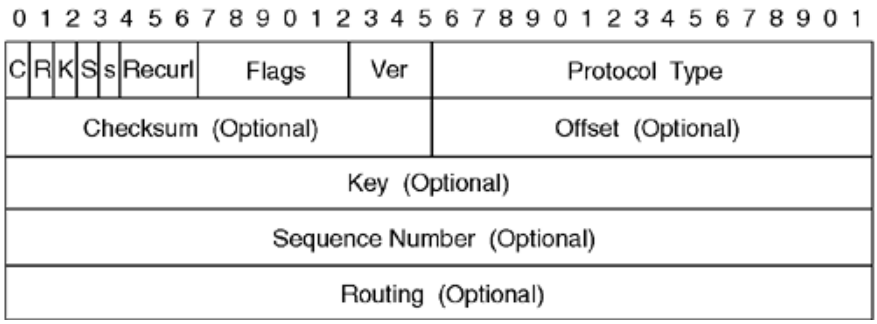
Da ne bi sve bilo idilično, GRE tunel, naravno, ima i svoje nedostatke. Jedan od najvećih je manjak sigurnosti. Paketi koji putuju GRE tunelom su nezaštićeni tako da ukoliko netko presretne promet, podatke koje šaljemo može zloupotrijebiti. Ovo se može spriječiti uvođenjem IPsec protokola kojim ćemo se opširnije baviti kasnije u radu. Također, GRE tunel sam po sebi ne provjerava trenutačno stanje tunela (eng. *Stateless*). Drugim riječima, usmjernik koji šalje podatke ne zna da li je tunel još uvijek aktivan, tj. da li je moguće uspostaviti komunikaciju sa drugom stranom tunela. Zbog toga se može dogoditi da izgubimo podatke koje jedan usmjernik pošalje, a drugi ih nikada ne primi. Srećom *Cisco* je od verzije operativnog sustava Cisco IOS® 12.2(8)T uveo komandu *keepalive*. *Keepalive* je naredba koja nam omogućava da konfiguriramo svakih koliko će usmjernik periodički provjeravati dostupnost druge strane tunela, te nakon koliko će propalih pokušaja dohvata druge strane tunela, proglastiti taj tunel "mrtvim" te će prestati slati promet tim tunelom.

3.1. Struktura GRE enkaspuliranog paketa

GRE paket ima oblik



Slika 3.1.1. Oblik GRE paketa
Izvor :http://www.brocade.com/content/html/en/configuration-guide/fastiron-08030b-l3guide/GUID-627671E9-375E-4E0F-B05A-E408A1CAE507-output_low.png



Slika 3.1.2 Zaglavlje GRE paketa
Izvor: http://book.soundonair.ru/cisco/images/1587050250/graphics/11fig02.gif

Pojasniti čemo polja koja se nalaze u zaglavlju GRE paketa (slika 3.1.2.):

- *C - Checksum present* - ako je *Checksum Present* bit postavljen u 1, *checksum* polje je aktivno i sadrži valjanu informaciju. Ako je postavljen ili *Checksum Present* ili *Routing Present* bit postavljen
- *R - Routing present* - ako je *Routing Present* bit postavljen u 1, *Offset* i *Routing* polja su aktivna i sadrže valjanu informaciju. Ako je postavljen ili *Checksum Present* ili *Routing Present* bit, *Checksum* i *Offset* polja su aktivna u GRE paketu.
- *K - Key present* - ako je aktivan *Key Present* bit, *Key* polje je aktivno u GRE paketu. U suprotnom, *Key* polje nije aktivno u GRE zaglavlju.
- *S – Sequence number* – ako je aktivan *Sequence number* bit, *Sequence number* polje je aktivno i sadrži valjanu informaciju
- *s – Strict Source Route* – preporučeno je da je ovaj bit postavljen ukoliko ako se sve informacije o *routing-u* sadrže od *Strict Source Routes*
- *Recur – Recursion Control* – sadrži broj dodatnih enkapsulacija koje su dopuštene. Zadana vrijednost mu je 0.
- *Flags* – ova polja su rezervirana i kod slanja paketa moraju biti 0./
- *Protocol Type – Protocol Type* polje sadrži informaciju o tipu protokola koji se nalazi u korisnom sadržaju (eng. *payload*) GRE paketa. Npr. Ako se unutar GRE paketa nalazi IP protocol, sadržaj ovog polja je 0x800.
- *Offset* – ovo polje nam govori o razmaku između početka *Routing* polja i prvog okteta aktivnog *Source Route Entry* koji se pregledava. Ovo polje je aktivno ako je *Routing present* ili *Checksum Present* polje aktivno, tj. postavljeno u 1 i sadrži valjanu informaciju.
- *Checksum* – sadrži zbroj za provjeru (prvi komplement) GRE zaglavlja i korisnog sadržaja paketa.

- *Key* – sadrži broj od četiri okteta koji se unosi od strane enkapsulatora. Koristi se tako da primatelj paketa može identificirati pošiljatelja.
- *Sequence Number* – sadrži 32-bitni broj koji unosi enkapsulator. Primatelj paketa čita *Key* polje da bi znao raspored kojim je pošiljatelj slao pakete.
- *Routing* – ovo polje se koristi kada nam je potrebno *Source Route Entries* (SREs). Rijetko se koristi, osim u slučajevima kada nam je potrebno koristiti *source* usmjerivanje na GRE paketima

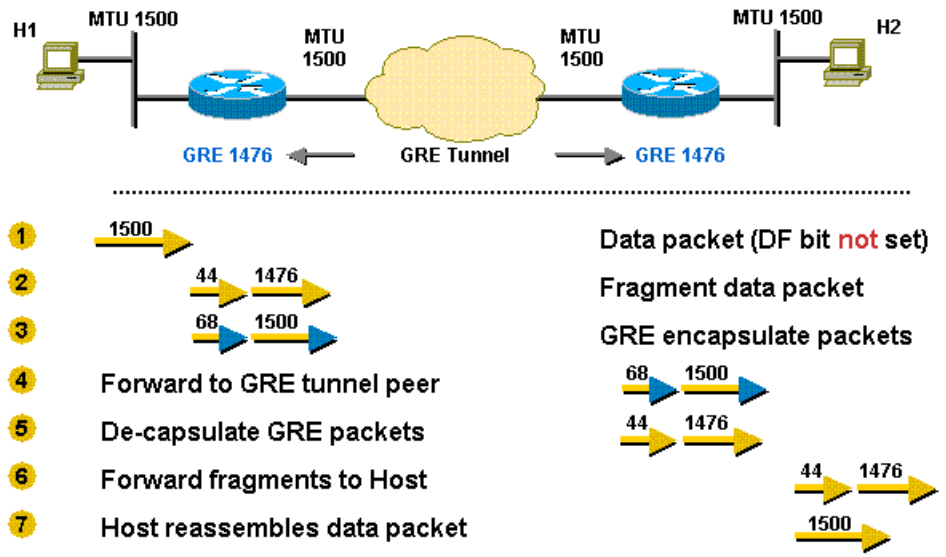
3.2. Fragmentacija GRE paketa

Fragmentacija je postupak u kojem jedan IP paket razdijelimo (fragmentiramo) na nekoliko segmenata. Veličina IP paketa je definirana i iznosi 65536 bajtova (64 KB). Međutim različiti načini prijenosa ne dozvoljavaju uvijek da veličina bude toliko, već da ona bude manja. Ta veličina se zove MTU (eng. *Maximum Transmission Unit*). MTU ovisi isključivo o načinu prijenosa podataka, tj. putu kojim podatak prolazi. Kod fragmentacije enkapsuliranih podataka postoje dva načina fragmentacije. Prvi je da se originalni paket najprije enkapsulira, zatim se fragmentira (šaljemo dva enkapsulirana fragmenta). Drugi način je to da se paket najprije fragmentira, a zatim enkaspulira (šaljemo dva enkapulacijska paketa.)

Kod fragmentacije GRE paketa najprije se paket fragmentira, a zatim se fragmentirani paket enkapsulira. Kod fragmentacije nam je jako važan PMTUD postupak. On nam dinamički određuje kolika nam je najmanja MTU veličina na cijelom putu koji će paket proći, te se fragmentacija paketa napravi imajući to u obzir. Također, u zaglavlju IP paketa, u *Flags* dijelu imamo tri kontrolne zastavice među kojima je prva rezervirana i mora uvijek biti postavljena u 0, druga je DF (*Don't Fragment*) koja nam govori da li je dozvoljeno fragmentiranje ili ne, i treća MF (*More Fragments*) koja nam govori da li je određeni paket zadnji u fragmentaciji ili slijedi još paketa. Ključnu ulogu nam igra DF bit jer nam on govori da li je dopušteno fragmentiranje paketa. Ako je DF postavljen u 1, fragmentiranje je zabranjeno, ako je DF postavljen u 0, fragmentiranje je dopušteno.

Primjer postupka fragmentacije u kojem je DF bit postavljen u 0 i MTU je 1476 bajtova (slika 3.2.1):

1. Usmjernik prima paket veličine 1500 bajtova na *tunnel* sučelje s DF bitom u 0. Paket se sastoji od IP zaglavlja od 20 bajtova i TCP korisnog sadržaja od 1480 bajtova.
2. Kako će paket biti prevelik za slanje, pogotovo kada se zbroji GRE zaglavlje od 24 bajta, usmjernik razdvaja paket u dva fragmenta. Prvi ima veličinu 1476 bajta (20 bajta IP zaglavlja + 1456 IP sadržaja), a drugi 44 bajta (20 bajta IP zaglavlje i 24 IP sadržaj). Sada nam paketi neće biti preveliki nakon što im se doda GRE zaglavlje.
3. Usmjernik dodaje GRE enkaspulaciju na svaki fragment koja se sastoji od 4 bajta GRE zaglavlja i 20 bajta IP zaglavlja. Ova dva fragmenta sada imaju duljinu od 1500 bajta i 68 bajta.
4. GRE+IP paketi se sada prolježuju na GRE tunelsko sučelje usmjernika.
5. GRE tunelsko sučelje skida GRE zaglavlje sa ta dva paketa.
6. Usmjernik prosljeđuje pakete na odredište.
7. Odredišni usmjernik prima pakete, raspakirava ih i sastavlja IP fragmente u originalni IP paket.



Slika 3.2.1 Postupak fragmentacije iz primjera
Izvor: http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html#anc11

4. IPSEC

IPsec (*Internet Protocol Security*) je protokol razijen od strane IETF-a (*Internet Engineering Task Force*) kako bi pružio sigurnu razmjenu podataka. Kod razvoja IP protokola (prije 30-ak godina) nije se puno radilo na sigurnosti. Jedan od razloga je to što su tvorci IP-a smatrali da korisnici neće zlouporabiti internet i iskorištavati njegove nedostatke u svrhu krađe podataka, krađe identiteta i sl. Također, tehnologija kriptografije nije bila toliko poznata i razvijena kao što je slučaj danas.

Najprije se dva računala moraju dogovoriti oko nekoliko stvari, prije ikakve razmjene podataka:

1. Koji će enkripcijski mehanizam koristiti (DES, trostruki DES)
2. Koji će mehanizam koristiti za potvrđivanje integriteta poruke (MD5 ili SHA-1)
3. Kako će se autentificirati konekcije, koristeći javni ključ, dijeljeni privatni ključ ili Kerberos

Kada se dogovore oko ove tri stvari, dolaze do druge runde pregovora:

1. Hoće li koristiti AH (*Authentication Header*) protokol
2. Hoće li koristiti ESP (*Encapsulating Security Payload*) protokol
3. Koji će enkripcijski mehanizam koristiti za ESP
4. Koji će enkripcijski mehanizam koristiti za AH

IPsec ima dva mehanizma koji mogu raditi zajedno ili svaki posebno, da bi se podaci poslali sigurno preko javne mreže:

1. AH (*Authentication Header*)
2. ESP (*Encapuslating Secure Payload*)

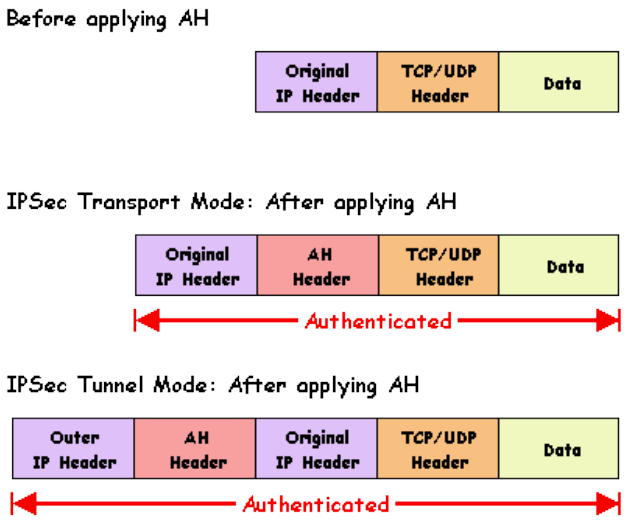
4.1. AH mehanizam

Authentication Header informacija se dodaje u paket između mrežnog i transportnog sloja, kod slanja. AH nam štiti mrežu na taj način što štiti podatke od toga da ih netko mjenja. Napadač nam može presresti podatke na putu od pošiljatelja prema primatelju i promijeniti

sadržaj paketa ili se lažno predstaviti kao primatelj ili pošiljatelj te na taj način doći u posjed osjetljivih podataka.

Da bi se to izbjeglo, IPsec koristi AH za digitalno potpisivanje sadržaj cijelog paketa. Taj potpis nam koristi iz tri razloga:

1. Zaštita od tzv. *Replay* napada. Napadač može presresti pakete, spremiti ih i modificirati, te zatim ih slati na način da se predstavi kao izvorni pošiljatelj kada on nije na mreži. IPsec to spriječava tako što sadrži pošiljateljev potspi u svim paketima.
2. Zaštita od izmjene sadržaja. IPsec dodaje potpis u svaki paket, što znači da niti jedna promjena sadržaja paketa ne može proći nezamječeno.
3. Zaštita od zavaravanja. Obe strane koje komuniciraju (npr. klijent i server) potvrđuju svoj identitet sa autentifikacijskim zaglavljem IPsec-a.



Slika 4.1.1 Paket prije i nakon korištenja AH mehaznima, u transportnom i tunelskom načinu rada
Izvor : http://www.isaserver.org

/articles-tutorials/articles/IPSec_Passthrough.html

AH se primjenjuje nad cijelim paketom, uključujući i korisni sadržaj i zaglavlja koja dodaje svaki od mrežnih slojeva slika 4.1.1.

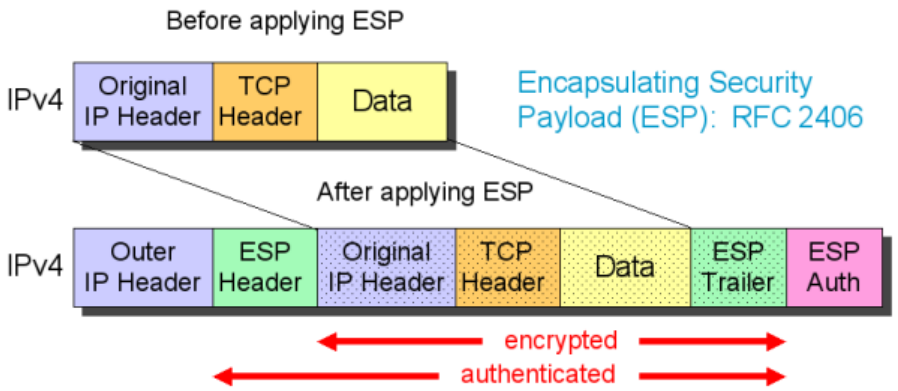
4.2. ESP mehanizam

AH u kojem smo govorili u prethodnom poglavlju nam spriječava napadača da izmjenjuje sadržaj paketa, ali ga ne spriječava da mu pročit sadržaj. Da bi se to spriječilo, IPsec koristi *Encapulating Security Payload* (ESP) mehanizam. ESP se koristi kako bi se enkripitirao sadržaj paketa.

ESP mehanizam je kompleksniji od AH mehanizma jer on sam podržava autentifikaciju, zaštitu od *Replay* napada te provjeru integriteta poruke. To mu omogućavaju 3 zasebna procesa (slika 4.2.1):

1. ESP zaglavlje
2. ESP blok na kraju paketa (eng. *trailer*)
3. ESP autentifikacijski blok

Svaka od ovih komponenti sadrži podatke koji su nam potrebni da bi osigurali autentifikaciju i provjeru integriteta poruke. Da bi spriječili izmjenu podataka, ESP klijent mora potpisati ESP zaglavlje, podatke i ESP blok na kraju zajedno. Kombinacija ovih preklapajućih procesa potpisivanja i enkripcije nam pružaju dobru sigurnost.



Slika 4.2.1. Paket prije i nakon upotrebe ESP mehanizma
Izvor: http://www.free-it.org/archiv/talks_2005/paper-11156/paper-11156.html

4.3. Načini rada IPsec-a

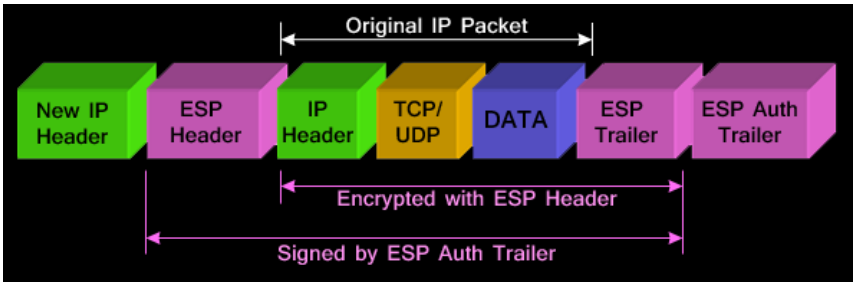
IPsec protkol se može konfigurirati tako da radi u dva načina rada: prijenosni (eng. *Transport*) i tuneliranje (eng, *Tunneling*). Koji način rada ćemo koristiti nam ovisi o konfiguraciji i o implementaciji IPsec-a.

4.3.1. Tuneliranje

Tuneliranje (eng. *Tunneling*) je zadani način rada kod IPsec-a. Sa tuneliranjem, cijeli originalni IP paket je zaštićen sa IPsec-om. To znači da IPsec djeluje nad cijelim originalnim IP paketom, enkriptira ga, dodaje mu novo IP zaglavlje i šalje ga na drugu stranu VPN tunela. Tunelski način rada se najčešće koristi kao veza između pristupnika (eng. *gateway*). Tako se koristi između dva usmjernika, vatrozida (eng. *firewall*) i sl.

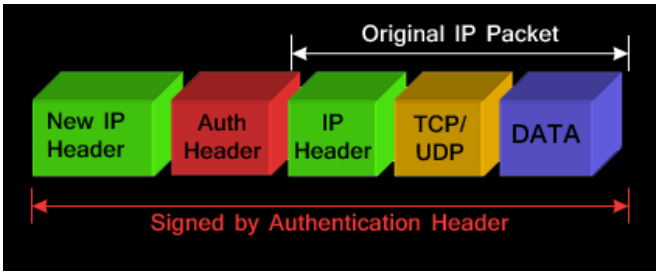
Tuneliranje se koristi za enkripciju prometa između osiguranih IPsec *gateway-a,* npr. između dva Cisco usmjernika povezana preko interneta IPsec VPN tunelom. Još jedna od upotreba tuneliranja je IPsec tunel između Cisco VPN klijenta i IPsec *gateway-a.* Klijent se spoji na IPsec *gateway,* promet koji dolazi od klijent je kriptiran, enkapsuliran u novi IP paket i poslan primatelju. Kada ga *firewall* dekriptira, originalni pošiljateljev paket se šalje u lokalnu mrežu.

U tunelskom načinu rada, IPsec zaglavlje (AH ili ESP zaglavlje) se dodaje između IP zaglavlja, i zaglavlja višeg mrežnog sloja (slika 4.3.1). Između AH i ESP mehanizma, ESP se najčešće koristi kod IPsec tunelskog načina rada. Kod ESP-a, vrijednost *Protocol* polja u novom IP zaglavlju se mjenja u njegov ID protokola, u 50.



Slika 4.3.1 Izgled paketa kod tunelskog načina rada i ESP-a
Izvor: http://www.firewall.cx/networking-topics/protocols/127-ip-security-protocol.html

Kod IPsec tuneliranja, AH mehanizam se može upotrijebiti zasebno ili zajedno sa ESP-om. Zadaća AH mehanizma je da čuva integritet cijelog paketa. Kako se određeni dijelovi novo dodanog IP zaglavlja mjenjaju u prijenosu, AH ne osigurava to zaglavlje jer ne može predvidjeti promjene koje će se dogoditi na putu prema primatelju. AH mehanizam osigurava sve što se ne mjenja u prijenosu, ali promijeni vrijednost polja *Protocol* u novo IP zaglavlju u vrijednost 51 jer je to njegov ID protokola (slika 4.3.2).



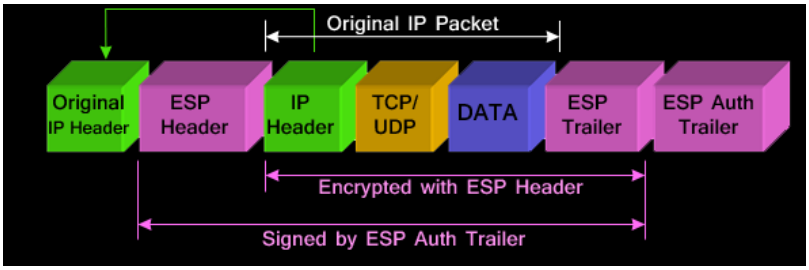
Slika 4.3.2 Izgled paketa kod tunelskog načina rada i AH-a
Izvor: *http://www.firewall.cx/networking-topics/protocols/127-ip-security-protocol.html*

4.3.2. Prijenosni način rada

Prijenosni (eng. *Transport*) način rada IPsec-a se najčešće koristi kod *end-to-end* načina komunikacije, tj. kada klijent komunicira sa serverom ili sa drugim klijentom, npr. kada se klijent spaja na server pomoću *Windows Remote Desktop* sesije, ili kada se klijent spaja na uređaj pomoću *Telnet*-a.

Prijenosni način rada IPsec-a se najčešće koristi uz neki drugi tunelski protokol, tipa GRE tunel. GRE tunelom se najprije enkapsulira IP paket, a zatim se IPsec-om zaštite GRE paketi. IPsec u prijenosnom načinu rada pruža sigurnost prometu unutar GRE tunela.

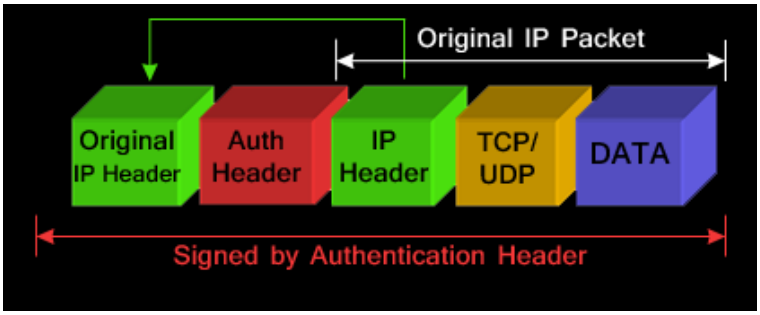
Prijenosni način rada nam pruža zaštitu podataka, tj. korisnog sadržaja IP paketa, i sastoji se od TCP/UDP zaglavlja zajedno sa podacima, između AH ili ESP zaglavlja. Korisni sadržaj paketa se enkapsulira sa IPsec zaglavljem i blokom na kraju (*trailer*). Originalno IP zaglavlje nam ostaje isto, osim šta se pol je *Protocol* promijeni u ESP ili AH, a originalni protokol nam se spremi u IP blok na kraju tako da ga kasnije možemo vratiti (slika 4.3.3).



Slika 4.3.3 Izgled paketa kod prijenosnog načina rada i ESP-a
Izvor: http://www.firewall.cx/networking-topics/protocols/127-ip-security-protocol.html

Za razliku od tuneliranja, ovdje možemo primjetiti da je originalno IP zaglavlje premješteno na sam početak (uz izmjenu vrijednosti *Protocol* polja u 50). Iz toga se može vidjeti da prijenosni način rada ne osigurava zaštitu i enkripciju originalnog IP zaglavlja, za razliku od tuneliranja koje ga zaštićuje.

Kao i kod ESP-a, AH također kopira originalno zaglavlje (slika 4.3.4) (mjenjajući *Protocol* polje u vrijednost 51). Time se ostavlja nezaštičeno originalno IP zaglavlje unutar kojeg se , između ostalog, nalaze i IP adrese pošiljatelja i primatelja.



Slika 4.3.4 Izgled paketa kod prijenosnog načina rada i AH-a
Izvor: http://www.firewall.cx/networking-topics/protocols/127-ip-security-protocol.html

5. GRE-over-IPsec

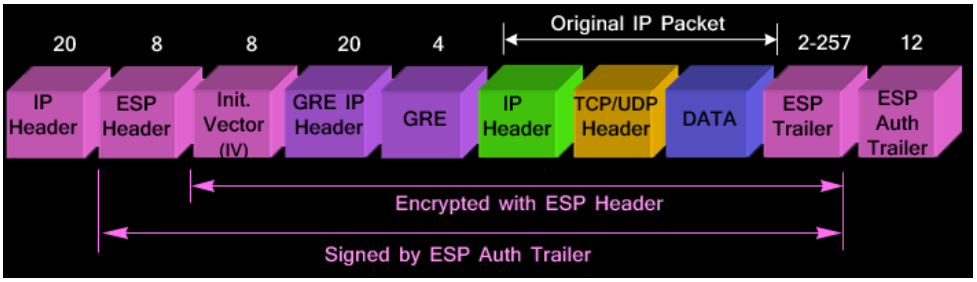
Kao što smo već ranije rekli, GRE protokol, tj. GRE tunel je vrlo fleksibilan i omogućava nam enkapsulaciju bilo kojeg drugog protokola. Možemo putem interneta, ili neke druge mreže, prenijeti bilo koji IP protokol (IP *broadcast,* IP *multicast*), ali isto tako i protokole koji nisu bazirani na IP-u, što inače nije moguće. GRE, dakle, je nam je jako koristan i ima puno prednosti. Međutim, manjak sigurnosti koji je prisutan kod GRE protokola je ono što mu je najveća mana, te ga čini vrlo ranjivim.

Zadaća IPsec-a je da uvede sigurnost. IPsec VPN tunel je vrlo siguran i omogućava nam da uspostavimo VPN između dvije lokacije, ali nam ne omogućava dinamičko usmjeravanje (eng. *dynamic routing*), što nam je vrlo u bitno u većim mrežama. IPsec tuneli podržavaju *unicast* pakete. GRE paket je po definiciju *unicast* paket, tako da nema problema kod slanja GRE paketa kroz IPsec tunel.

Iz tog razloga koristimo kombinaciju GRE tunela i IPsec protokola, što zovemo GRE-over-IPsec. To nam omogućava da povežemo dvije lokacije virtualnim tunelom koji je u potpunosti siguran, ali još uvijek nam podržava protokole za usmjeravanje, IP *multicast* ili višeprotokolni (eng. *multiprotocol*) promet.

5.1. GRE-over-IPsec tunelski način rada

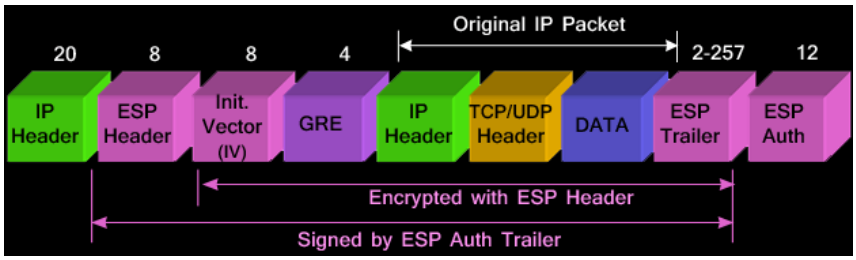
Kod GRE IPsec tunelskog načina rada, cijeli GRE paket (koji sadržava i originalni IP paket) se enkapsulira, krpitira i zaštićuje unutar IPsec paketa (Slika 5.1.1). Tunelski način rada nam u ovom slučaju ima i tu prednost da zaštićuje cijeli GRE paket, tako da ne ostavlja niti jedan njegov dio nezaštićen. Nedostatak ovog načina je to da se dodaje dodatno zaglavlje na paket, tako da se veličina paketa povećava. To dodatno zauzimanje prostora nam smanjuje mjesto koje je dostupno originalnom IP paketu, tj. informaciji u njemu. To nam znači da moramo uvesti dodatnu fragmentaciju da bi mogli sve zajedno poslati kroz mrežu.



Slika 5.1.1 GRE IPsec tunelski način rada
Izvor: http://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/872-cisco-router-gre-ipsec-tunnel-transport.html

5.2. GRE-over-IPsec prijenosni način rada

Kod GRE IPsec prijenosnog načina rada, cijeli GRE paker se enkspulira unutar IPsec paketa, međutim njegovo zaglavlje se premješta na sam početak, ispred IPsec paketa (Slika 5.2.1). To nam znači da je GRE zaglavlje nezaštićeno i podložno napadima.



Slika 5.2.1 GRE IPsec prijenosni način rada
Izvor: http://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/872-cisco-router-gre-ipsec-tunnel-transport.html

Ovaj način rada ima i još neka ograničenja. Ukoliko nam kriptirani promet prolazi kroz uređaje koji koriste *Network Address Translation* (NAT) ili *Port Address Forward* (PAT), prijenosni način rada se ne može koristiti. Također, ako odredišta GRE tunela i GRE IPsec tunela nisu jednaka, moramo koristiti tunelski način rada. Ovi problemi kod prijenosnog načina rada nam jako ograničavaju njegovu implementaciju.

5.3. Fragmentacija GRE IPsec paketa

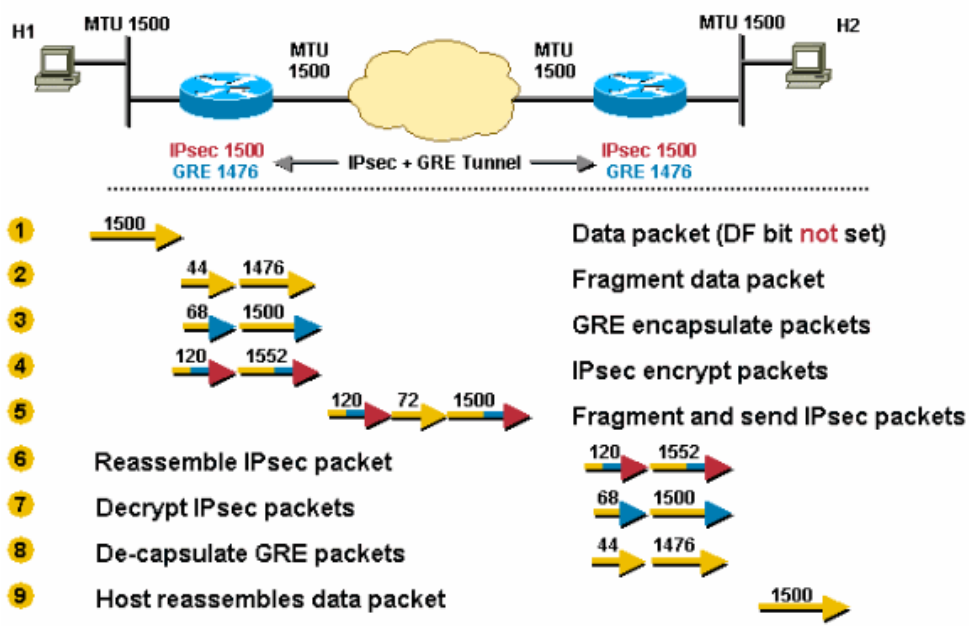
Kod fragmentacije GRE paketa koji su kriptirani IPsec-om imamo puno kompleksniju situaciju nego kod fragmentacije "čistog" GRE paketa. IP paket se fragmentira i na svaki fragment tog paketa se dodaje GRE zaglavlje. Ukoliko je jedan od fragmenata dovoljno velik da je njegov MTU, nakon kriptiranja IPsec-om, prevelik dolazimo do problema jer je takav paket potrebno dodatno fragmentirati. Klijent kome je taj promet namjenjen, morati će sastaviti takav paket prije dekripcije. Ovo se naziva dvostruka fragmentacija (jednom nakon GRE protokola, jednom nakon IPsec-a). Ova dvostruka fragmentacija dodatno opterećuje usmjernik na drugoj strani tunela te se time povećava kašnjenje i smanjuje propusnost usmjernika. Također, u procesu sastavljanja takvih paketa, procesor (CPU) usmjernika se jako opterećuje.

Ova situacija se može izbjeći ako postavimo "ip mtu" vrijednost, na GRE tunelskom sučelju usmjernika, dovoljno nisku uzimajući u obzir i GRE i IPsec zaglavlja koja će biti dodana na originalni IP paket.

Ovakvu situaciju ćemo demonstrirati na primjeru. IPsec-om se zaštićuje GRE promet, MTU izlaznog sučelja je 1500, MTU IPsec-a je 1500, a MTU GRE IP paketa je 1476 (1500-24). Radi ovih vrijednosti, TCP/IP paket će se dvostruko fragmentirati. Paket će se fragmentirati nakon GRE enkapsulacije, a zatim će se jedan taj fragment dodatno fragmentirati kod kriptiranja IPsec-om (Slika 5.3.1):

1. Usmjernik prima paket veličine 1500 bajta
2. Prije enkapsulacije, GRE paket od 1500 bajtova se rastavlja na dva fragmenta, jedan od 1476 bajta (1500-24) i 44 bajta (24 podaci+20 IP zaglavlje).
3. GRE enkapsulira IP fragmente i dodaje 24 bajta svakom paketu. Dobivamo dva GRE paketa veličine 1500 bajtova (1476+24) i 68 bajta (44+24).
4. IPsec kriptira pakete i dodaje im 52 bajta (IPsec tunelski način rada), i dobivamo pakete od 1552 bajta (1500+52) i 120 bajta (68+52).
5. Paket od 1552 bajta je prevelik jer nam je maksimalni MTU 1500. Taj paket fragmentiramo i dobivamo paket od 1500 bajta i 72 bajta (52+20 novo IP zaglavlje). Ta tri paketa (1500, 72 i 120) se prosljeđuju prema odredištu korištenjem GRE + IPsec.

6. Usmjernik na drugoj strani tunela prima ta tri paketa. Najprije sastavlja pakete od 1500 bajta i 72 bajta da bi dobio paket koji je prije fragmentacije imao 1552 bajta. Sa paketom od 120 bajta za sada ne radi ništa.
7. Zatim dekriptira oba IPsec + GRE paketa i dobiva dva GRE paketa od 1500 bajta i 68 bajta.
8. GRE dekapsulira ta dva GRE paketa i dobiva IP fragmente od 1476 bajta i 44 bajta. Ti fragmenti se prosljeđuju prema destinaciji.
9. Klijent kojem je paket izvorno namjenjen, sastavlja dva IP fragmenta u originalni IP paket veličine 1500 bajta.



Slika 5.3.1. Postupak fragmentacije iz primjera
Izvor: http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html#anc19

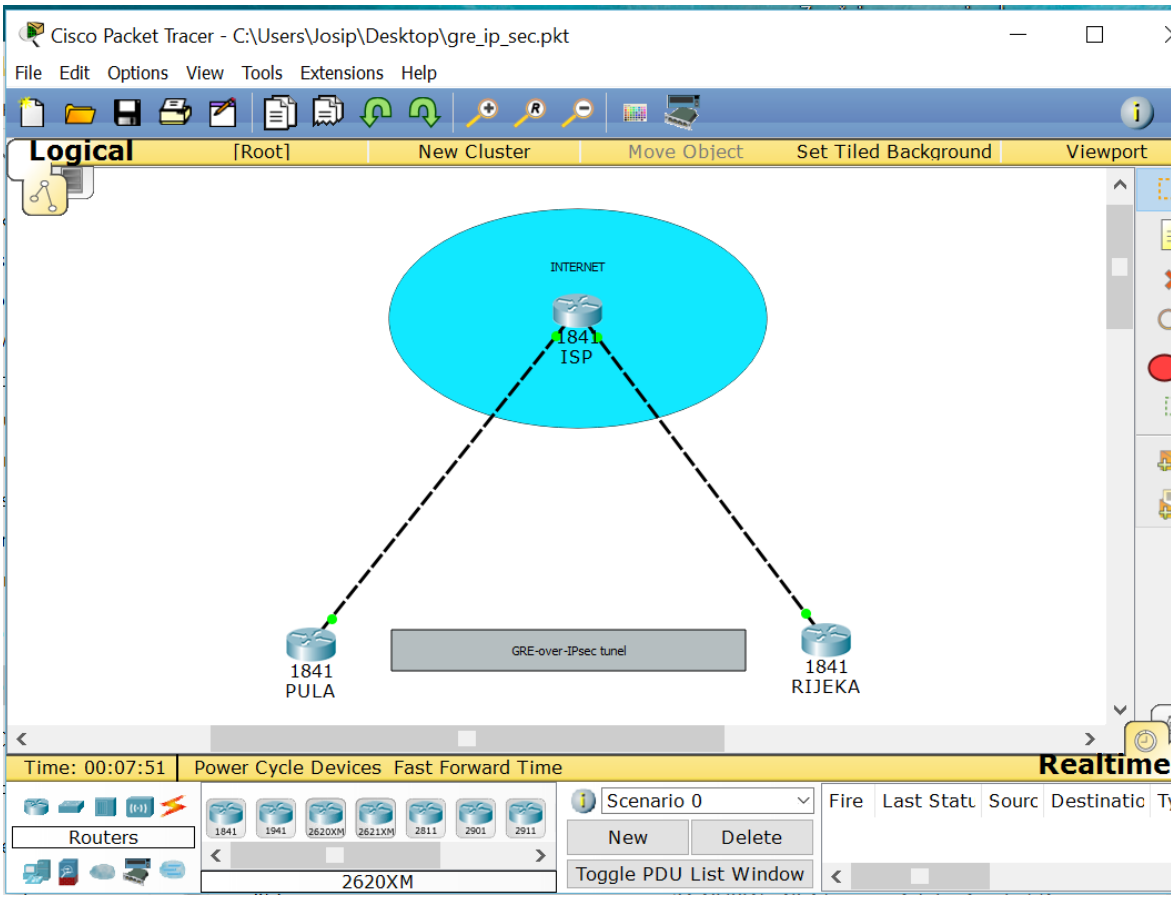
U ovom slučaju se sve moglo pojednostaviti te se mogla preskočiti dvostruka fragmentacija tako da smo na početku postaviti “ip mtu” vrijednost od 1420 bajtova.

6. Cisco Packet Tracer

Cisco Packet Tracer je programski alat razvijen od strane *Cisco Systems-a.* Omogućava korisniku da kreiraju mrežne sustave te da simuliraju moderne mrežne sustave. Program nam omogućava da simuliramo konfiguracije Cisco usmjernika i preklopnika pomoću simuliranog sučelja u koje se pomoću naredbenog retka upisuju naredbe za konfiguriranje uređaja. Radi na principu povuci i pusti (eng. *drag and drop*) te se na taj način dodaju i brišu simulacijski uređaji. Program je primarno namjenjen polaznicima *Certified Cisco Network Associate Academy* kao sredstvo pomoću kojeg uče osnovne CCNA koncepte. Polaznici CCNA akademije mogu besplatno preuzeti i koristiti ovaj alat za edukativne potrebe.

Uz to što se koristi za simulaciju pojedinih mrežnih topologija, *Packet Tracer* se može korisiti i za suradnju. Od verzije *Packet Tracer-a* 5.0, podržava i vise-korisničku (eng. *multi-user*) platformu koja omogućuje da se više korisnika poveže te da povežu različite simulirane mrežne topologije preko računalne mreže. *Packet Tracer* također omogućava instruktorima da naprave simulacije koje zatim učenici moraju dovršiti. Ovaj alat se najčešće koristi u edukacijskim krugovima kao obrazovno pomagalo. *Cisco Systems* tvrdi da je ovaj alat jako koristan i za eksperimentiranje u računalnim mrežama.

Kako je mrežna oprema koja se koristi u ovom radu vrlo skupa, u nedostatku opreme koristio sam ovaj alat za simulacije i testiranje GRE tunela te za pronalazak najboljeg rješenja za GRE i GRE over IPsec tunele (slika 6.1).



Slika 6.1 Sučelje Packet Tracer alata sa simulacijom GRE tunela

7. Zaključak

U ovom radu sam dokazao funkcionalnost GRE tunela, te GRE-over-IPsec tunela, te smo naveli njegove prednosti i mane. Bilo je vrlo zanimljivo konfigurirati opremu jer konfiguriranjem uređaja možemo korak po korak i shvatiti logiku unutar samih uređaja, te načina na koje oni funkcioniraju i protokole kojima izvode naše naredbe.

Kod izrade ovog rada, od velike mi je pomoći bilo to što sam pohađao *Cisco akademiju,* CCNA program, koja se održava u prostorima našeg fakulteta. Ovdje sam se prvi put susreo i upoznao sa ovom mrežnom opremom, te naučio osnove konfiguriranja. Nažalost, u sklopu studija Komunikacije više smo radili teorijski dio računalnih mreža, a manje praktični dio tako da mi je pohađanje *Cisco akademije* jako puno značilo.

Da bi mogli shvatiti rad GRE tuneliranja, morali smo se dotaknuti i nekih osnovnih pojmova vezano uz računalne mreže da bi mogli shvatiti na kojim razinama GRE i IPsec protokoli djeluju, što sve moramo predviditi dok paket putuje od izvora prema odredištu te predvidjeti i otkloniti sve probleme s kojima se možemo susresti da bi postigli onu funkcionalnost računalne mreže koju želimo.

8. Conclusion

In this paper I have proved functionality of GRE and GRE-over-IPsec tunnels, and I have explained pros and cons of using them. It was very interesting to configure equipment used in this paper because by configuring them you can understand just how the equipment is functioning and you can see step-by-step how the equipment is translating our informations and commands.

.

For writing this paper, attending of *Cisco Academy,* CCNA program was very helpful. Here I was introduced to network equipment and I have learned basics of configuration. Unfortunaly, at our faculty program, *Communications,* we didn't have a lot of chance to see and learn configuration of this kind of network equipment. We were more focused on theory and less on practical part of Computer Networking.

To understand how GRE tunnel is functioning, we first had to explain basics terms which are used in computer networking, so that we can explain at which network levels GRE and IPsec protocols are working, what we must anticipate in travel of the packet from source to destination and remove all the possible problems which the packet may endure on his travel so that we get funcionality of network which we want.

Izvori:

[1] *http://searchenterprisewan.techtarget.com*

[2] *http://www.ciscopress.com/articles/article.asp?p=348253&seqNum=7*

[3] *https://www.ietf.org*

[4] *http://www.techtarget.com/*

[5] *http://www.lantronix.com/*

[6] *https://www.packet6.com/getting-started-with-ciscos-500-series-smb-switches/*

[7] *https://supportforums.adtran.com/*

[8] *http://www.rfc-base.org/rfc-2784.html*

[9] *http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html#anc11*

[10] *https://technet.microsoft.com/en-us/library/cc958821.aspx*

[11] *http://www.firewall.cx/networking-topics/protocols/127-ip-security-protocol.html*

[12] *http://www.isaserver.org/articles-tutorials/articles/IPSec_Passthrough.html*

[13] *http://www.free-it.org/archiv/talks_2005/paper-11156/paper-11156.html*

[14] *http://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/872-cisco-router-gre-ipsec-tunnel-transport.html*

[15] *http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html#anc19*

[16] *https://supportforums.cisco.com/document/86786/how-add-wic-2t-card-router-2800*

Dodatak A

Konfiguracija usmjernika PULA kod uspostavljenog GRE-over-IPsec tunela

```
Building configuration...

Current configuration : 1313 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname PULA
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
lifetime 3600
!
crypto isakmp key CISCO address 192.168.23.3
!
!
!
crypto ipsec transform-set TRANS esp-aes 256 esp-sha-hmac
!
crypto map MYMAP 10 ipsec-isakmp
set peer 192.168.23.3
set transform-set TRANS
match address 100
!
!
!
!
```

```
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface Loopback0
ip address 172.16.1.1 255.255.255.0
!
interface Tunnel1
ip address 192.168.13.1 255.255.255.0
mtu 1476
tunnel source FastEthernet0/0
tunnel destination 192.168.23.3
!
!
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
duplex auto
speed auto
crypto map MYMAP
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 192.168.13.0 0.0.0.255 area 0
network 172.16.3.0 0.0.0.255 area 0
network 172.16.1.0 0.0.0.255 area 0
!
ip classless
ip route 192.168.23.3 255.255.255.255 192.168.12.2
!
ip flow-export version 9
!
!
access-list 100 permit gre any any
!
!
```

```
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```

Dodatak B

Konfiguracija usmjernika RIJEKA kod uspostavljenog GRE-over-IPsec tunela

```
Building configuration...

Current configuration : 1281 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname RIJEKA
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
```

```
group 5
lifetime 3600
!
crypto isakmp key CISCO address 192.168.12.1
!
!
!
crypto ipsec transform-set TRANS esp-aes 256 esp-sha-hmac
!
crypto map MYMAP 10 ipsec-isakmp
set peer 192.168.12.1
set transform-set TRANS
match address 100
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface Loopback0
ip address 172.16.3.3 255.255.255.0
!
interface Tunnel1
ip address 192.168.13.3 255.255.255.0
mtu 1476
tunnel source FastEthernet0/0
tunnel destination 192.168.12.1
!
!
interface FastEthernet0/0
ip address 192.168.23.3 255.255.255.0
duplex auto
speed auto
crypto map MYMAP
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
```

```
shutdown
!
router ospf 1
log-adjacency-changes
network 192.168.13.0 0.0.0.255 area 0
network 172.16.3.0 0.0.0.255 area 0
!
ip classless
ip route 192.168.12.1 255.255.255.255 192.168.23.2
!
ip flow-export version 9
!
!
access-list 100 permit gre any any
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```

Dodatak C

Konfiguracija usmjernika ISP kod uspostavljenog GRE-over-IPsec tunela

```
Building configuration...

Current configuration : 576 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ISP
!
!
```

```
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.23.2 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
```

```
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```