FTN Napredna Internet infrastruktura

Predmet: Napredna Internet infrastruktura

Izvodjači nastave: prof. dr Zora Konjović, Milan Kerac

Autori materijala: Milan Kerac, Ivan Nejgebauer

Zimski semestar 2009

FTN Napredna Internet infrastruktura

Šta je Internet infrastruktura?

Šta smo do sada naučili iz oblasti koje pokrivaju Internet infrastrukturu?

Opšte Standardi [1]

- U nedostatku standarda:
  - brzo se umnožava broj potrebnih implementacija za svaku vrstu komunikacije
  - korisnik se mora vezati za jednog proizvođača bez obzira na to što bi mu za neke potrebe više odgovarao drugi
  - promena proizvođača je skopčana sa velikim troškovima
- Standardi omogućavaju:
  - nezavisnost od jednog proizvođača
  - garanciju karakteristika

Opšte Standardi [2]

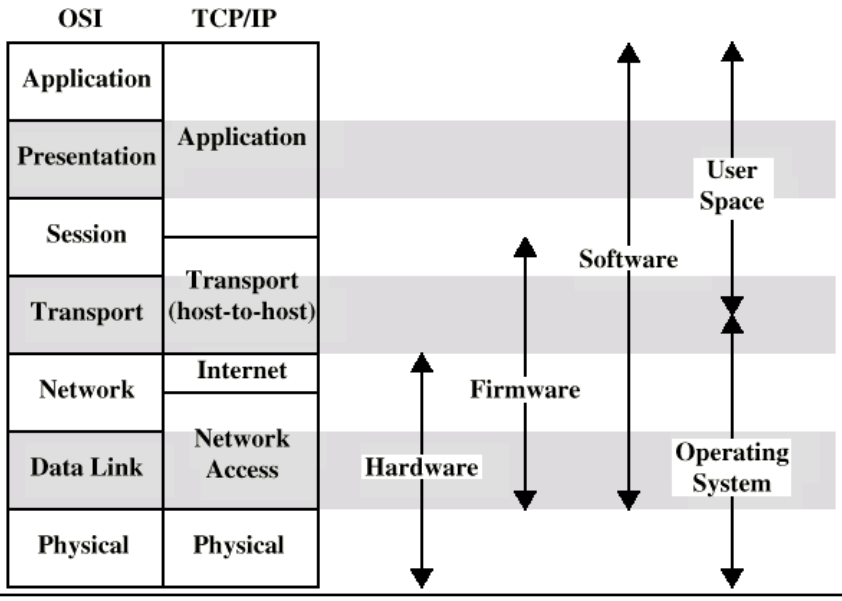
- Organizacije za standardizaciju
  - *Internet Society* – RFC, standardi vezani za Internet protokole – besplatni `http://www.ietf.org/rfc.html`
  - ISO/IEC – razne vrste standarda, između ostalog i oni vezani za komunikacije – plaćaju se `http://www.iso.org`
  - ITU-T (ranije CCITT) – telekomunikacioni standardi – plaćaju se `http://www.itu.int`
  - IEEE (serija 802) – standardi za lokalne računarske mreže – besplatni `http://standards.ieee.org`

Opšte OSI referentni model

OSI = *Open Systems Interconnection.*
Sedam nivoa:

- **fizički**
- **prenosni (data link)**
- **mrežni (network)**
- **transportni**
- **nivo sesije**
- **prezentacijski**
- **aplikacioni.**

Opšte OSI – TCP/IP



Opšte Nivo 1

- Opisuje:
  - električne (optičke)
  - mehaničke
  - funkcionalne i
  - proceduralne karakteristike prenosnih medijuma.
- Vrste prenosnih medijuma:
  - Žični
    - koaksijalni kabel
    - parice (neoklopljene i oklopljene)
    - optičko vlakno
  - Bežični

Opšte Nivo 2

- Opisuje razmenu podataka između uređaja koji dele isti prenosni medijum.
- Daje rešenje sledećih problema:
  - pristup prenosnom medijumu - MAC (*Medium Access Control*)
  - adresiranje uređaja povezanih na prenosni medijum – LLC (*Logical Link Control*)
  - kontrola protoka – LLC
  - detekcija i korekcija grešaka - LLC

Opšte

Nivo 3

Ako posmatramo skup uređaja povezanih na isti prenosni medijum, za komunikaciju nam je dovoljan nivo 2.

Šta ukoliko imamo više ovakvih skupova uređaja koji su međusobno povezani?

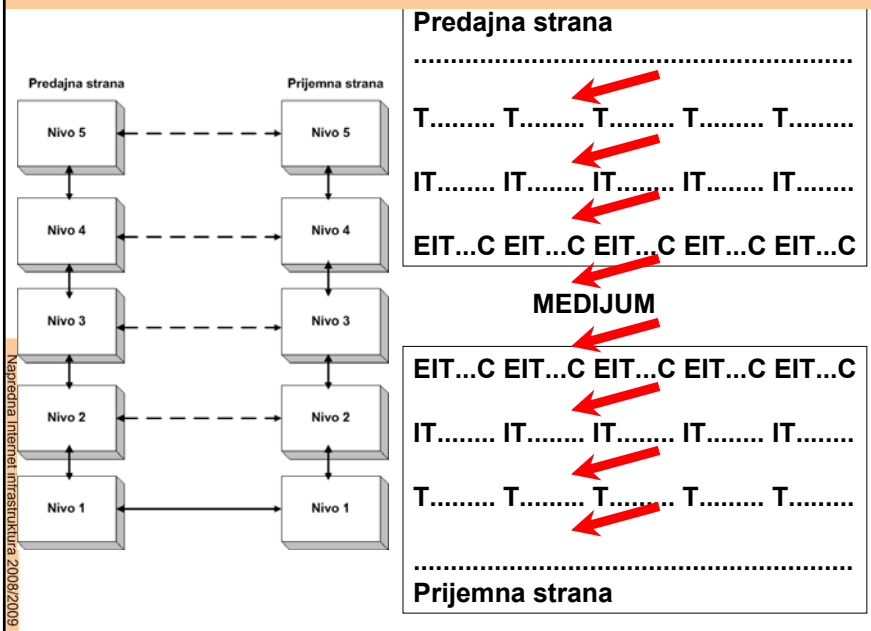
Nivo 3 opisuje razmenu podataka između ovakvih skupova uređaja.

Daje rešenje sledećih problema:

- adresiranje skupova uređaja i samih uređaja (različita vrsta adresiranja u odnosu na nivo 2)
- rutiranje – određivanje putanje prenosa podataka od izvora do odredišta

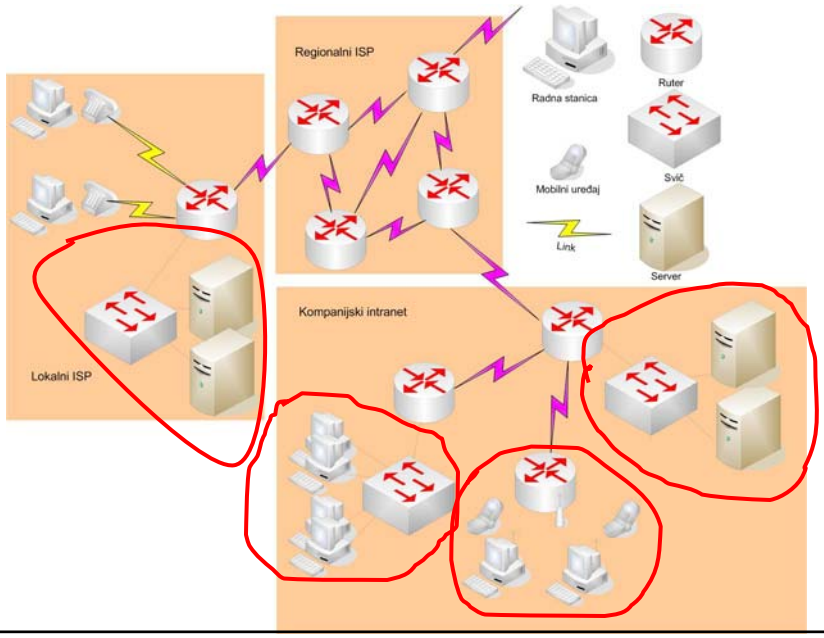
Opšte

Kako izgleda prenos podataka



Nivo 2

Deljeni medijum - Ethernet, Token Ring



Nivo 2

Lokalne mreže (LAN)

Definicija: mreža za prenos podataka, optimizovana za geografski mala područja, kao što su zgrada ili kampus. Obično se izvode sa deljenim vezama.
Mreže koje spajaju geografski veća područja se ponekad nazivaju **MAN** (*Metropolitan Area Network*).

Nivo 2

LAN standardi

IEEE 802 serija:
- 802.2 (LLC)
- 802.3 (CSMA/CD)
- 802.5 (Token Ring)

IEEE standardi su prihvaćeni od strane ISO i važe na međunarodnom nivou.

Nivo 2

Ethernet

Sistem sa zajedničkim medijumom.
Fizička izvedba:
- 10BASE2
- 10BASE5
- 10BASE-T
- 100BASETX
- 100BASEFX
- 1000BASET
- 1000BASESX
- 1000BASELX

Kontrola pristupa medijumu: CSMA/CD (IEEE 802.3).

Nivo 2

CSMA/CD

Algoritam koji koristi Ethernet (802.3):

ako je medijum slobodan, šalji; inače pređi na korak 2;

prati stanje medijuma; čim se oslobodi, pokušaj sa slanjem;

ako tokom slanja dođe do kolizije, prestani sa slanjem i emituj kratak signal (*jamming*);

čekaj izvesno vreme i vrati se na korak 1

Nivo 2

Kolizioni domen

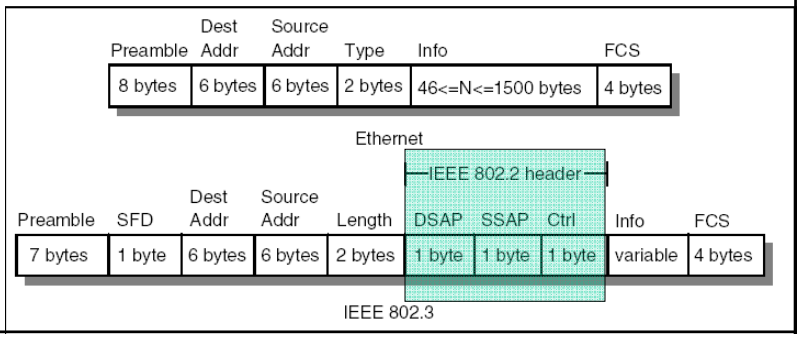
Dve stanice pripadaju jednom **kolizionom domenu** ako i samo ako prilikom istovremenog slanja frejma na deljeni medijum izazovu koliziju.

Nivo 2

Ethernet paket (frejm)

Uvodni niz od 56 bita za sinhronizaciju.
SFD: *Start of Frame Delimiter.*
Frejm:

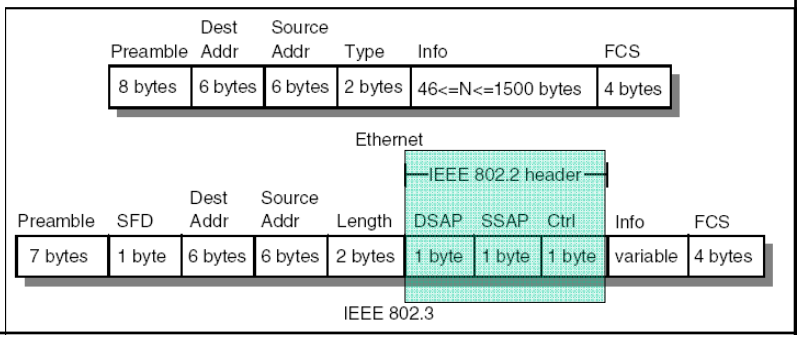
- odredišna i polazna adresa
- Tip/Dužina
- Podaci
- Kontrolna suma.



Nivo 2

Ethernet paket (frejm)

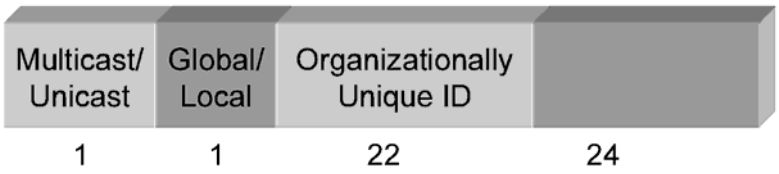
Maksimalna dužina Ethernet frejma 1518 B
Minimalna dužina Ethernet frejma 64 B
Moguće koristiti oba frejma na "na istoj žici"
Vrednost u polju Type veća od 1500, (IP – 2048 (0800))
DSAP i SSAP su polja u koja se upisuju oznake za *destination* i *source service Access Point*



Napredna Internet infrastruktura 2008/2009

Nivo 2

Ethernet frejm (adresno polje)



- Multicast = "To a group of stations on this LAN"
- Broadcast = "To all stations"
  = 111111....111 = FF:FF:FF:FF:FF:FF

Nivo 2

Broadcast domen

Dve stanice pripadaju jednom **broadcast domenu** ako i samo ako jedna stanica može da primi frejm poslat na broadcast adresu od strane druge stanice i obrnuto.

Nivo 2 Svičevi [1]

- Povezuju radne stanice, habove, svičeve
- Princip rada: paket primljen sa jednog porta emituje na drugi port
- Kako svič zna gde da uputi paket?
  - Svič analizira sve frejmove i na osnovu polaznih Ethernet adresa određuje koja je radna stanica priključena na određeni port.
  - Tabelu sa adresom radne stanice i brojem porta na koji je priključena svič čuva u memoriji.
  - Na osnovu odredišne adrese iz frejma i tabele svič zna na koji port treba da uputi paket.
  - Ima slučajeva kad se frejmovi šalju na sve portove (kada je frejm namenjen svima (broadcast) ili kada se ne zna port sa kojim je povezan sistem sa adresom kojoj je frejm namenjen (svič još nije formirao kompletnu tabelu).

Nivo 2 Svičevi [2]

Display Database Entries (100 at a time)

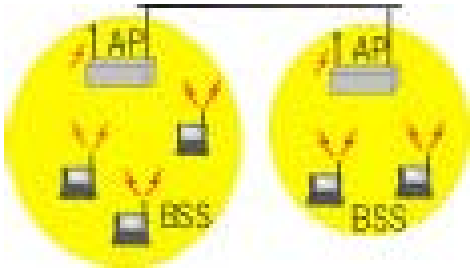
Unit	Port	VLAN	Mac Address	Status
			Ageing Time = 1800 secs	
1	3	1	00:40:05:39:ab:00	Learned
1	2	1	00:40:95:03:f8:4a	Learned
1	1	1	00:40:95:1a:fa:68	Learned
1	1	1	00:4f:49:01:1f:5a	Learned
1	1	1	00:50:ba:a8:b5:c2	Learned
1	1	1	00:60:52:02:5b:4d	Learned
1	1	1	00:a0:00:0c:8e:02	Learned
1	1	1	00:c0:df:e0:59:69	Learned
1	1	1	00:e0:1e:ea:6b:b2	Learned
1	1	1	08:00:20:99:e9:c5	Learned
1	1	1	08:00:4e:fa:3a:d8	Learned
			Total = 11 Perm = 0	

Port 3 - radna stanica
Port 2 - radna stanica
Port 1 - svič preko koga je naš svič povezan sa ostatkom mreže

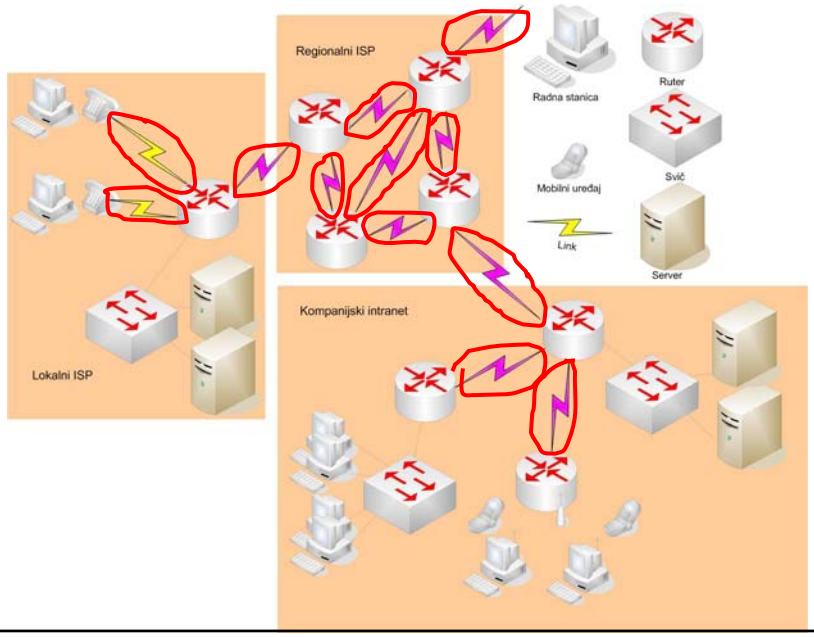
Nivo 2 Wireless LAN

Wireless LANs:
- IEEE 802.11 standard
- MAC protocol
- Slobodni opseg spektra: 900Mhz, 2.4Ghz

- **wireless hosts**
- **access point (AP)**



Nivo 2 Tačka-tačka veze – PPP i SLIP



Nivo 2 SLIP

Serial Line IP, RFC 1055.
Enkapsulacija: sa početnim i završnim znakom za frejm.

Problemi:
- obe strane moraju unapred znati sve parametre
- MTU se mora istovetno podesiti
- podržava samo IP
- nema proveru ispravnosti prenosa

Nivo 2 PPP

Point-to-Point Protocol, RFC 1661.
Rešava probleme SLIP-a:
- parametri se dogovaraju prilikom uspostavljanja veze
- postoji provera ispravnosti prenosa
- podržava i protokole osim IP-a
- mogućnost autentifikacije

Nivo 3

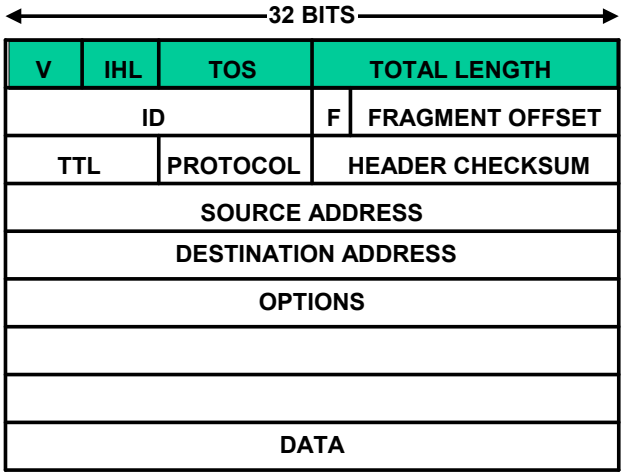
Ako posmatramo skup uređaja povezanih na isti prenosni medijum, za komunikaciju nam je dovoljan nivo 2.
Šta ukoliko imamo više ovakvih skupova uređaja koji su međusobno povezani?
Nivo 3 opisuje razmenu podataka između ovakvih skupova uređaja.
Daje rešenje sledećih problema:

- adresiranje skupova uređaja i samih uređaja (različita vrsta adresiranja u odnosu na nivo 2)
- rutiranje – određivanje putanje prenosa paketa

Internet Protokol - IP

RFC 791
Protokol trećeg OSI nivoa
IP paketi imaju zaglavlje i sadržaj
Ne garantuje isporuku
Paketi ne zavise jedan od drugog, prilikom prenosa paketi mogu putovati različitim putanjama
Paketi na odredište stižu proizvoljnim redosledom

Nivo 3 Detaljan opis IP paketa [1]



Nivo 3 Detaljan opis IP paketa [2]

V - verzija
- trenutno 4
- 4 bita

IHL - Internet Header Lenght
- broj 32-bitnih reči u zaglavlju
- 4 bita

TOS - Type of service
- tretman IP paketa u transportu
- 8 bita

TL - Total Lenght
- totalna dužina IP paketa u bajtima
- 16 bita

Nivo 3 Detaljan opis IP paketa [4]

ID - identification
- **16 bita**

F - Flags
- **3 bita**

FO - Fragment Offset
- **13 bita**

Nivo 3 Detaljan opis IP paketa [6]

TTL - Time to Live
- **postavlja gornju granicu postojanja paketa u tranzitu**
- **8 bita**

Protocol
- **oznaka protokola višeg nivoa**
- **8 bita**

Header checksum
- **kontrolna suma sadržaja zaglavlja**
- **16 bita**

Nivo 3 Detaljan opis IP paketa [8]

SA - Source Address
- polazna adresa
- 32 bita

DA - Destination Address
- odredišna adresa
- 32 bita

Options

DATA

Nivo 3 IP adresa [1]

Neophodna za komunikaciju

32-bitni broj koji se prikazuje kao četiri decimalna broja razdvojena tačkom

Na primer: 192.168.21.23

11000000 10101000 00010101 00010111

Dva dela:
- oznaka mreže (početni bitovi adrese), ID mreže
- oznaka sistema u okviru mreže (ostatak adrese)

Nivo 3 IP adresa [2] - kako do ID mreže

Prvobitna podela je na pet klasa

Klasa A 1.0.0.0 - 127.255.255.255

Počinje sa 0, 7 bita za oznaku mreže, 24 bita za oznaku računara, podrazumevana maska širine 8

Klasa B 128.0.0.0 - 191.255.255.255

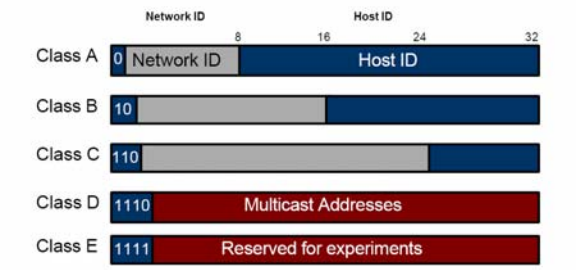
Počinje sa 10, 14 bita za oznaku mreže, 16 bita za oznaku računara, podrazumevana maska širine 16

Klasa C 192.0.0.0 - 223.255.255.255

Počinje sa 110, 21 bit za oznaku mreže, 8 bita za oznaku računara, podrazumevana maska širine 24

Klasa D 224.0.0.0 - 239.255.255.255

Klasa E 240.0.0.0 - 255.255.255.255



Nivo 3 IP adresa [3] - kako do ID mreže

IP Mrežu definišem sa ID i mrežnom maskom.

Broj bita za oznaku mreže određuje je pomoću mrežne maske (od 1 do 30 bita)

Specifičnost mrežne maske (dužina maske) – broj jedinica

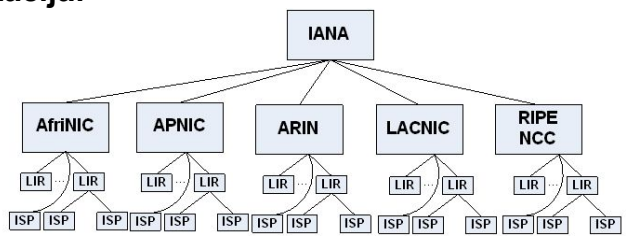
Mrežna maska se može zapisati u istom obliku kao i IP adresa

192.168.21.0, 255.255.255.0

192.168.21.0/24

Nivo 3 IP adresa [4] – Javni opseg

Javni opseg IP adresa
Javna IP adresa je jedinstvena na Internetu i jednoznačno određuje tačku koja učestvuje u komunikaciji
IANA – *Internet Assigned Numbers Authority,* organizacija zadužena da obezbedi centralnu koordinaciju osnovnih mehanizama na kojima se zasniva funkcionalnost Interneta.
Organizacija:



AfriNIC (African Network Information Centre) - Africa Region
APNIC (Asia Pacific Network Information Centre) - Asia/Pacific Region
ARIN (American Registry for Internet Numbers) - North America Region
LACNIC (Latin-American and Caribbean IP Address Registry) – Latin America and some Caribbean Islands
RIPE NCC (Réseaux IP Européens) - Europe, the Middle East, and Central Asia

Nivo 3 IP adresa [5] – Privatni opseg

Pretpostavka: Tačke koje se adresiraju pripadaju složenoj računarskoj mreži koja funkcioniše primenom TCP/IP familije protokola.
Podela:
• Privatne tačke su tačke koje direktno komuniciraju isključivo sa tačkama unutar složene računarske mreže kojoj pripadaju. Pristup javnim servisima ili servisima drugih računarskih mreža ostvaruje se preko posrednika (Proxy, NAT, Aplikativni serveri ...)
• Javne tačke su tačke koje direktno komuniciraju sa drugim javnim tačkama na Internetu

Nivo 3 IP adresa [6] – Privatni opseg

Adresiranje:

• Privatne tačke mogu da koriste adrese koje su jedinstvene u složenoj računarskoj mreži kojoj tačke pripadaju, ali ne moraju biti jedinstvene u odnosu na adrese tačaka koje pripadaju drugim računarskim mrežama. Za adresiranje privatnih tačaka koriste se IP adrese koje pripadaju privatnim IP adresnim opsezima. Privatni adresni opsezi definisani su dokumentom RFC 1918

```
10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
```

Šta se dobija:

Racionalnija upotreba javnih IP adresa, definisanje logičke arhitekture složene računarske mreže u cilju bolje kontrole tokova saobraćaja, povećan stepen bezbednosti u računarskoj mreži

Nivo 3 - 2 IP na lokalnoj mreži

Enkapsulacija:

Ethernet II (DIX, "Bluebook"), RFC 894

802.3, RFC 1042

MTU (*Maximum Transmission Unit*): maksimalna veličina IP paketa koji se može preneti preko određenog medijuma.

Za Ethernet sa Ethernet II enkapsulacijom MTU je 1500 bajtova.

Nivo 3 - 2 Razlika u formatu adresa

IP: 32 bita.
Ethernet: 48 bita.
Mora postojati mapiranje između ovih formata.
Za mapiranje IP – Ethernet koristi se ARP (*Address resolution protocol*), RFC 826.
Za obrnuto mapiranje koristi se RARP (*Reverese ARP*).

Nivo 3 - 2 ARP: mehanizam

Stanica A: `192.168.24.1`, `0:40:99:3:15:6`.
Pitanje: Ko ima IP adresu `192.168.24.2`?
Paket sa ARP upitom se šalje na specijalnu Ethernet adresu `ff:ff:ff:ff:ff:ff` (tzv. *broadcast* adresa).

Stanica B: `192.168.24.2`, `0:4f:37:1:1f:5a`.
Odgovor: `192.168.24.2` je na `0:4f:37:1:1f:5a`.
Paket sa odgovorom se šalje na Ethernet adresu `0:40:99:3:15:6`.

Nivo 3 - 2 IP na p-t-p vezama

Adrese na OSI 2 nivou ne postoje.
Na OSI 1 nivou može se koristiti asinhroni ili sinhroni prenos.
Dva metoda za IP enkapsulaciju na p-t-p vezama:

- SLIP (*Serial Line IP*), RFC 1055, jednostavan metod koji se danas relativno retko koristi.
- PPP (*Point to Point Protocol*), RFC 1661, može da posluži i za enkapsulaciju drugih protokola.

Nivo 3 IP fragmentacija [1]

Dešava se kad IP paket treba proslediti preko veze koja ima manji MTU od veličine paketa.
IP paket se na odredištu rekonstruiše od fragmenata i onda prosleđuje protokolu višeg nivoa.
Fragmenti mogu stići na odredište u bilo kom redosledu.

Nivo 3 Rutiranje [1]

Lokalni LAN segment: direktno su dostupni svi sistemi na istom segmentu.
Problem: šta raditi sa saobraćajem za sisteme van lokalnog segmenta?
Ruter (gateway): sistem kome se šalje saobraćaj za odredišta van lokalnog segmenta.
Svrha rutiranja: sistem mora utvrditi *kome* i *kuda* da šalje IP pakete.
Svaki sistem prilikom konfigurisanja za rad u mreži dobija sledeće parametre:

- svoju IP adresu i mrežnu masku (na osnovu čega zna kojoj IP mreži pripada)
- IP adresu rutera (*default gateway*).

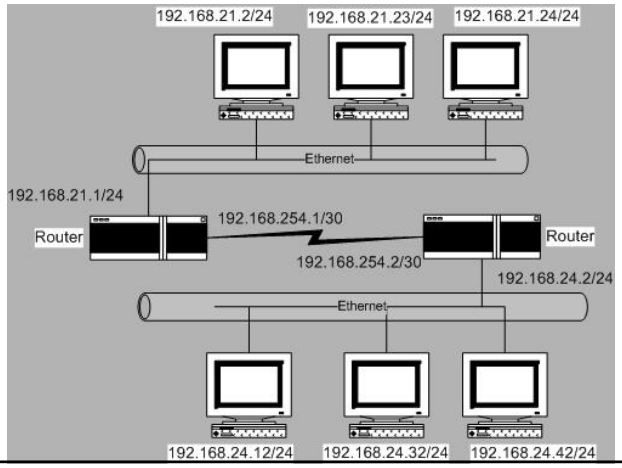
Nivo 3 Rutiranje [2]

Najjednostavniji slučaj: lokalni LAN segment.
Sistem zna kojoj IP mreži pripada, i zna IP adresu rutera.
Sav saobraćaj sa odredištem van njegove IP mreže šalje se ruteru.

Nivo 3 Tabela za rutiranje [1]

Za svaku stavku: adresa, maska, adresa rutera, interfejs.
Primer: sistem na lokalnom segmentu koji nije ruter

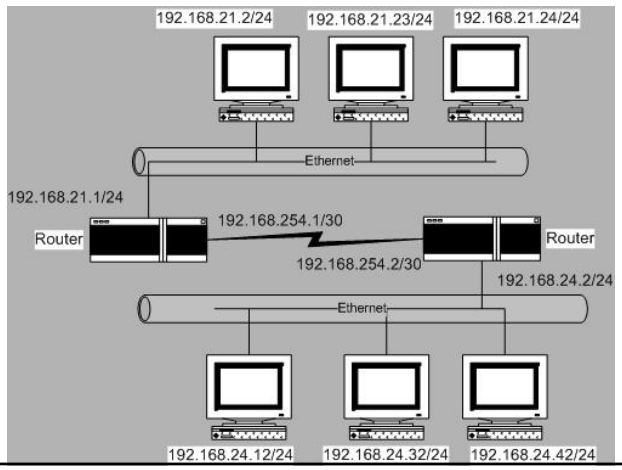
```
192.168.24.0    255.255.255.0  0.0.0.0        eth0
0.0.0.0         0.0.0.0        192.168.24.2   eth0
```



Nivo 3 Tabela za rutiranje [2]

Ruter:

```
192.168.24.0    255.255.255.0    0.0.0.0        eth0
192.168.254.0   255.255.255.252  0.0.0.0        sl0
192.168.21.0    255.255.255.0    192.168.254.1  sl0
```



Nivo 3 Dinamičko rutiranje

Proširivanjem mreže i povezivanjem većeg broja IP mreža konfigurisanje rutera postaje složenije; ako se to radi ručno (statički) raste mogućnost greške.

Dinamičko rutiranje je način da se podaci o dostupnosti odredišta i adresama rutera za pojedina odredišta razmenjuju automatski.

I dalje je potrebna minimalna statička konfiguracija.

Nivo 3 Protokoli za rutiranje [1]

Vektor udaljenosti (distance-vector).
Predstavnik: RIP (*Routing Information Proto-col*), RFC 1058.
Metrika: mera udaljenosti odredišta. RIP smatra metriku 16 za beskonačnu.
Problem: spora konvergencija u slučaju prekida neke veze.

Nivo 3 Protokoli za rutiranje [2]

Stanje veza (link-state).
Predstavnik: OSPF (*Open Shortest Path First*), RFC 2328.
Ruteri razmenjuju podatke o stanju svojih veza (interfejsa) sa susednim ruterima.
Svaki ruter ima potpunu sliku topologije cele mreže.

Nivo 3 Ruteri [1]

- Ruter je uređaj specijalizovan za rutiranje
- Dodatne funkcije
  - Filtriranje saobraćaja – bezbednost
  - Koncentrator za različite vrste tunela
  - Rešavanje zadataka iz oblasti kriptografije
- Različite tehnologije za povezivanje mreža
  - LAN Ethernet
  - LAN Token Ring
  - Serijske veze
    - Sinhrone
    - Asinhrone
  - ISDN - Integrated Services Digital Network
  - ATM - Asynchronous Transfer Mode
  - Frame relay

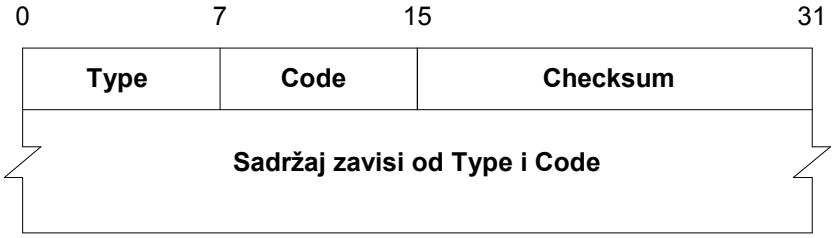
Nivo 3 ICMP

Internet Control Message Protocol, RFC 792.
Protokol na istom nivou kao IP, enkapsulira se u IP pakete sa oznakom protokola 1 (jedan).

Služi za:
- dijagnostiku,
- upravljanje,
- razmenu poruka o greškama.

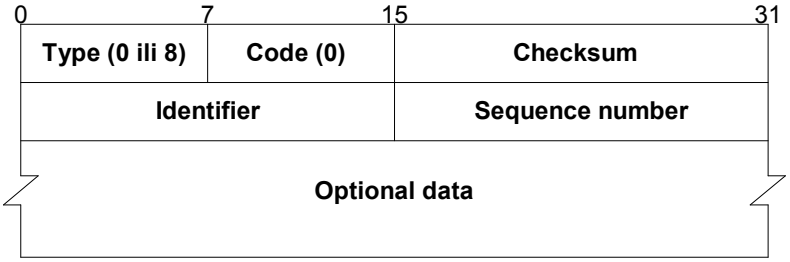
Primer: program *ping*, koji služi za proveru dostupnosti sistema na mreži.

Nivo 3 Format ICMP paketa



Type - 8 bita - identifikacija tipa ICMP poruke, koja može da se odnosi na više događaja
Code - 8 bita - tačno ukazuje na događaj
Checksum - 16 bita - kontrolna suma koja se odnosi na ceo ICMP paket

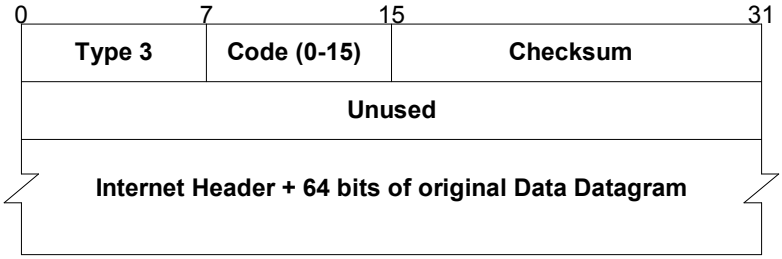
Nivo 3 Ping



Ping - služi za proveru dostupnosti hosta na mreži

Type - 0 echo reply, 8 echo request
Code - 0

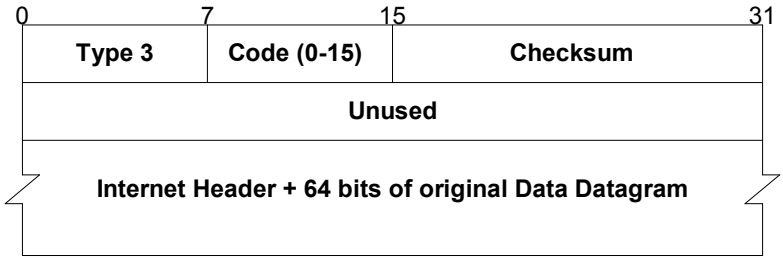
Nivo 3 Destination unreachable [1]



Type - 3
Code - uzima vrednosti od 0 do 15
Unused - mora celo polje da bude popunjeno 0

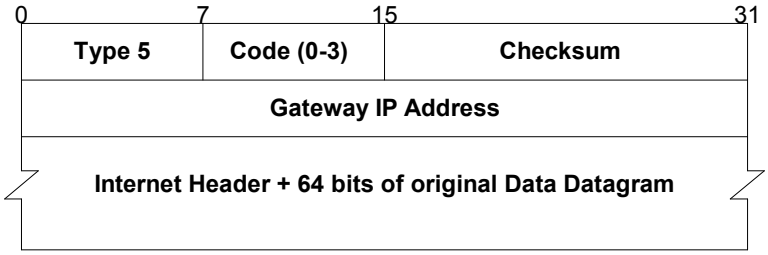
Moramo imati IP zaglavlje paketa koji je izazvao generisanje ICMP poruke o grešci.
Iz 64 bita sadržaja IP paketa dobijamo informacije koje su nam potrebne za protokole višeg nivoa

Nivo 3 Destination unreachable [2]



Code - 0 - network unreachable - ruter zna na koji port da pošalje paket, ali link nije aktivan
Code - 1 - host unreachable - ARP zahtev ne dobija odgovor ili administrativna zabrana (IP filtriranje)
Code - 4 - potrebno izvršiti fragmentaciju ali je DF fleg postavljen

Nivo 3 Redirekcija



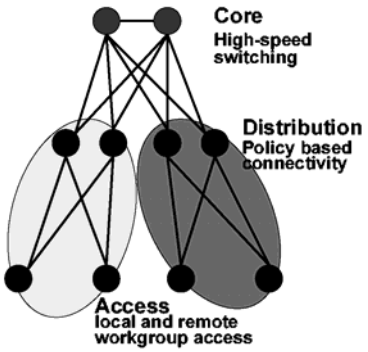
Type - 5
Code - 0 - Redirekcija za mrežu

Nivo 3 Redirekcija

Slučaj: tri povezane mreže, dva rutera na jednom od segmenata.
Sistem zna samo za jedan ruter; šalje mu i saobraćaj koji bi efikasnije bilo uputiti drugom ruteru.
Ruter tada šalje ICMP REDIRECT poruku sa IP adresom pogodnijeg rutera.

Opšte Dizajn mreže [1]

- **Centralni nivo**
  - **povezuje delove distributivog nivoa u celinu**
  - **kičma velike brzine**
- **Distributivni nivo**
  - **obuhvata oblasti**
  - **definiše brodkast domene**
  - **moguće kombinacije medijuma**
  - **definiše politiku zaštite**
  - **definiše veze ka drugim mrežama**
- **Pristupni nivo**
  - **svičovan medijum**
  - **kontrola na drugom nivou**
- **Uređaji za povezivanje – ruteri, L2, L3 svičevi**



Opšte Dizajn mreže [2]

- Kada rutirati
  - Brodkast kontrola
  - Povezivanje VLAN
  - Zaštita
  - Povezivanje LAN-ova izvedenih u različitim tehnologijama

Nivo 2-3 VLAN [1]

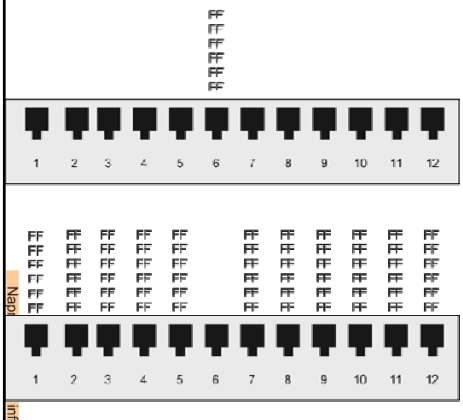
- Činjenica - Korporativne mreže povezuju velik broj radnih stanica;
- Činjenica - Upotreba Ethernet protokola u WAN delu, za posledicu ima povezivanje velikog broja radnih stanica;
- Problem - Kontrola saobraćaja na nivou 2 gotovo da nije moguća, narušena bezbednost i funkcionalnost mreže;
- Problem - Veliki broadcast domeni stvaraju tehničke probleme koji mogu izazvati prekide funkcionalnosti mreže;
- Rešenje – Mehanizam za podelu broadcast domena, njihovo povezivanje preko nivoa 3

Nivo 2-3 VLAN [2]

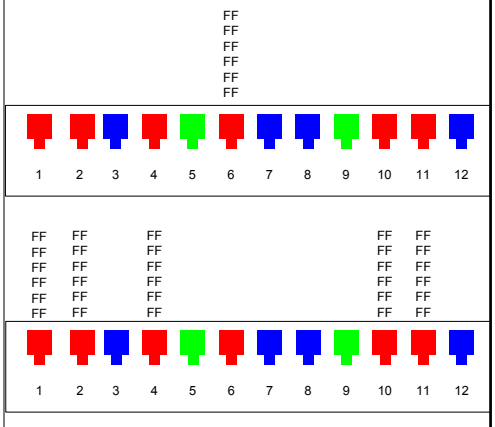
- **Običan svič** – Frejm adresiran na *broadcast* adresu prosleđuje na sve portove;
- **Ideja** - Frejm primljen sa jednog porta može da se prosledi samo na portove koji pripadaju istoj grupi kao i port sa kog je primljen frejm;

Nivo 2-3 VLAN [3]

- Običan svič



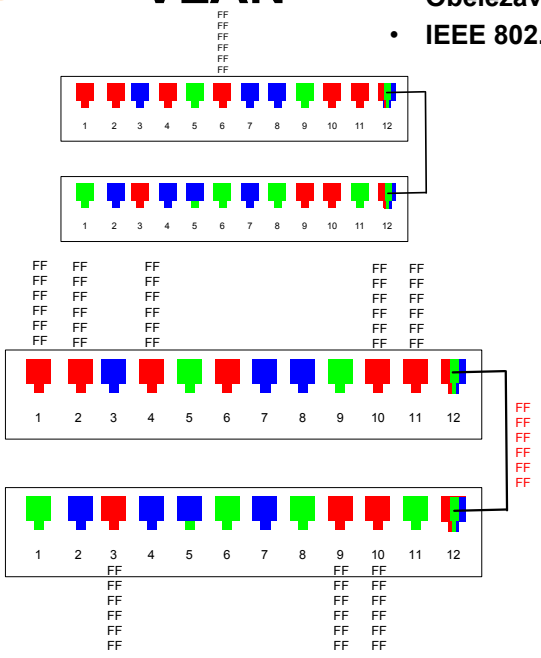
- VLAN svič



Nivo 2-3

VLAN [4]

- Obeležavanje frejma
- IEEE 802.1Q



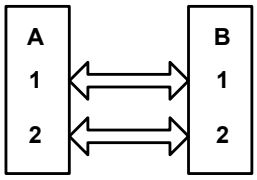
Nivo 2-3

VLAN [5]

- **Komunikacija između VLAN-ova – Samo preko nivoa 3;**
- **Potrebna veza preko 802.1Q linka sa ruterom ili upotreba svičeva sa implementiranom podrškom za rad sa protokolima nivoa 3 (rutiranjem). (*Layer 3 Switch, L3 Switch*)**
- **IP subnet se poklapa sa VLAN-om;**
- **Velike mogućnosti za kreiranje različitih logičkih arhitektura**

Nivo 4 Portovi

- Sistemi se identifikuju pomoću IP adrese
- Za potrebe aplikacija potrebno je više podataka



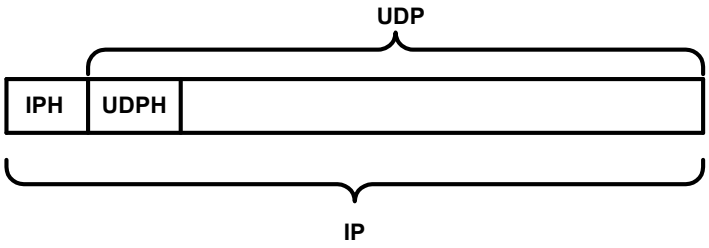
- Portovi - lokalno proširenje IP adrese (analogija lokali na TF centrali)
- 16 bita, neoznačeni, 0 - 65535
- Rezervisani portovi od 1 - 1023

Nivo 4 Klijent - Server

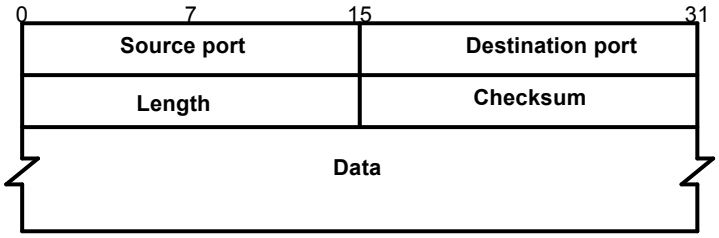
- Mrežne aplikacije se pišu tako da podrazumevaju da se sa jedne strane nalazi klijent, a sa druge strane server
- Server, po prijemu zahteva od klijenta, obradi klijentov zahtev i pošalje mu odgovor

Nivo 4 UDP

- *User Datagram Protocol,* RFC768
- Jednostavan protokol
- Za kratke poruke (do veličine MTU)
- Ne garantuje isporuku
- Enkapsulira se u IP paket sa oznakom protokola 17



Nivo 4 Format UDP paketa



- UDP paket ima svoje zaglavlje i podatke
- Source port - 16 bita - port aplikacije koja šalje podatke
- Destination port - 16 bita - port aplikacije kojoj su podaci poslati
- Length - 16 bita - dužina UDP paketa u bajtima
- Checksum - 16 bita - kontrolna suma koja se odnosi i na zaglavlje i na podatke

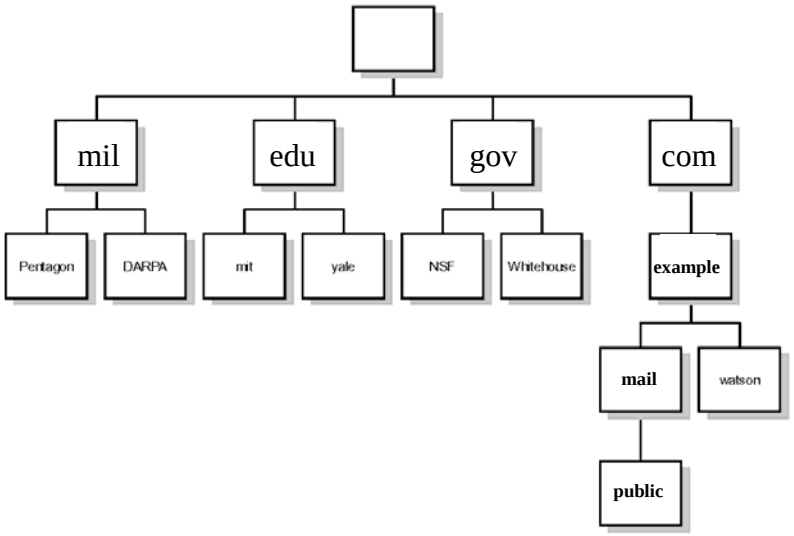
Nivo 5 DNS

- *Domain Name System*, RFC 1034, RFC 1035.
- Distribuirani sistem za opis hijerarhijski organizovanih skupova imena i pridruživanje različitih vrsta podataka tim imenima.
- Recimo: mail.example.org - 192.168.24.1
- Za upite koristi UDP sa rezervisanim portom 53.

Nivo 5 DNS, hijerarhija [1]

- FQDN (*Fully Qualified Domain Name*): public.mail.example.com.
- Puna imena se dobijaju zapisivanjem oznaka s leva na desno, od najspecifičnije (na najnižem nivou) ka najmanje specifičnom. Oznake se razdvajaju tačkama.
- Vrh hijerarhije ima prazno ime.

Nivo 5 DNS, hijerarhija [2]



Nivo 5 DNS, pretpostavke

- **Dostupnost podataka bitnija je od njihove ažurnosti (ali ima načina da se veća ažurnost zahteva).**
- **Podaci se većinom sporo menjaju.**
- **U sistemu je obezbeđena redundantnost.**
- **Granice administrativne odgovornosti za podatke uglavnom se poklapaju sa organizacionom strukturom institucija koje podatke održavaju.**

Nivo 5 DNS, organizacija

- **Područje odgovornosti nekog servera zovu se *zone*. Podaci o zonama zapisani su lokalno za primarne servere; sekundarni serveri preuzimaju podatke od primarnih.**
- **Server može da poveri (*delegira*) odgovornost za deo neke zone drugim serverima.**

Nivo 5 Primer zone

```
@    IN    SOA    ns.example.org. root.example.org. (
                  1999120300     ; serial
                  43200          ; reload
                  1800           ; retry
                  604800         ; expire
                  86400)         ; minimum TTL
           NS     ns.example.org.
           MX     0  mail.example.org.
ns         A      192.168.24.2
mail       A      192.168.24.1
blast      CNAME  blob.example.org.
blob       A      192.168.24.3
           MX     0  blob.example.org.
           MX     10 mail.example.org.
```

Nivo 5 Mapiranje adresa u imena

- **Problem: znajući IP adresu nekog sistema, kako mu saznati ime?**
- **Naročiti pseudo-domen: in-addr.arpa.**
- **Komponente decimalnog zapisa IP adrese u obrnutom redosledu čine nivoe hijerarhije i razgraničavaju zone.**
- **Recimo: 2.24.168.192.in-addr.arpa.**

Nivo 5 Zona za inverzno mapiranje

- **Koristi se PTR tip RR.**

```
@    IN    SOA    ns.example.org. root.example.org. (
                  1999120300     ; serial
                  43200          ; reload
                  1800           ; retry
                  604800         ; expire
                  86400)         ; minimum TTL
           NS     ns.example.org.
1          PTR    mail.example.org.
2          PTR    ns.example.org.
3          PTR    blob.example.org.
```

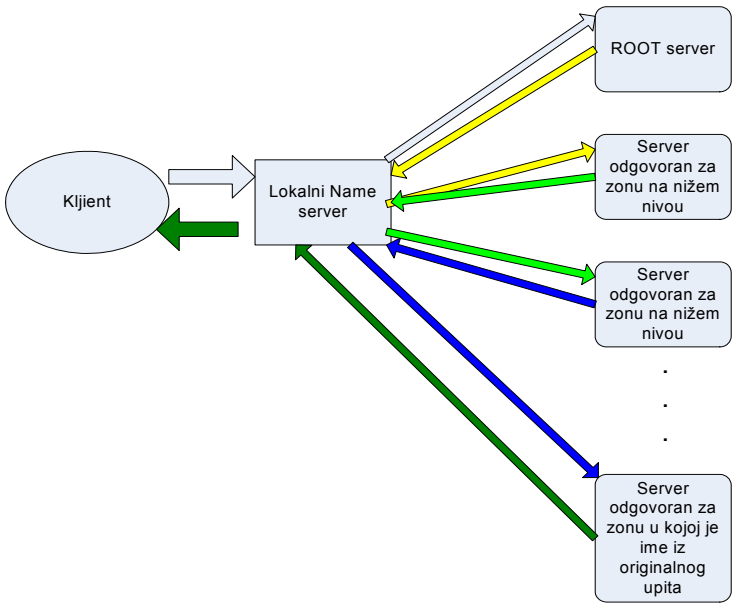
Nivo 5 DNS, dobijanje odgovora

- U svakom distribuiranom sistemu može se desiti da pojedinačni server ne može da vrati direktan odgovor klijentu.
- Rekurzivno: server sam prosleđuje upit dalje (povoljnije klijentu, zahtevnije serveru).
- Iterativno: server vraća klijentu poruku sa indikacijom kome se sledećem treba obratiti (zahtevnije klijentu, povoljnije serveru).

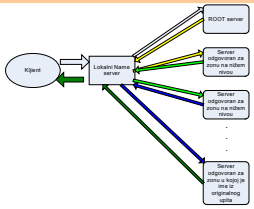
Nivo 5 DNS, dobijanje odgovora

- Svaki korisnički sistem ima *resolver* zadužen za slanje upita za aplikacije i prosleđivanje dobijenih odgovora aplikacijama.
- Konfiguracioni parametar korisničkog sistema je adresa Lokalnog Name servera, koji je zadužen za prosleđivanje upita i vraćanje dobijenih odgovora.
- Lokalni Name server je posrednik za grupu korisničkih sistema koji olakšava posao *resolver-ima* samih korisničkih sistema.
- Root Name Servers – Serveri zaduženi za “root” zonu na vrhu hijerarhije.
  Trenutno {a-m}.root-servers.net.

Nivo 5 DNS, dobijanje odgovora



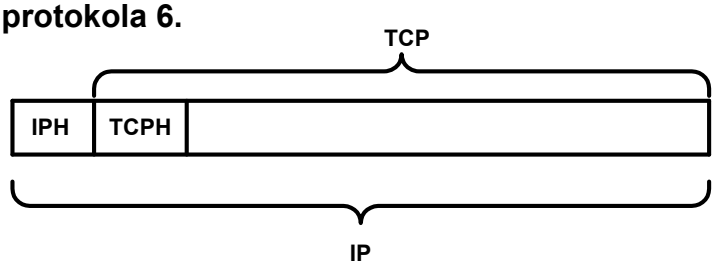
Nivo 5 DNS, dobijanje odgovora



- **Klijent (njegov *resolver*) šalje upit Lokalnom Name serveru.**
- **Lokalni Name server šalje upit root-serveru**
- **Root-server šalje odgovor Lokalnom Name serveru sa informacijom ko je odgovoran za zonu na nižem nivou hijerarhije.**
- **Lokalni Name server šalje upit sistemu koji je definisan odgovorom root-servera**
- **...**
- **Lokalni Name server šalje upit sistemu koji je odgovoran za zonu kojoj pripada ime za koje se šalje upit.**
- **Sistem koji je odgovoran za zonu kojoj preipada ime za koje se šalje upit odgovara sa IP adresom kojoj je dodeljeno ime iz upita, odgovor se šalje Lokalnom Name serveru, koji dalje odgovor prosleđuje Klijentu (njegovom *resolver-u*)**

Nivo 4 TCP [1]

- *Transmission Control Protocol*, RFC 793.
- Protokol koji ima garanciju isporuke (pod uslovom da funkcionišu protokoli nižeg nivoa), predviđen za prenos niza podataka željene dužine (po načinu na koji podatke posmatra aplikacija) — za razliku od UDP-a.
- Ima portove, kao i UDP.
- TCP segment enkapsulira se u IP paket sa oznakom protokola 6.



Nivo 4 TCP [2]

- U klijent/server modelu, na način koji se koristi kod TCP/IP mreža, serveri koji žele da im se klijenti obraćaju pomoću TCP-a uglavnom koriste rezervisane (poznate) portove.
- TELNET: 23, SMTP: 25, HTTP: 80.
- Primer TCP veze: zahtev za Web stranicom
  - klijent otvara IP konekciju ka serveru sa odredišnom IP adresom servera i odredišnim portom 80;
  - server prima zahtev i šalje odgovor u paketima gde su zamenjene polazna i odredišna IP adresa i polazni i odredišni port.

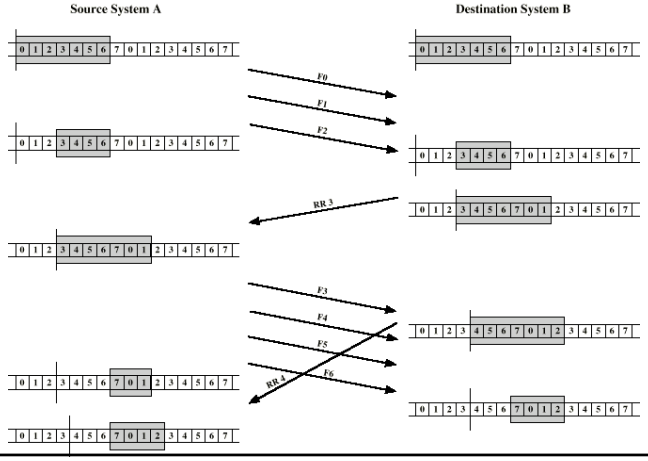
Nivo 4 TCP, zaglavlje [1]

- **Enkapsulacija u IP, protokol ID=6.**

SP	DP
SEQUENCE	
ACKNOWLEDGMENT	
HL / FLAGS	WINDOW
CHECKSUM	URGENT

Nivo 4 TCP, zaglavlje [2]

- **SP, DP: izvorni i odredišni port.**
- **SEQUENCE, ACKNOWLEDGMENT: vrednosti za označavanje pozicije poslatih i proveru redosleda primljenih segmenata.**
- **WINDOW: mehanizam za kontrolu toka podataka.**
- **CHECKSUM: provera validnosti celog segmenta.**



Nivo 4 TCP, zaglavlje [3]

- Značajni bitovi FLAGS polja:
  - URG
  - ACK
  - PSH
  - RST
  - SYN
  - FIN

Nivo 4 TCP, stanja veze [1]

- Fiktivno mirno stanje: CLOSED.
- Pasivno otvaranje: LISTEN.
- Uspostavljanje veze: SYN_SENT, SYN_RCVD.
- Kada se veza uspostavi, nalazi se u stanju ESTABLISHED.

Nivo 4 TCP, stanja veze [2]

- Aktivno zatvaranje: FIN_WAIT_1, FIN_WAIT_2, CLOSING.
- Pasivno zatvaranje: CLOSE_WAIT, LAST_ACK.
- Iz aktivnog zatvaranja prelazi se u stanje TIME_WAIT, iz pasivnog u CLOSED.

Nivo 4TCP, uspostavljanje veze [1]

- Tzv. *three-way handshake*.
- Klijent šalje SYN, prelazi u SYN_SENT.
- Server prima SYN, šalje SYN+ACK, prelazi u SYN_RCVD.
- Klijent prima SYN+ACK, šalje ACK, prelazi u ESTABLISHED.
- Server prima ACK, prelazi u ESTABLISHED.

Nivo 4TCP, uspostavljanje veze [2]

- Za svaki smer veze se prilikom početne razmene nezavisno dogovaraju sekvence.
- Takođe, dogovara se MSS (*Maximum Segment Size*), obično se računa kao MTU izlaznog interfejsa umanjena za 40 (dužine IP i TCP zaglavlja).
- Za MSS se uzima manja od razmenjenih vrednosti.

Nivo 4 TCP, zatvaranje veze

- Veza je dvosmerna.
- Svaki smer se može nezavisno zatvoriti.
- Veza čiji je jedan smer zatvoren se naziva poluzatvorenom (*half-closed*).

Nivo 4 Path MTU Discovery

- Specifikacija: RFC 1191.
- Način da se optimalno izabere vrednost MSS (maksimalna veličina segmenta) za neku vezu, cilj je da se izbegne fragmentacija.
- Šalju se IP paketi sa postavljenim DF flegom, pa se veličina MSS smanjuje ako se dobije ICMP NEED_FRAG poruka.

FTN Napredna Internet infrastruktura

Sada smo sigurni da imamo dobro osnovno znanje da se upustimo u dalje otkrivanje tajni Internet infrastrukture.

Internet infrastrktura [1]

- Ip mreže, u odnosu na ostale tipove mreža u današnjim komunikacionim sistemima, preuzimaju vodeću ulogu.
- Ip mreže imaju sledeće prednosti u odnosu na dosadašnje komunikacine sisteme:
  - skalabilnost,
  - efikasnost,
  - podrška velikom broju raznorodnih servisa i
  - mogućnost brze reakcije na tržišne zahteve za novim servisima.
- Prednosti IP mreža ne treba da sakriju mane koje proističu iz ovih prednosti.

Internet infrastrktura [2]

- Raznorodnost servisa za koje se prenose podaci IP mrežom:
  - Standardni Internet servisi,
  - Servisi za prenos govora,
  - Servisi za prenos videa,
  - Servisi za podršku širokom spektru poslovanja,
  - Servisi mobilne telefonije,
  - ....
- Svaki od servisa ima vrlo specifične zahteve koji se postavljaju pred IP mrežu (npr. dostupnost znači jedno za standardne Internet servise i servise za podršku poslovanju, a nešto sasvim drugo za servise za prenos govora)

Internet infrastrktura [4]

- Osnove na kojima se zasniva funkcionalnost IP mreža:
  - Korisnički podaci i podaci od kojih zavisi funkcionalnost IP mreže prenose se istim "kanalom".
    - Prednost: nema potrebe za paralelnom kontrolnom infrastrukturom.
    - Mana: moguće narušavanje funkcionalnosti usled odredjenih zavisnosti između korisničkih i podataka od kojih zavisi funkcionalnost mreže
  - Osnovni tehnološki koncept omogućava any-to-any i end-to-end konektivnost.
    - Prednost: Jednostavnost korišćenja, širenja i prilagođavanja novim situacijama.
    - Mana: Mogućnost širokog uticaja na funkcionalnost mreže.
  - Funkcionalnost se zasniva na standardima IETF koji su široko dostupni.
    - Prednost: Velika baza za razvoj i unapređenje servisa.
    - Mana: Suviše brz razvoj koji je teško pratiti.

Internet infrastrktura [5]

- Tipovi IP mreža:
  - Korisnička mreža
  - ISP mreža
- Na prvi pogled nema nekih bitnih razlika.
- Ako ih sagledamo kroz prizmu IP saobraćaja uočićemo razlike.

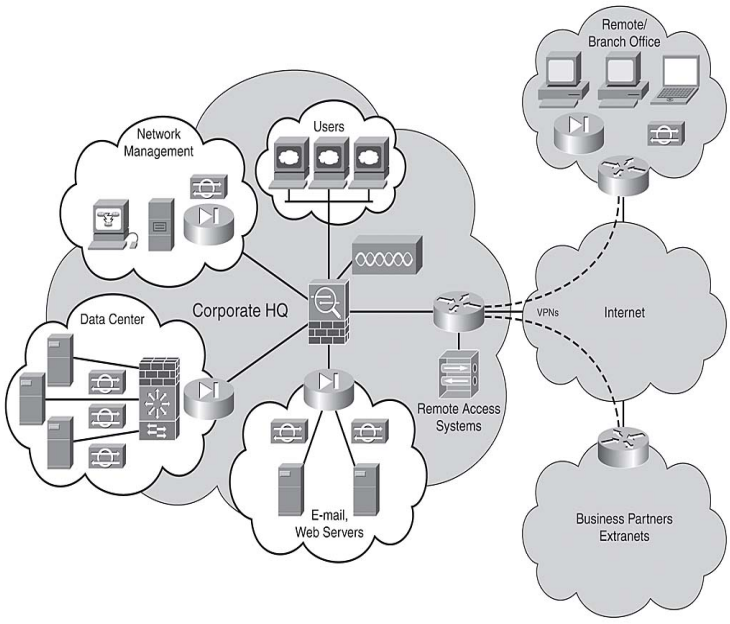
Internet infrastrktura [6]

- **Korisničke mreže pružaju infrastrukturnu podršku IS u poslovnim sistemima i posredno utiču na stvaranje profita.**
- **Korisničke mreže treba da:**
  - **Obezbede internim korisnicima upotreba internih servisa organizacije koja je vlasnik mreže.**
  - **Obezbede se internim korisnicima upotreba eksternih servisa.**
  - **Obezbede svim eksternim korisnicima upotrebu servisa namenjenih eksternim korisnicima.**
  - **Obezbede određenim eksternim korisnicima upotrebu dela internih servisa.**

Internet infrastrktura [7]

- **Bez obzira na veličinu korisničke mreže imaju zajedničke karakteristike:**
  - **Jasno definisanu arhitekturu (centralni, distributivni i pristupni nivo).**
  - **Jasno definisanu granicu gde je kraj korisničke mreže (privatne), odnosno početak ISP mreže (javne). Granica jasno razdvaja prava po vlasništvu, odgovornost za funkcionalnost i prava pristupa.**
  - **Jasno definisani protokoli koji obezbeđuju funkcionalnost korisničke mreže (protokoli za dinamičko rutiranje, protokoli za nadgledanje i upravljanje mrežom ...)**
  - **Jasno definisani tokovi IP saobraćaja unutar mreže i strogo upravljani tokovi saobraćaja na prelazu privatno – javno u skladu sa politikom zaštite.**
  - **Ne postoji tranzitni saobraćaj kroz korisničke mreže, tokovi saobraćaja ili nastaju ili se završavaju u okviru korisničke mreže.**

Internet infrastrktura [8]



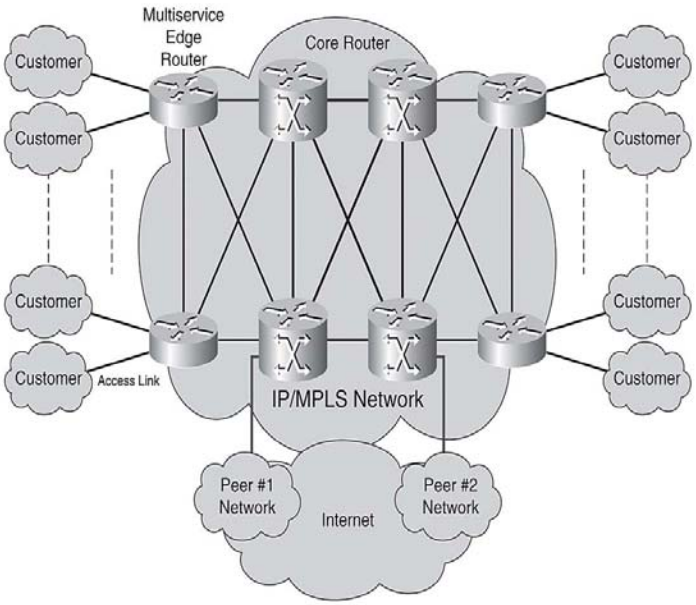
Internet infrastrktura [9]

- **ISP mreže su osnovno sredstvo za stvaranje profita.**
- **ISP mreže treba da:**
  - **Obezbedi tranzitni saobraćaj za svoje korisnike "mušterije" između sebe i za njihov pristup svim javnim servisima.**
  - **Obezbedi uslove za kvalitetan pristup servisima koje ISP uslužno pruža za svoje korisnike, a koje nudi eksternim korisnicima (hosting).**
  - **Obezbedi uslove za kvalitetan pristup servisima koje ISP nudi eksternim korisnicima (VoIP).**

Internet infrastrktura [10]

- **Bez obzira na veličinu ISP mreže (lokalna, regionalna, kontinentalna ili globalna), izdvajaju se zajedničke karakteristike:**
  - **Jasno definisanu arhitekturu (centralni deo, rubni deo sa "points of presence" (PoP)).**
  - **Jasno definisanu granicu prema dve grupe entiteta, korisničkim mrežama i drugim ISP mrežama. Granica jasno razdvaja prava po vlasništvu, odgovornost za funkcionalnost i prava pristupa.**
  - **Jasno definisani protokoli koji obezbeđuju funkcionalnost ISP mreže (protokoli za dinamičko rutiranje, protokoli za nadgledanje i upravljanje mrežom ...). Ovi protokoli imaju uticaja i na funkcionalnost susednih mreža.**
  - **Slabo definisani tokovi tranzitnog saobraćaja.**
  - **Velika količina tranzitnnog saobraćaja ali i prisutnost tokova saobraćaja koji ili nastaju ili se završavaju u okviru mreže.**

Internet infrastrktura [11]



Internet infrastrktura [12]

- **Poredjenje po upravljanju tokovima saobraćaja**

Korisničke mreže	ISP mreže
• Stroga gramica ka Internetu – Saobraćaj od spoljneg sveta ka unutrašnjoj mreži moguć kao povratni smer veze inicirane iz unutražnje mreže ili iniciran spolja uz strogu kontrolu. – Prvo se sve zabrani, pa se prave izuzeci. • Prave se da podrže interni saobraćaj i pretpostavlja se mala količina eksternog saobraćaja – Daje mogućnost analize tokova saobraćaja do nivoa aplikacije (mala količina saobraćaja omogućava komplikovanije analize koje "usporavaju" i zahtevnije su po pitanju resursa.	• Relaksirane granice – Namenjene za tranzitni saobraćaj, sav saobraćaj je dozvoljen dok se ne zabrani (što je retko). – Prvo se sve dozvoli, pa se prave izuzeci. • Prave se za brz transport tranzitnog saobraćaja – Komplikovanije analize tokova saobraćaja su potpuno suprotne prirodi same mreže, pogotovu na njenim rubnim delovima

Internet infrastrktura [13]

- **Ako računarske mreže posmatramo sa tačke gledišta tokova saobraćaja dolazimo do podataka koji su nam dragoceni u procesu dizajna mreže (do nivoa uticaja na izbor konkretne aktivne opreme) i definisanja logičke arhitekture mreže (od adresnog plana do politike zaštite).**

Grupe tokova saobraćaja [1]

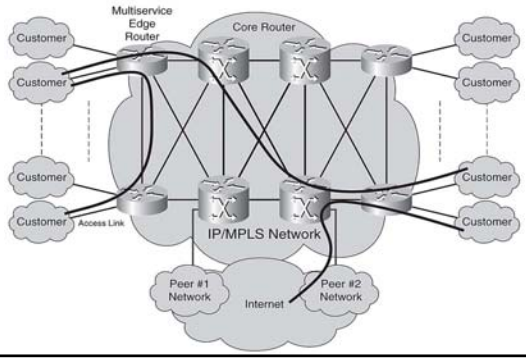
- Šta se može naći na interfejsu uređaja
  - frejm u kome je enkapsuliran IP paket namenjen tranzitu,
  - frejm u kome je enkapsuliran IP paket namenjen višim slojevima na samom uređaju,
  - frejm u kojima nije enkapsuliran IP (ARP, CDP ...),
  - frejm u koji je enkapsuliran IP paket koji izaziva pokretanje određenih procedura na trećem nivou.

Grupe tokova saobraćaja [2]

- Grupe tokova saobraćaja:
  - Grupa korisničkog saobraćaja
  - Grupa kontrolnog saobraćaja
  - Grupa upravljačkog saobraćaja
  - Grupa servisnog saobraćaja

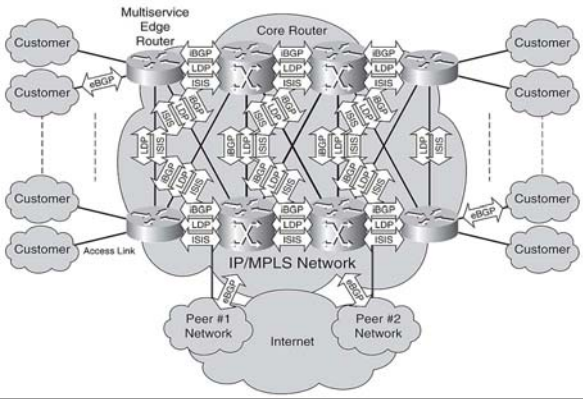
Grupe tokova saobraćaja [3]

– **Grupa korisničkog saobraćaja**
  - **Računarske mreže postoje zbog ove grupe.**
  - **Sa tačke gledišta komunikacionih uređaja u pitanju je tranzitni saobraćaj.**
  - **Saobraćaj nastaje ili je namenjen korisničkim aplikacijama na krajnjim rubovima mreže.**
  - **Funkcionalnost mreže može indirektno da zavisi.**



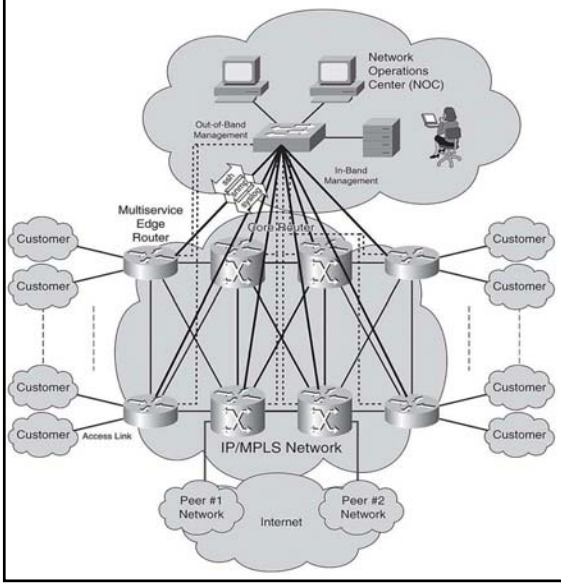
Grupe tokova saobraćaja [4]

– **Grupa kontrolnog saobraćaja**
  - **Saobraćaj na osnovu koga se automatski podešava konfiguracija komunikacionih uređaja, odnosno same mreže.**
  - **Protokoli za dinamičko rutiranje su tipičan primer iz ove grupe.**
  - **Funkcionalnost mreže je direktno zavisna od ove grupe.**



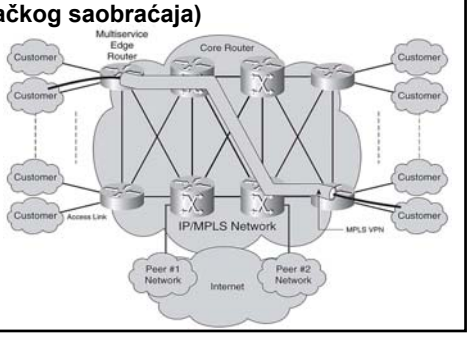
Grupe tokova saobraćaja [5]

– **Grupa upravljačkog saobraćaja**
  - **Saobraćaj iz ove grupe posledica je procesa pristupa, nadgledanja i upravljanja komunikacionim uređajima od strane administratora i specijalizovanih softvera za administraciju mreža.**
  - **Funkcionalnost mreže je direktno zavisna od ove grupe.**



Grupe tokova saobraćaja [6]

– **Grupa servisnog saobraćaja**
  - **Trenutna upotreba mreža podrazumeva postojanje velikog broja servisa koji se zasnivaju na IP saobraćaju sa različitim zahtevanim karakteristikama (različit tretman u tranzitu, kriptovanje, dodatna zaglavlja ...)**
  - **U osnovi je u pitanju korisnički saobraćaj sa potrebom za posebnim tretmanom na komunikacionim uređajima (IPSec zahteva upotrebu modula za enkripciju, QoS zahteva dodatnu obradu zaglavlja i utiče na tretman ostalih grupa saobraćaja ...).**
  - **Postojanje ove grupe saobraćaja utiče i na kompleksnost grupa kontrolnog saobraćaja i upravljačkog saobraćaja)**
  - **Funkcionalnost mreže može indirektno da zavisi, funkcionalnost pojedinih servisa direktno zavise od ove grupe.**



Grupe tokova saobraćaja [7]

– **Zavisnost funkcionalnosti mreže i servisa od grupa tokova saobraćaja**

	Korisnički	Kontrolna	Upravljačka	Servisna
Funkcionalnost mreže		*	*	
Funkcionalnost pojedinog servisa	*	*	*	*

Grupe tokova saobraćaja [8]

– **Osnovne osobine grupa tokova saobraćaja:**
  - **Grupe tokova su logičke kategorije.**
  - **Sve grupe tokova saobraćaja se pojavljuju na interfejsima komunikacionih uređaja (svi su u jednoj istoj "cevi", pogotovo sa tačke gledišta mrežnog i transportnog nivoa).**

Grupe tokova saobraćaja [9]

- Upravljane tokovima saobraćaja
  - Zašto želimo da upravljamo tokovima saobraćaja?
    - Podizanje nivoa bezbednosti mreže.
    - Podizanje nivoa bezbednosti servisa.
    - Definisanje logičkih grupa
      - » po servisima
      - » po korisnicima
      - » po organizacionoj strukturi
    - Definisanje toka saobraćaja radi ostvarivanja specijalnog tretmana, fino definisanje tokova iz servisne grupe tokova saobraćaja

Grupe tokova saobraćaja [10]

- Upravljane tokovima saobraćaja
  - Gde želimo da upravljamo (U korisničkoj ili ISP mreži)?
    - Korisnička mreža
      - » Unutrašnja mreža
      - » Granica prema ostalim mrežama
    - ISP mreža
      - » Unutrašnja mreža
      - » Granica prema ostalim mrežama

Grupe tokova saobraćaja [11]

- Upravljane tokovima saobraćaja
  - Kojim grupama tokova želimo da upravljamo?
    - Najčešće se želi upravljati tokovima saobraćaja iz korisničke i servisne grupe.
    - Mogućnost greške u konfiguraciji i nenamernog narušavanja tokova saobraćaja iz upravljačke i kontrolne grupe

Grupe tokova saobraćaja [12]

- Alati i mehanizmi za upravljanje tokovima saobraćaja
  - Filtriranje saobraćaja
    - Mrežni nivo, transportni nivo, aplikatni nivo
  - Prevodjenje IP adresa
    - Mrežni nivo
  - Socks servis
    - transportni - aplikativni nivo
  - HTTP Proxy servis
    - aplikativni nivo
  - Tuneliranje
    - prenosni nivo, mrežni nivo, transportni nivo, aplikativni nivo
  - QoS
    - prenosni nivo, mrežni nivo

Filtriranje [1]

- Filtriranje saobraćaja
  - Access Control Lists – često se vezuju za Cisco opremu
  - Iptables – Linux
  - Windows Frirewall
- Osnovna ideja je da se opiše tok saobraćaja (ili skup tokova saobraćaja) i da se definiše akcija koja se primenjuje na paketu koji pripada nekom toku i skupu tokova saobraćaja.
- Filtriranje se može vršiti na svim uređajima koji se povezuju u računarske mreže
  - komunikacioni uređaji – većinom tranzitni saobraćaj, izuzetak su kontrolna i upravljačka grupa tokova saobraćaja.
  - korisnički uređaji (radne stanice, serveri, mobilni uređaji ...)) Tokovi saobraćaja počinju ili se završavaju na njima, mada su mogući i izuzeci kod višenamenskih uređaja (npr. serveri i radne stanice konfigurisane da u mreži obavljaju funkcije rutera).

Filtriranje [2]

- Filtriranje na komunikacionim uređajima
  - Prvo se definiše lista sa pravilima.
    - Jedno pravilo se odnosi na jedan opis toka saobraćaja ili jednog skupa tokova saobraćaja. `<akcija, opis toka ili skupa tokova>`
    - Pravilo definiše akciju koja će se izvršiti ukoliko razmatrani paket pripada opisanom toku ili skupu tokova sobraćaja. Moguće akcije su “slobodan prolaz” ili “prolaz nije dozvoljen”.
      `<akcija, opis toka ili skupa tokova>`

Filtriranje [3]

- Filtriranje na komunikacionim uređajima
  - Prvo se definiše lista sa pravilima.
    - Pravila se navode sekvencijalno.
    - Poslednje pravilo u listi je podrazumevano pravilo.
    - Podrazumevano pravilo moze biti jedno od sledeća dva:
      - » Slobodan prolaz za sve, ili
      - » Prolaz nije dozvoljen nikome.
    - Opis se vrši na osnovu parametara protokola (najčešće III i IV nivoa):
      - » Protokol, IP ili ICMP (III nivo), TCP ili UDP (IV nivo)
      - » Polazne adrese ili mreže kojoj pripada polazna adresa (III nivo)
      - » Adresa odredišta ili mreže kojoj pripada adresa odredišta (III nivo)
      - » Tip i kod ICMP poruka (III nivo)
      - » Polazni port ili opseg polaznih portova (IV nivo)
      - » Odredišni port ili opseg odredišnih portova (IV nivo)
      - » Stanje TCP veze, npr. established (IV nivo)
      - » ...

Filtriranje [4]

- Filtriranje na komunikacionim uređajima
  - Lista se primenjuje na interfejsima uređaja u ulaznom ili izlaznom smeru posmatrano iz uređaja.
    - Na jednom interfejsu, u jednom smeru može se primeniti samo jedna lista.
    - Ulazni smer definiše da će svi paketi koji sa “žice” stižu na interfejs biti razmatrani paketi, a da ce svi paketi koji se šalju sa interfejsa na “žicu” proći bez razmatranja.
    - Izlazni smer definiše da će svi paketi koji sa “žice” stižu na interfejs proći bez razmatranja, a da ce svi paketi koji se šalju sa interfejsa na “žicu” biti razmatrani paketi.
    - Ako je lista primenjena u ulaznom smeru, prvo se vrši filtriranje, pa ako se paket ne odbaci, vrši se dalja obrada (rutiranje ...)
    - Ako je lista primenjena u izlaznom smeru nakon završene obrade, vrši se rutiranje, odredi se interfejs na koji se prosleđuje paket, pa se onda vrši filtriranje i ako se paket ne odbaci, prosleđuje se dalje.

Filtriranje [5]

- Filtriranje na komunikacionim uređajima
  - Lista se primenjuje na interfejsima uređaja u ulaznom ili izlaznom smeru posmatrano iz uređaja.
    - Provera pripadnosti razmatranog paketa opisanom toku ili skupu tokova vrši, za svako pravilo posebno i to redom kojim su navedena pravila u listi koja se primenjuje na datom interfejsu.
    - Čim se ustanovi pripadnost razmatranog paketa nekom toku ili skupu tokova opisanih u određenom pravilu, izvršava se definisana akcija nad razmatranim paketom i prestaje se vršiti provera pripadnosti razmatranog paketa, bez obzira da li postoji još navedenih pravila u listi.
    - U slučaju da razmatrani paket ne pripada ni jednom, u listi, opisanom toku ili skupu tokova, nad njim se izvršava akcija definisana u podrazumevanom pravilu za tu listu.

Filtriranje [6]

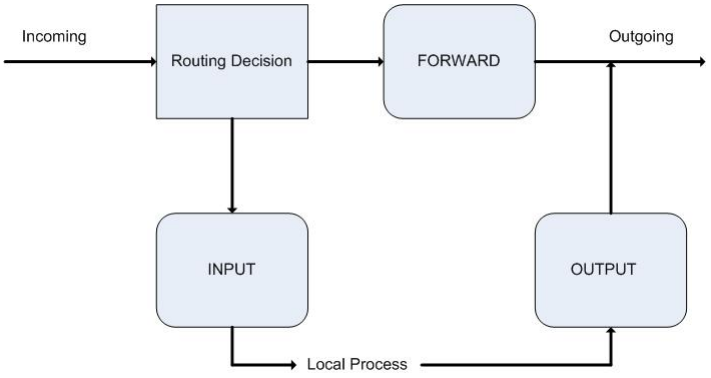
- Filtriranje na komunikacionim uređajima
  - Lista sa pravilima može da se koristi i u drugim namenama
  - Praksa je potvrdila da su ove liste dobar alat za opisivanje tokova saobraćaja.
  - U klasičnom filtriranju koristimo dve akcije “slobodan prolaz” ili “prolaz nije dozvoljen”.
  - Zašto ne bi proširili akcije i na taj način proširili mogućnosti upravljanja tokovima saobraćaja?
  - Policy Based Routing koristi `Route-map` za proširenje ovih mogućnosti uz pomoć izraza `match` *`ime_liste`* `set` *`proširena_akcija`*

Filtriranje [7]

- Filtriranje na korisničkim uređajima
  - Prvo se definiše lista sa pravilima.
    - Jedno pravilo se odnosi na jedan opis toka saobraćaja ili jednog skupa tokova saobraćaja. `<akcija, opis toka ili skupa tokova>`
    - Pravilo definiše akciju koja će se izvršiti ukoliko razmatrani paket pripada opisanom toku ili skupu tokova sobraćaja.
    - Pravila se navode sekvencijalno.
    - Poslednje pravilo u listi je podrazumevano pravilo.
    - Podrazumevano pravilo moze biti jedno od sledeća dva:
      - » Slobodan prolaz za sve, ili
      - » Prolaz nije dozvoljen nikome.
    - Opis se vrši na osnovu parametara protokola (najčešće III i IV nivoa):
      - » Protokol, IP ili ICMP (III nivo), TCP ili UDP (IV nivo)
      - » Polazne adrese ili mreže kojoj pripada polazna adresa (III nivo)
      - » Adresa odredišta ili mreže kojoj pripada adresa odredišta (III nivo)
      - » Tip i kod ICMP poruka (III nivo)
      - » Polazni port ili opseg polaznih portova (IV nivo)
      - » Odredišni port ili opseg odredišnih portova (IV nivo)
      - » Stanje TCP veze, npr. established (IV nivo)
      - » ...

Filtriranje [8]

- Filtriranje na korisničkim uređajima
  - Definisana lista se može primeniti kao:
    - INPUT pravila
    - OUTPUT pravila
    - FORWARD pravila



Filtriranje [9]

- Filtriranje - mane
  - *Stateless* filtriranje
    - Svaki razmatrani paket se posebno tretira.
    - Ne razmatraju se veze razmatranog paketa sa ranije razmatranim paketima, niti uticaj na buduće razmatrane pakete.
    - U slučaju dvosmerne komunikacije moraju se definisati posebna pravila za svaki smer. Jedno za zahtev, drugo za odgovor.
    - Primer: Ako želimo korisnicima sa "branjene" mreže da omogućimo korišćenje standardnog Internet servisa Web-a.
      - » U smeru ka javnoj mreži mora se dopustiti odredišni TCP port 80 za sve javne adrese (pravilo za zahteve).
      - » U smeru ka "branjenoj" mreži moraju se dopustiti odredišni TCP portovi u intervalu od 1024 – 65535.
      - » Otvara se mogućnost bezuslovnog pristupa navedenim TCP portovima
  - Fragmeti IP paketa mogu zaobići filtriranje
    - Zaglavlje višeg nivoa nalazi se samo u jednom fragmentu.
  - Postoje servisi koji se ne mogu obuhvatiti ovakvim filtriranjem.
  - "Statičko" nedostaje dinamika, suviše se oslanja na administratora.
  - Opis tokova sobraćaja može postati suviše složen i težak za održavanje.

Filtriranje [10]

- Filtriranje - *Stateful*
  - Neki od nedostataka mogu se ispraviti upotrebom *Stateful* filtriranja.
  - Razmatraju se:
    - Polazna i odredišna IP adresa
    - Polazni i odredišni TCP i UDP portovi
    - TCP *sequence* oznaka i *pseudo-sequence* UDP
    - Podaci iz komandnih kanala aplikativnog nivoa
  - Na osnovu ovih podataka kreira se informacija o svakoj TCP sesiji ili UDP pseudo-sesiji.
  - Sesija – Skup dva ili više tokova saobraćaja koji jednoznačno određuju komunikaciju između dve aplikacije.

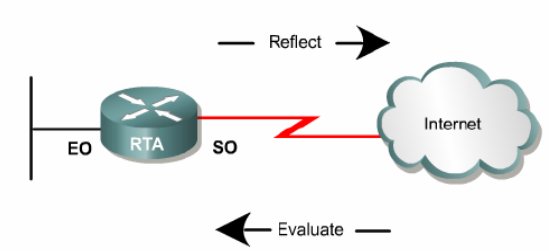
Filtriranje [11]

- **Filtriranje – *Stateful***
- **Refleksivne ACL**
- **Uvodi se dinamika. Privremeno filtriranje se aktivira u slučaju iniciranja sesije (TCP ili UDP) sa "branjene" mreže.**
- **Privremeno filtririanje predstavlja dodavnje privremenih prlavila u postojeću, na interfejsu primenjenu, listu.**
- **Na ovaj način se u ulaznom smeru ka "branjenoj" mreži dopušta samo saobraćaj koji pripada iniciranoj sesiji.**
- **Privremeno pravilo se briše iz liste po završetku sesije:**
  - TCP - odmah po detektovanju RST flega ili par sekundi po detektovanju FIN flegova ili po isticanju vremenskih ograničenja u slučaju odsustva saobraćaja.
  - UDP - po isticanju vremenskih ograničenja u slučaju odsustva saobraćaja.
- **Ograničenje – nema podršku za aplikacije koje u toku sesije barataju sa tokovima čiji se portovi menjaju (sesija je skup koji ima više od dva elementa).**
  - **FTP – komandni kanal (port 21) i kanal za transport podataka**
  - **H323**

Filtriranje [12]

- **Filtriranje – *Stateful* – refleksivne ACL**

```
interface Serial 0
description Access to the Internet via this interface
ip access-group inboundfilters in
ip access-group outboundfilters out
!
ip reflexive-list timeout 120
!
ip access-list extended outboundfilters
permit tcp any any reflect tcptraffic
!
ip access-list extended inboundfilters
permit bgp any any
permit eigrp any any
deny icmp any any
evaluate tcptraffic
```



Filtriranje [13]

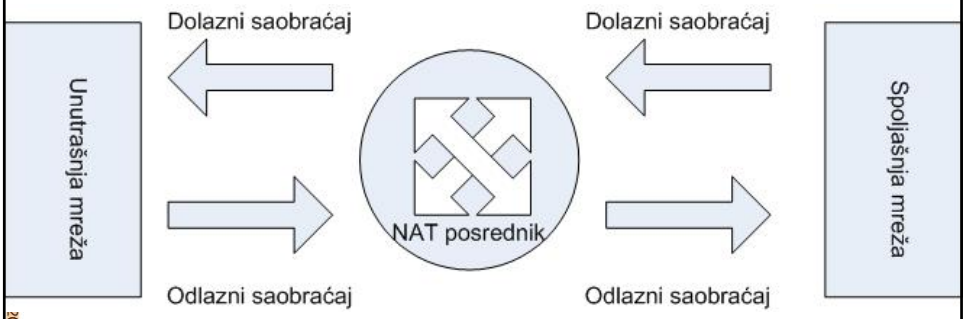
- Filtriranje – *Stateful*
- Context-Based Access Control - CBAC
- Podrška za aplikacije koje u toku sesije barataju sa tokovima čiji se portovi menjaju (sesija je skup koji ima više od dva elementa).
- Uvodi se tumačenje aplikativnog nivoa.
- Razmatra se komandni kanal aplikativnog nivoa.
- Ograničen broj aplikacija sa kojima se radi.
- Neprimerena upotreba može dovesti do pada performansi.

NAT [1]

- Zašto NAT
  - Ograničen adresni prostor IPv4. Razvoj servisa za posledicu ima primenu arhitekture Interneta u poslovnim i kućnim mrežnim okruženjima. Sve se više "troše" adrese iz javnog adresnog opsega koji je ograničen. Uptreba privatnih IP adresa (rfc 1918) omogućava primenu arhitekture Interneta u izolovanim mrežama. NAT omogućava vezu sa drugim mrežama u slučaju upotrebe privatnih adresa.
  - Povišen nivo bezbednosti mreže. NAT omogućava selektivnu komunikacija izolovane mreže sa okruženjem. (npr. može se otvoriti nova veza ka okruženju, ali iz okruženja se ne može otvoriti veza ka izolovanoj mreži).
  - Proširena mogućnost administracije mreže. Lakša rekonfiguracija adresnog opsega, preusmeravanje saobraćaja na osnovu parametara iz zaglavlja III i IV nivoa.
  - Poboljšanje karakteristika servisa (Load Sharing).

NAT [2]

- Prevođenje IP adresa - NAT (RFC 1631)
  - NAT, PAT – Cisco terminologija,
  - Masquerade, NAT– Linux
  - ????? – MS
- Posrednik koji, na spoju mreže sa okruženjem, može da menja adresna polja IP paketa i koji zna kakve su izmene izvršene.
- Vrši se preslikavanje između skupova IP adresa.



NAT [3]

- Ako se preslikavanje vrši između skupova sa privatnim IP adresama, regularno korišćenim javnim IP adresama razlikujemo:
  - Statički NAT
    - Jedna IP adresa sa unutrašnje mreže uvek se preslikava na istu IP adresu sa spoljašnje mreže i obrnuto. Omogućava dostupnost sistema u unutrašnjoj mreži za sisteme iz sopljašnje mreže.
  - Dinamički NAT
    - Skup IP adresa sa unutrašnje mreže preslikava se na skup adresa sa spoljašnje mreže
      - » Preslikavanje 1 na 1
      - » Preslikavanje “NA”

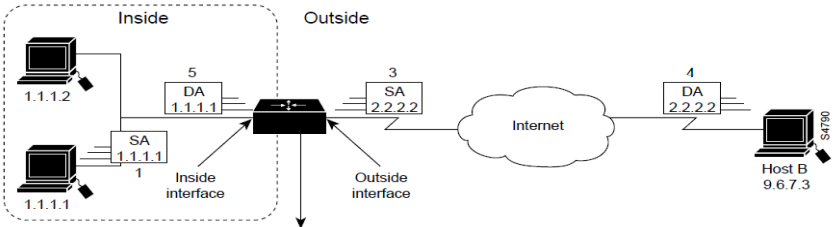
NAT [4]

– Podelu možemo izvršiti i na osnovu adresa za koje se vrši preslikavanje (zamena):
  - Source NAT – vrši se preslikavanje (zamena) polazne adrese. Uvek se vrši posle procesa rutiranja.
  - Destination NAT – vrši se preslikavanje (zamena) odredišne adrese. Uvek se vrši pre procesa rutiranja.

– Ako se preslikavanje vrši između skupova sa preklopljenim adresnim opsezima (bilo da su privatne ili javne) – vrši se istovremeno preslikavanje i polazne i odredišne.
  - Statičko
  - Dinamičko (uz upotrebu DNS-a)

NAT [5]

– Statički NAT
  - Jedna IP adresa sa unutrašnje mreže uvek se preslikava na istu IP adresu sa spoljašnje mreže i obrnuto. Omogućava dostupnost sistema u unutrašnjoj mreži za sisteme iz sopljašnje mreže.
  - Definiše se interfejs preko koga je povezana unutrašnja mreža.
  - Definiše se interfejs preko koga je povezana spoljašnja mreža.
  - Administrator formira tabelu sa parovima IP adresa (IP adresa sa unutrašnje mreže – IP adresa spoljašnje mreže)



Inside local IP address	Inside global IP address
1.1.1.2	2.2.2.3
1.1.1.1	2.2.2.2

NAT [6]

- Dinamički NAT
  - Skup IP adresa sa unutrašnje mreže preslikava se na skup adresa sa spoljašnje mreže - Preslikavanje 1 na 1
  - Definiše se interfejs preko koga je povezana unutrašnja mreža.
  - Definiše se interfejs preko koga je povezana spoljašnja mreža.
  - Definiše se skup spoljašnjih IP adresa na koje će se preslikavati unutrašnje adrese. (`IP nat pool`)
  - Definišu se unutrašnje IP adrese za koje će se vršiti preslikavanje (obično preko `access-list`).
  - Unutrašnja IP adresa se preslikava na prvu slobodnu spoljašnju adresu iz `ip nat pool`-a.
  - Tabela preslikavanja formira se dinamički i sadrži osnovni zapis:

IP adresa sa unutrašnje mreže	Polazni port (TCP/UDP)	Dodeljena IP adresa spoljašnje mreže	Dodeljeni polazni (TCP/UDP)port
1.1.1.1		2.2.2.1	
1.1.1.2		2.2.2.2	

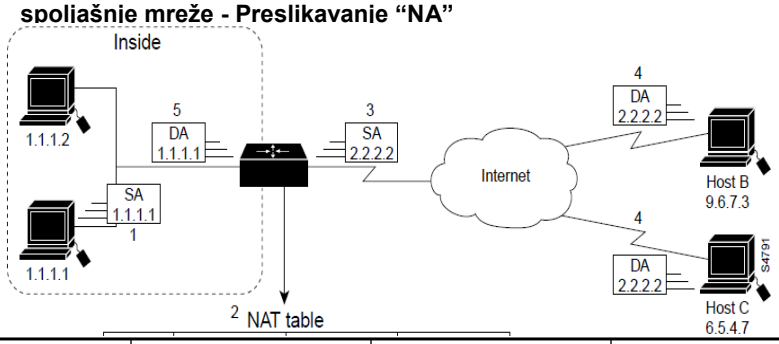
NAT [7]

- Dinamički NAT
  - Skup IP adresa sa unutrašnje mreže preslikava se na skup adresa sa spoljašnje mreže - Preslikavanje “NA”
  - Definiše se interfejs preko koga je povezana unutrašnja mreža.
  - Definiše se interfejs preko koga je povezana spoljašnja mreža.
  - Definiše se skup spoljašnjih IP adresa na koje će se preslikavati unutrašnje adrese. (`IP nat pool`)
  - Definišu se unutrašnje IP adrese za koje će se vršiti preslikavanje (obično preko `access-list`).
  - Unutrašnja IP adresa se preslikava na prvu slobodnu spoljašnju adresu iz `ip nat pool`-a.
  - Tabela preslikavanja formira se dinamički i sadrži prošireni zapis:

IP adresa sa unutrašnje mreže	Polazni port (TCP/UDP)	Dodeljena IP adresa spoljašnje mreže	Dodeljeni polazni (TCP/UDP)port
1.1.1.1	24569 (TCP)	2.2.2.2	2000 (TCP)
1.1.1.2	34567 (TCP)	2.2.2.2	2001 (TCP)

NAT [8]

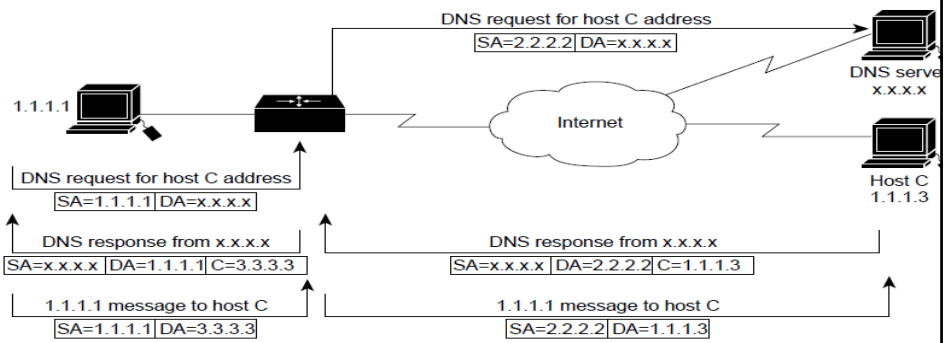
– **Dinamički NAT**
  - **Skup IP adresa sa unutrašnje mreže preslikava se na skup adresa sa spoljašnje mreže - Preslikavanje "NA"**



IP adresa sa unutrašnje mreže	Polazni port (TCP/UDP)	Dodeljena IP adresa spoljašnje mreže	Dodeljeni polazni (TCP/UDP)port
1.1.1.1	24569 (TCP)	2.2.2.2	2000 (TCP)
1.1.1.2	34567 (TCP)	2.2.2.2	2001 (TCP)

NAT [9]

- **Ako se preslikavanje vrši između skupova sa preklopljenim adresnim opsezima (bilo da su privatne ili javne) – vrši se istovremeno preslikavanje i polazne i odredišne adrese.**
  - **Statičko**
  - **Dinamičko (uz upotrebu DNS-a)**

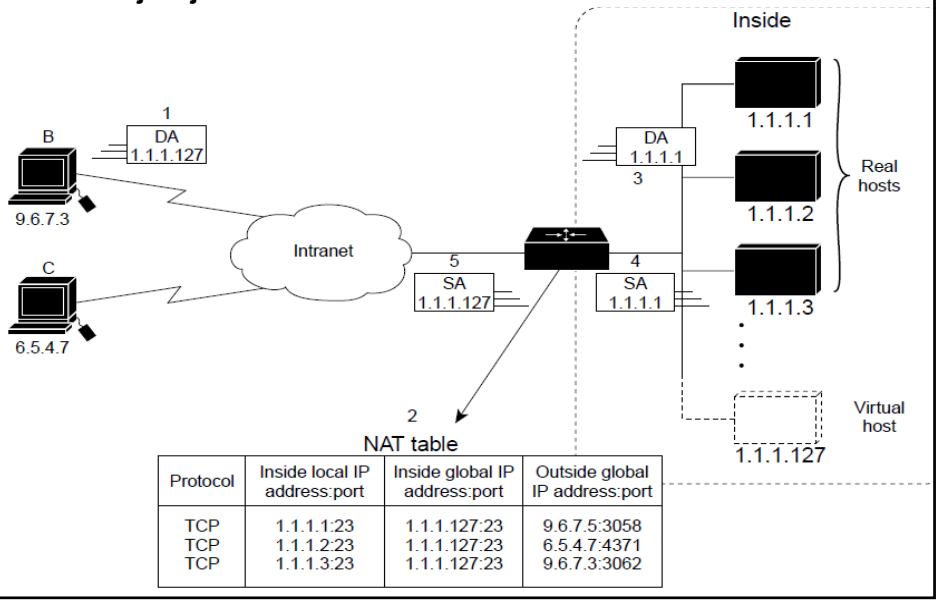


NAT table

Inside local IP address	Inside global IP address	Outside global IP address	Outside local IP address
1.1.1.1	2.2.2.2	1.1.1.3	3.3.3.3

NAT [10]

– **Poboljšanje karakteristika servisa.**



Protocol	Inside local IP address:port	Inside global IP address:port	Outside global IP address:port
TCP	1.1.1.1:23	1.1.1.127:23	9.6.7.5:3058
TCP	1.1.1.2:23	1.1.1.127:23	6.5.4.7:4371
TCP	1.1.1.3:23	1.1.1.127:23	9.6.7.3:3062

SOCKS servis [1]

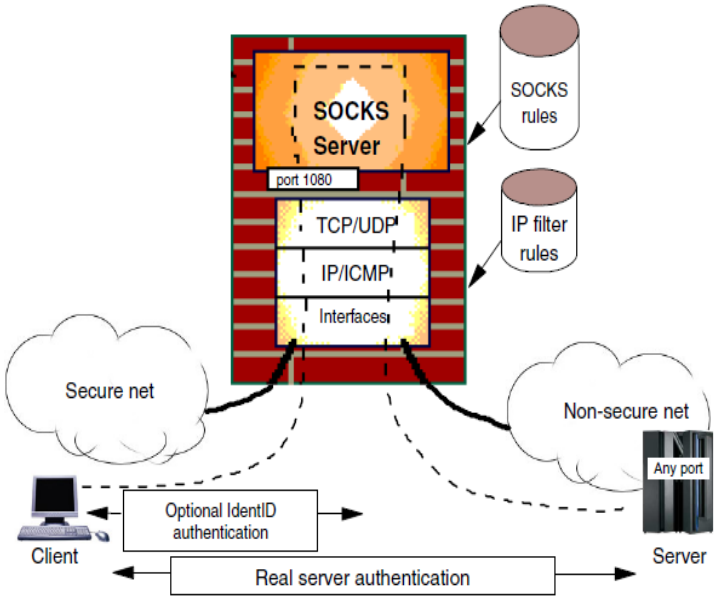
– **SOCKS servis omogućava upravljanje tokovima saobraćaja.**

– **Upravljanje se vrši između transportnog i aplikativnog nivoa. Moglo bi se reći da se upravljnanje vrši na nivou sesije OSI referentnog modela.**

– **Kako funkcioniše SOCKS servis (slučaj komunikacije u kljijent server arhitekturi):**

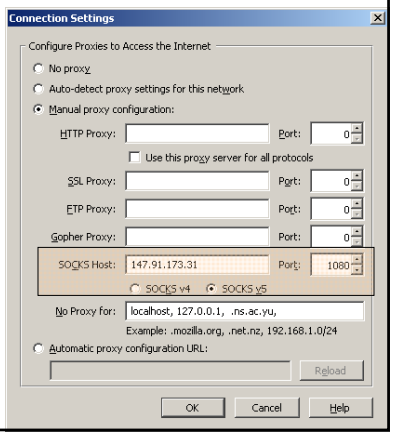
- Direktna komunikacija podrazumeva otvaranje direktne sesije između klijenta i aplikativnog servera.
- Upotrebom SOCKS servisa, klijent inicira sesiju sa SOCKS serverom;
- SOCKS server vrši autorizaciju zahteva na osnovu polazne IP adrese i autentifikacije korisnika;
- Ako je korisnika sa određene adrese autorizovan da ima pravo konekcije ka traženom aplikativnom serveru, SOCKS server inicira novu sesiju ka aplikativnom serveru iz klijentovog zahteva.
- SOCKS server ima dve otvorene sesije, ka klijentu i ka aplikativnom serveru.
- SOCKS server (putem sesije ka klijentu) prima sve podatke poslate od strane klijenta i prosleđuje ih (putem sesije ka aplikativnom serveru) do aplikativnog servera, takođe prima sve podatke od aplikativnog servera i prosleđuje ih klijentu.

SOCKS servis [2]



SOCKS servis [3]

– **SOCKS servis podrazumeva postojanje:**
  - **SOCKS servera – rezervisani TCP port 1080 za sesije ka klijentu.**
  - **SOCKS klijenta –presreće iniciranje sesije ka aplikativnom serveru i usmerava je ka Socks serveru i zadužen je za poslove vezane za autentifikaciju, autorizaciju i održavanje sesije ka Socks serveru. Realizuje se u "kodu" aplikativnih klijenata, a može biti i integrisan u implementaciju TCP/IP protokol steka.**



SOCKS servis [4]

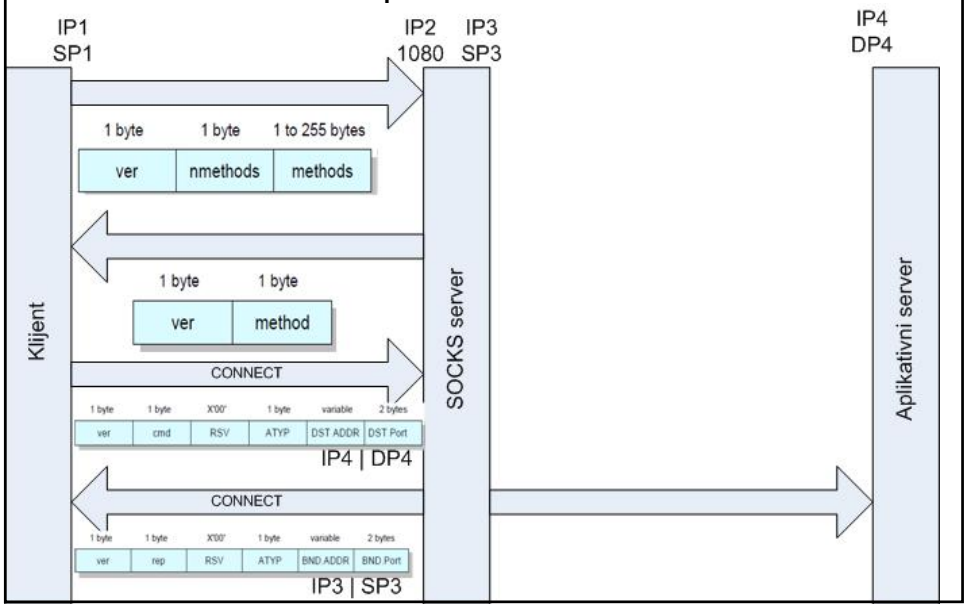
- **Prve implementacije SOCKSv4**
  - **Mane SOCKSv4 – Podržava samo TCP i loši mehanizmi za pouzdano slanje lozinke.**
- **SOCKSv5**
  - **Podrška za rad sa UDP**
  - **Znatno poboljšani mehanizmi za autentifikaciju.**

SOCKS servis [5]

- **SOCKSv5 – RFC 1928**
- **Podrška za rad:**
  - **IPv4, IPv6**
  - **TCP, UDP**
  - **Metodi autentifikacije:**
    - User name/password authentication
    - One-time password generators
    - Kerberos
    - Remote Authentication Dial-In User Services (RADIUS)
    - Password Authentication Protocol (PAP)
    - IPSec authentication method
  - **Enkripcija**
    - DES
    - 3DES
    - IPSec
  - **Tuneliranje**
    - PPTP
    - L2TP
  - Razmena ključeva
    - SKIP, ISAKMP

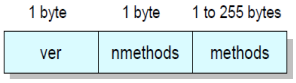
SOCKS servis [6]

– **SOCKSv5 – TCP connect procedura**



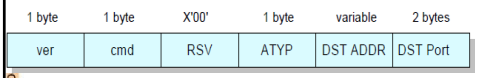
SOCKS servis [7]

– **TCP connect procedura - Inicijalizacija, autentifikacija**



– **ver – Verzija - x05 SOCKSv5**
– **nmethods – broj metoda koje slede**
– **methods – podržane metode autentifikacije i enkapsulacije (npr. kriptovanje)**
  - **X'00'** No authentication required
  - **X'01'** GSSAPI – RFC 1961
  - **X'02'** User name/password
  - **X'03' to X'7F'** IANA assigned
  - **X'80' to X'FE'** Reserved for private methods
  - **X'FF'** No acceptable methods

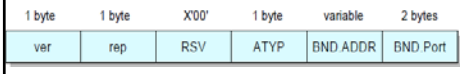
– **TCP connect procedura - Zahtev**



VER Socks protocol version. For SOCKSv5, the value is hexadecimal X'05'.
CMD SOCKS command in octets:
X'01' Connect
X'02' BIND
X'03' UDP associate
RSV Reserved for future use.
ATYP Address types in octets:
X'01' IPv4 address
X'03' Domain-name
X'04' IPv6 address
DST.ADDR Desired destination address.
DST.PORT Desired destination port in network octet order.

SOCKS servis [8]

– **TCP connect procedura - odgovor**



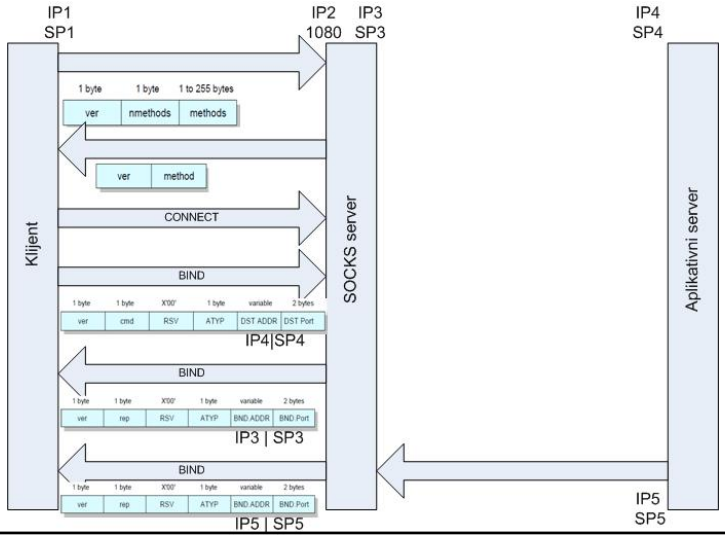
VER Socks protocol version. x05 za SOCKSv5.
REP Reply field:
- **X'00'** Succeeded
- **X'01'** General SOCKS server failure
- **X'02'** Connection not allowed by ruleset
- **X'03'** Network unreachable
- **X'04'** Host unreachable
- **X'05'** Connection refused
- **X'06'** TTL expired
- **X'07'** Command not supported
- **X'08'** Address type not supported
- **X'09' to X'FF'** Unassigned

RSV Reserved for future use.
ATYP Address types in octets:
- **X'01'** IPv4 address
- **X'03'** Domain name
- **X'04'** IPv6 address

BND.ADDR Adresa koju SOCKS server koristi kao polaznu ka javnoj mreži.
BND.PORT Port koji SOCKS server koristi kao polazni port ka aplikativnom serveru

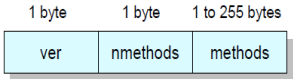
SOCKS servis [9]

– **SOCKSv5 – TCP BIND procedura – omogućava prihvatanje konekcije inicirane od strane aplikativnog servera ka klijentu (FTP npr.). Prvo se obavi CONNECT procedura.**



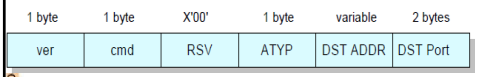
SOCKS servis [10]

– **TCP BIND procedura - Inicijalizacija, autentifikacija**



- **ver – Verzija - x05 SOCKSv5**
- **nmethods – broj metoda koje slede**
- **methods – podržane metode autentifikacije i enkapsulacije (npr. kriptovanje)**
  - **X'00'** No authentication required
  - **X'01'** GSSAPI – RFC 1961
  - **X'02'** User name/password
  - **X'03' to X'7F'** IANA assigned
  - **X'80' to X'FE'** Reserved for private methods
  - **X'FF'** No acceptable methods

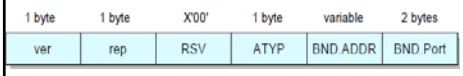
– **TCP BIND procedura - Zahtev**



VER Socks protocol version. For SOCKSv5, the value is hexadecimal X'05'.
CMD SOCKS command in octets:
X'01' Connect
X'02' BIND
X'03' UDP associate
RSV Reserved for future use.
ATYP Address types in octets:
X'01' IPv4 address
X'03' Domain-name
X'04' IPv6 address
DST.ADDR Desired destination address.
DST.PORT Desired destination port in network octet order.

SOCKS servis [11]

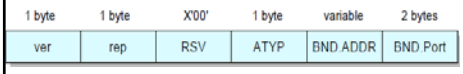
– **TCP BIND procedura – odgovora ima dva, prvi odgovor:**



VER Socks protocol version. x05 za SOCKSv5.
REP Reply field:
X'00' Succeeded
X'01' General SOCKS server failure
X'02' Connection not allowed by ruleset
X'03' Network unreachable
X'04' Host unreachable
X'05' Connection refused
X'06' TTL expired
X'07' Command not supported
X'08' Address type not supported
X'09' to X'FF' Unassigned
RSV Reserved for future use.
ATYP Address types in octets:
X'01' IPv4 address
X'03' Domain name
X'04' IPv6 address
BND.ADDR Adresa na kojoj SOCKS server “sluša” i očekuje inicijalizaciju od app. servera.
BND.PORT Port na kom SOCKS server “sluša” i očekuje inicijalizaciju od app. servera.

SOCKS servis [12]

– **TCP BIND procedura – odgovora ima dva, drugi odgovor:**



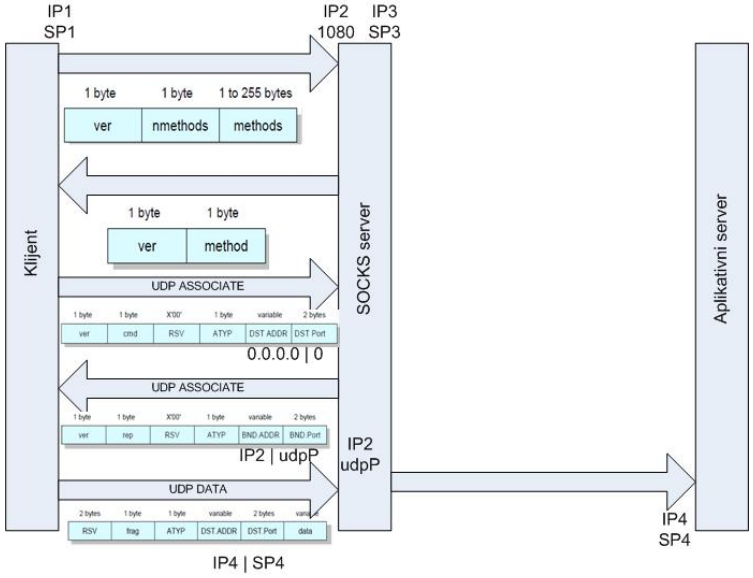
VER Socks protocol version. x05 za SOCKSv5.
REP Reply field:
- **X'00'** Succeeded
- **X'01'** General SOCKS server failure
- **X'02'** Connection not allowed by ruleset
- **X'03'** Network unreachable
- **X'04'** Host unreachable
- **X'05'** Connection refused
- **X'06'** TTL expired
- **X'07'** Command not supported
- **X'08'** Address type not supported
- **X'09' to X'FF'** Unassigned

RSV Reserved for future use.
ATYP Address types in octets:
- **X'01'** IPv4 address
- **X'03'** Domain name
- **X'04'** IPv6 address

BND.ADDR Adresa app. servera koji ostvaruje konekciju ka klijentu.
BND.PORT Polazni TCP port app. servera.

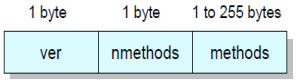
SOCKS servis [13]

– **SOCKSv5 – UDP Associate – SOCKS servis za UDP**



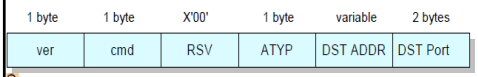
SOCKS servis [14]

– **TCP UDP Associate procedura - Inicijalizacija, autentifikacija**



– **ver – Verzija - x05 SOCKSv5**
– **nmethods – broj metoda koje slede**
– **methods – podržane metode autentifikacije i enkapsulacije (npr. kriptovanje)**
  - **X'00'** No authentication required
  - **X'01'** GSSAPI – RFC 1961
  - **X'02'** User name/password
  - **X'03' to X'7F'** IANA assigned
  - **X'80' to X'FE'** Reserved for private methods
  - **X'FF'** No acceptable methods

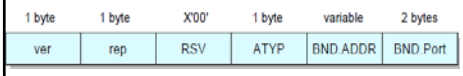
– **TCP UDP Associate - Zahtev**



VER Socks protocol version. For SOCKSv5, the value is hexadecimal X'05'.
CMD SOCKS command in octets:
X'01' Connect
X'02' BIND
X'03' UDP associate
RSV Reserved for future use.
ATYP Address types in octets:
X'01' IPv4 address
X'03' Domain-name
X'04' IPv6 address
DST.ADDR Adresa na koju klijent želi da šalje UDP (ako zna) ili sve nule ako ne zna adresu.
DST.PORT UDP port na koji klijen želi da šalje UDP (ako zna) ili sve nule ako ne zna.

SOCKS servis [15]

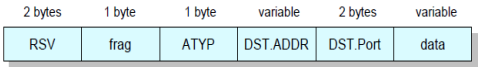
– **TCP UDP Associate – odgovor:**



VER Socks protocol version. x05 za SOCKSv5.
REP Reply field:
X'00' Succeeded
X'01' General SOCKS server failure
X'02' Connection not allowed by ruleset
X'03' Network unreachable
X'04' Host unreachable
X'05' Connection refused
X'06' TTL expired
X'07' Command not supported
X'08' Address type not supported
X'09' to X'FF' Unassigned
RSV Reserved for future use.
ATYP Address types in octets:
X'01' IPv4 address
X'03' Domain name
X'04' IPv6 address
BND.ADDR Adresa na koju klijent mora da šalje UDP segmente.
BND.PORT Port na koji klijent mora da šalje UDP segmente.

SOCKS servis [16]

- **Po slanju bilo kog odgovora, sem *x00 Succeeded*, SOCKS server mora da raskine TCP konekciju, najduže 10 sekundi po detektovanju stanja koje je generisalo odgovor.**
- **Po prijemu odgovora *x00 Succeeded* klijent:**
  - **U slučaju CONNECT i BIND procedure, počinje sa razmenom podataka sa aplikativnim serverom, indirektno preko SOCKS servera.**
  - **U slučaju UDP Associate, šalje UDP segmente na port koji je dobio od SOCKS servera u odgovoru i na svaki UDP segmet postavlja UDP request** zaglavlje. SOCKS server šalje UDP segmente na adresu i port koji su specificirani u zaglavlju



RSV Reserved for future use. All bytes are zero.
FRAG Current fragment number.
ATYP Address types in octets:
X'01' IPv4 address
X'03' Domain-name
X'04' IPv6 address
DST.ADDR Desired destination address.
DST.PORT Desired destination port in network octet order.
DATA User data.

Aplikativni PROXY servis [1]

- **Najčešća primena za HTTP na aplikativnom nivou.**
  - **SQUID cache proxy server – http://www.squid-cache.org**
  - **Microsoft Internet Security and Acceleration Server (ISA Server)**
- **Aplikativni nivo, što za posledicu ima da se posebni serveri koriste za različite protokole na aplikativnom nivou.**
- **Klijent zahtev, originalno namenjen nekom serveru, šalje proxy serveru.**
- **Proxy server je zadužen da obezbedi odgovor, lokalno iz svog keša ili direktno od servera kome je klijentov zahtev bio namenjen.**
- ***Cache* funkcionalnost.**

Aplikativni PROXY servis [2]

- Šta se dobija upotrebom HTTP proxy servisa:
  - U početku - dominantna upotreba *cache* funkcionalnosti koja je omogućivala:
    - podizanje kvaliteta HTTP servisa za krajnjeg korisnika,
    - smanjenje troškova za *bandwidth* korisnika i ISP-a
  - Dodatno, ali ne manje bitno:
    - Filtriranje (III, IV, V nivo)
    - Autentifikacija i autorizacija
    - Logovanje aktivnosti
    - Shaping
    - Odličan alat, koji zajedno sa drugim načinima upravljanja omogućava definisanje i primenu kompleksne politike upravljana tokovima saobraćaja.

Aplikativni PROXY servis [3]

- HTTP proxy serveri mogu biti povezani međusobno, što za rezultat ima optimizaciju *cache* funkcionalnosti.
- Logički gledano odnosi mogu biti:
  - *parent/child* i
  - *sibling*
- *parent/child:* U slučaju da HTTP Proxy server (*child*) nema keširan objekat koji zahteva klijent, zahtev se prosleđuje drugom HTTP Proxy serveru (*parent*). *Parent* server vraća odgovor *child* serveru, ili iz keša ako poseduje odgovor, ili sam obezbeđuje odgovor od servera kome je originalni klijentski zahtev bio namenjen.
- *sibling:* više povezanih servera na istom hijerarhijskom nivou, omogućava *load-balancing* servera. Svaki server nezavisno odlučuje šta radi za zahtevom čiji odgovor ne poseduje u svom kešu. Server nikada ne obezbeđuje drugom serveru odgovor od servera kome je originalni klijentski zahtev bio namenjen.
- Protokol koji omogućava povezivanje HTTP proxy servera je ICPv2, definisan u RFC 2186 i RFC 2187.

Aplikativni PROXY servis [4]

- *Transparent Proxying*
- Slučaj kada se HTTP konekcija od klijenta ka serveru preusmeri (bez znanja klijenta) ka HTTP proxy serveru.
- Šta se na ovaj način dobija:
  - Nema nikakve dodatne konfiguracije na strani klijenta
  - Bolji manevarski prostor za reakciju u slučaju problema sa funkcionalnošću HTTP proxy servisa.
- Šta se gubi:
  - Zahteva NAT (konfiguracija složenija, samim tim i verovatnoća za grešku u konfiguraciji cele mreže raste)
  - Mogući problemi sa *Path MTU Dicovery* mehanizmom
  - Problem u radu sa starijim verzijama HTTP klijenata
  - Gubimo funkcionalnost autentifikacije i autorizacije na Proxy serveru
  - Podrška samo za HTTP (SSL, FTP i drugi protokoli nemaju podršku)
  - ...

Aplikativni PROXY servis [5]

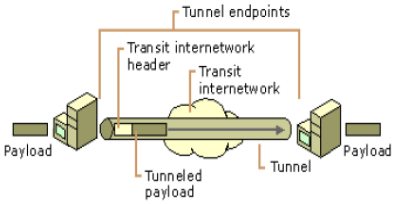
- *Reverse Proxy Mode - httpd-accelerator*
- Svi HTTP zahtevi ka HTTP serveru se završavaju na Proxy serveru, koji po potrebi kontaktira stvarni HTTP server (u slučaju da ne poseduje kopiju odgovora).
- Moguće konfiguracije:
  - Proxy server u javnoj mreži, HTTP server u privatnoj “bezbednoj”.
  - Proxy server prima HTTP zahteve za više različitih HTTP servera.
  - *Load Balancing*.
  - Više Proxy servera povezanih preko ICP, primaju zahteve za jedan HTTP server.

Tuneliranje [1]

- U slučaju kada se osnovna jedinica prenosa nekog protokola enkapsulira u osnovnu jedinicu prenosa protokola koji je prvi niži po referentnom modelu komunikacije, govorimo o klasičnoj (regularnoj) enkapsulaciji.
- "spoljašnji" protokol je prvi niži u odnosu na "unutrašnji" protokol.

- Drugačije kombinacije "spoljašnjeg" i "unutrašnjeg" protokola u zavisnosti od njihove pozicije u referentnom modelu možemo nazvati tuneliranje.

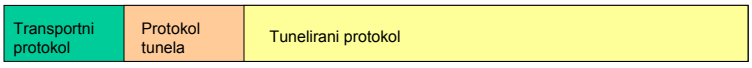
- Logical path through which encapsulated packets travel



Tuneliranje [2]

Arhitektura:

- Transportni protokol – protokol transportne mreže.
- Protokol tunela – definiše, kreira, raskida, upravlja tunelom.
- Tunelirani protokol – originalne jedinice prenosa koje se prenose kroz tunel.



Tuneliranje [3]

Problemi tuneliranja:

- **Tuneliranje za posledicu ima povećanje veličine osnovne jedinice prenosa:**
  - **Što može dovesti do fragmentacije koja je loša po pitanu end-to-end performansi.**
  - **Krajnje tačke, koje učestvuju u komunikaciji, nisu upoznate sa činjenicom da tunel snižava MTU.**
- **Tuneliranje zahteva dodatne aktivnosti u procesiranju osnovnih jedinica prenosa.**
- **Može dovesti do problema u radu između različitih implementacija.**

Tuneliranje [4]

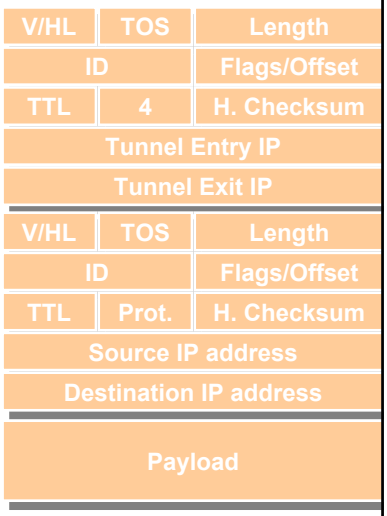
- **Neke upotrebe tuneliranja:**
  - **Podrška za rad sa protokolima koje tranzitna mreža ne podržava:**
    - **Ruteri koji podržavaju tunelirani protokol, koriste tunele da "premoste" rutere koji ih ne podržavaju (povezivanje dve IPX mreže preko IP infrastrukture)**
    - **IPv6** "6bone", **multikast** "Mbone"
  - **Forsiranje paketa ka odredištu koje nije isto sa definisanim odredištem u zaglavlju paketu:**
    - **Prenos paketa sa "neregularnim" adresama kroz mrežu (tunelirani protokol i tranzitni protokol mogu biti isti).**
    - ***mobile IP***
  - **VPN**
  - **Tuneliranje otvara novu dimenziju u mrežama.**

Tuneliranje [5]

- Tuneliranje i nivoi protokola referentnog modela.
- Tuneliranje uključuje različite kombinacije nivoa protokola i samim tim se narušava koncept referentnog modela, ili se drugačije može reći – dodaje se nova dimenzija u referentni model.
- Različiti pogledi:
  - Ako gledamo sa tačke tuneliranog protokola – L2, L3, aplikativni
    - PPTP i L2TP tuneliranje spada u L2 tuneliranje
  - Ako gledamo sa tačke transportnog protokola – L3, aplikativni
    - PPTP i L2TP tuneliranje spada u L3 tuneliranje
- Postavlja se pitanje gde tunelirati (sa tačke gledišta transportnog protokola)
- 3 nivo je razuman
  - dovoljno je nisko da je transparentan za aplikacije i servise.
  - dovoljno je visoko za obezbeđenje komunikacije i upravljanje njome u okviru transportne mreže (omogućava end-to-end tuneliranje).

Tuneliranje [6]

- IP – IP tunel
- Opisan u RFC 1993
- Polazna i odredišna adresa - krajevi tunela
- *Protocol id* = 4
- Određena polja se kopiraju iz originalnog zaglavlja (TOS, neki flegovi ...)
- Originalno zaglavlje nema promena (sem TTL)
- Forsiramo odredište, prenos paketa sa privatnim adresama kroz javnu infrastrukturu

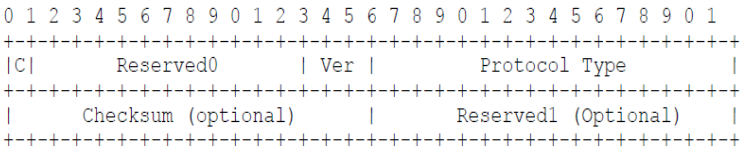


Tuneliranje [7]

- Generic Routing Encapsulation – GRE
- RFC 1701
- RFC 2784
- Pokusaj da se napravi generalno rešenje koje neće zavisiti od specifičnosti tuneliranog protokola i transportnog protokola.
- Za transportni protokol se najčešće koristi IP, oznaka za GRE u IP paketu je 47

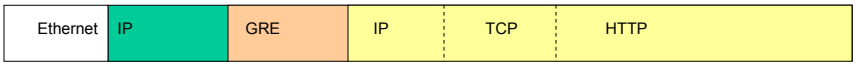
Tuneliranje [8]

- Generic Routing Encapsulation – GRE – RFC 2784
- C – označava postojanje opcionih polja
- Reserved0 – Za buduće namene
- Protocol Type – oznaka protokola enkapsuliranog u GRE u istom formatu kako se označava i kod Ethernet-a (oznaka za IP je 0800)
- Checksum – kontrolna suma zaglavlja i osnovne jedinice prenosa koja je enkapsulirana
- Reserved1 – Za buduće namene



Tuneliranje [9]

- Generic Routing Encapsulation – GRE – RFC 2784
- C – označava postojanje opcionih polja
- Reserved0 – Za buduće namene
- Protocol Type – oznaka protokola enkapsuliranog u GRE u istom formatu kako se označava i kod Ethernet-a
- Checksum – kontrolna suma zaglavlja i osnovne jedinice prenosa koja je enkapsulirana
- Reserved1 – Za buduće namene



Tuneliranje [10]

- Generic Routing Encapsulation – GRE
- Nema podršku za primenu mehanizama zaštite (autentifikaciju, integritet, poverljivost, neporecivost)
- Može da se koristi sa IPSec
- Koristi se za formiranje LAN – LAN tunela
- Podrška sa *multicast*
- RFC 2784 GREv0
- PPTP proširenje - GREv1

Tuneliranje [11]

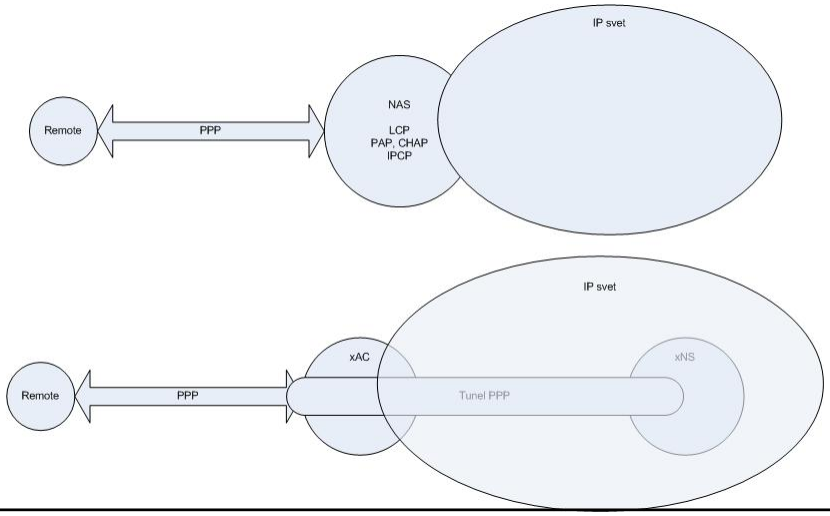
- PPP - RFC 1661
- PPP omogućava prenos različitih protokola III nivoa kroz *point-to-point* veze.
- Najčešći scenario:
  - korisnik ostvari fizičku vezu sa Network Access Server-om (NAS) upotrebom neke od komunikacionih tehnologija javne telekomunikacione mreže (*dialup POTS, ISDN, ADSL, Frame Relay, ...*) i koristi PPP za prenos IP-a.
  - PPP je tunel protokol za prenos IP preko javne klasične telekomunikacione mreže.
  - U ovom slučaju se poklapaju tačke terminacije fizičke veze i PPP sesije.

Tuneliranje [12]

- PPP sesija omogućava:
  - Upravljanje na osnovu stanja veze (detekcija pada kvaliteta, prekid veze, reuspostavljanje veze ...)
  - Enkapsulaciju različitih protokola sa III nivoa
  - Različite metode autentifikacije (PAP, CHAP)
  - Razmenu parametara protokola III nivoa vezanih za automatsku konfiguraciju interfejsa
  - ...

Tuneliranje [13]

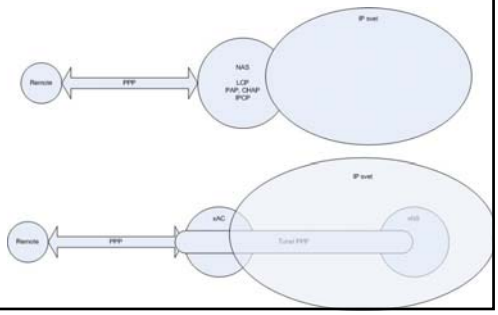
– **Analizom mogućnosti koje PPP pruža postavlja se potreba za razdvajanje tačke na kojoj se terminira fizička veza i tačke na kojoj se terminira PPP sesija.**



Tuneliranje [13]

– **Funkcije NAS-a:**
  1. **Direktni interfejs (fizički) namenjen za podršku komunikacionim tehnologijama telekomunikacionog provajdera čije usluge se koriste (POST, ISDN, FrameRelay, digitalne iznajmljene veze ...)**
  2. **Logička terminacija PPP LCP**
  3. **Autentifikacija**
  4. **Agregacija linkova (PPP multilink)**
  5. **Logička terminacija NCP (*network control* protokola)**
  6. **Funkcije rutiranja između interfejsa NAS-a**

– **xAC – funkcije 1, 2 i ređe 3**
– **xNS – funkcije 3, 4, 5 i 6**

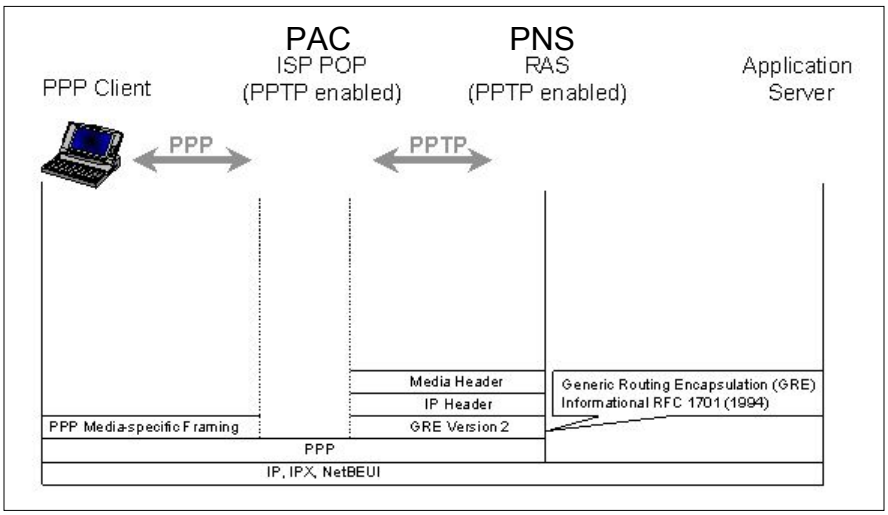


Tuneliranje [14]

- Point to Point Tunneling Protocol PPTP – RFC 2637
- Ekstenzija PPP
- Omogućava prenos PPP frejmova preko IP mreže
  - Tunelirani protokol – PPP
  - Protokol tunela – GRE
  - Transportni protokol – IP

Tuneliranje [15]

- PPTP – RFC 2637

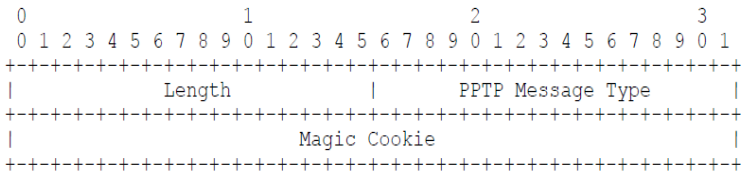


Tuneliranje [16]

- Point to Point Tunneling Protocol PPTP – RFC 2637
- Jednostavan za upotrebu – pogotovo korisnički deo
- Microsoft presudno utiče na rasprostranjenost (autori RFC-a delom su iz Microsofta)
- PPTP formira tunel između PAC (PPTP-Access-Concentrator) i PNS (PPTP-Network-Server)
- Ima mogućnost tuneliranja više PPP sesija kroz jedan tunel
- PPTP sesija je skup više od dva toka saobraćaja
  - Upravljački kanal – kreiranje, upravljanje i raskidanje tunela
  - Kanal za prenos podataka – tunel

Tuneliranje [17]

- Point to Point Tunneling Protocol PPTP – RFC 2637
- Upravljački kanal
  - Formira se TCP sesija (rezervisani TCP port 1723)
  - U cilju dogovaranja parametara za uspostavu tunela ili raskid tunela razmenjuje se set poruka definisanih standardom
  - Sve poruke moraju imati sledeća polja:
    - Lenght – dužina poruke
    - PPTP Message Type – kontrolna ili upravljačka poruka
      - » Trenutno ne postoje definicije za upravljačke poruke
    - "Magic Cookie" – uvek isti 1A2B3C4D – osnovna provera ispravnosti formiranja zaglavlja – u slučaju da vrednost ne odgovara obavezno se raskida sesija

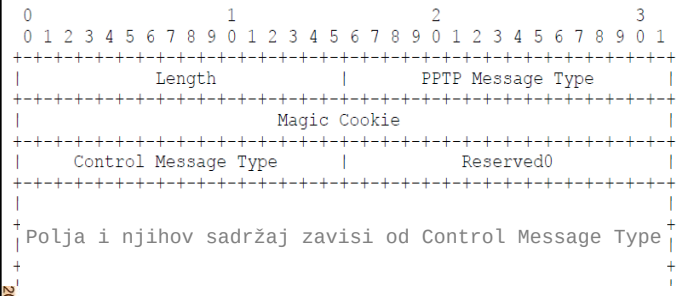


Tuneliranje [18]

- Point to Point Tunneling Protocol PPTP – RFC 2637
- Upravljački kanal – kontrolne poruke

```
(Control Connection Management)
Start-Control-Connection-Request - 1
Start-Control-Connection-Reply - 2
Stop-Control-Connection-Request - 3
Stop-Control-Connection-Reply - 4
Echo-Request  - 5
Echo-Reply  - 6
```

```
(Call Management)
Outgoing-Call-Request - 7
Outgoing-Call-Reply - 8
Incoming-Call-Request - 9
Incoming-Call-Reply - 10
Incoming-Call-Connected - 11
Call-Clear-Request - 12
Call-Disconnect-Notify - 13
```

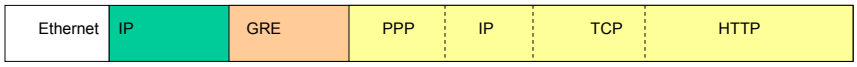


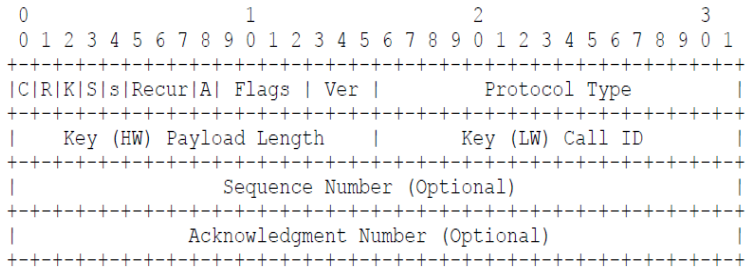

```
(Error Reporting)
WAN-Error-Notify – 14

(PPP Session Control)
Set-Link-Info  -15
```


Tuneliranje [19]

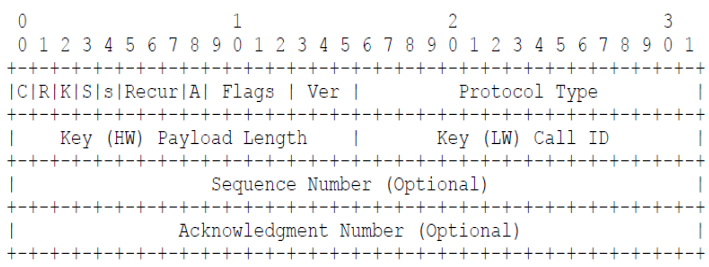
- Point to Point Tunneling Protocol PPTP – RFC 2637
- Kanal za prenos podataka - Tunel
  - PPP frejm se enkapsulira u GREv1 jedinicu prenosa
  - GREv1 se enkapsulira u IP





Tuneliranje [20]

- C - (Bit 0) Checksum Present. Set to zero (0).
- R - (Bit 1) Routing Present. Set to zero (0).
- K - (Bit 2) Key Present. Set to one (1).
- S - (Bit 3) Sequence Number Present.
- s - (Bit 4) Strict source route present. Set to zero (0).
- Recur - (Bits 5-7) Recursion control. Set to zero (0).
- A - (Bit 8) Acknowledgment sequence number present.
- Flags - (Bits 9-12) Must be set to zero (0).
- Ver - (Bits 13-15) Must contain 1 (enhanced GRE).
- Protocol Type - Set to hex 880B [8].
- Key - Use of the Key field is up to the implementation. PPTP uses it as follows:
  - Payload Length - (High 2 octets of Key) Size of the payload,
  - Call ID - (Low 2 octets) Contains the Peer's Call ID
- Sequence Number - Contains the sequence number of the payload.
- Acknowledgment Number - Contains the sequence number of the highest numbered GRE packet received

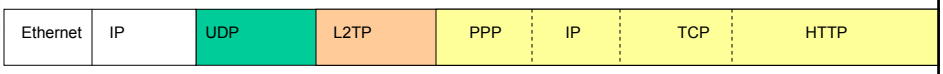


Tuneliranje [21]

- **Point to Point Tunneling Protocol PPTP – RFC 2637**
- **PPTP specifikacija ne propisuje metode autentifikacije i kriptovanja**
- **Dopušteno je da se klijent i server dogovore o tipu autentifikacije i kriptovanja (koriste se PPP prošireni mehanizmi dogovaranja)**
- **Najčešće implementacije:**
  - **Autentifikacija:**
    - Clear password: client authenticates to the server
    - Hashed password: client authenticates to the server
    - Challenge-response: client and server authenticate each other
  - **Kriptovanje:**
    - Microsoft Point-to-Point Encryption (MPPE) -> stream cipher using RSA RC-4

Tuneliranje [22]

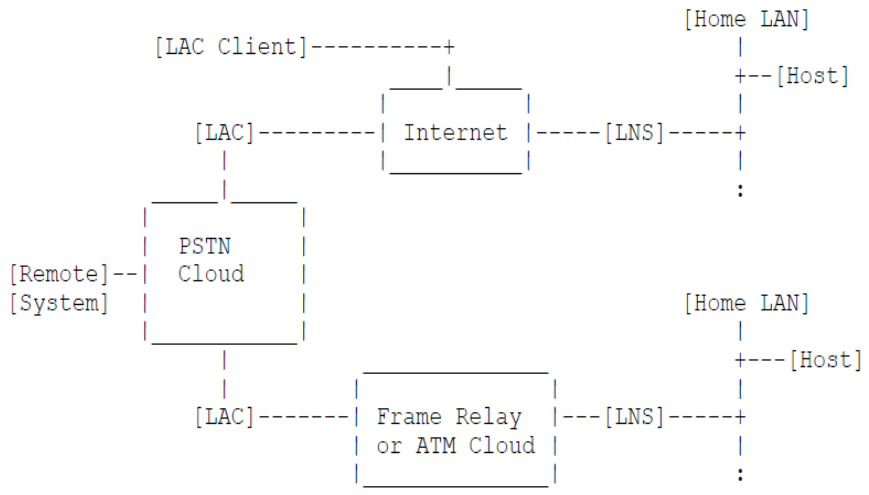
- Layer Two Tunneling Protocol – L2TP – RFC 2661
- Omogućava prenos PPP frejmova preko IP, Frame Relay, ATM i drugih mreža
  - Tunelirani protokol – PPP
  - Protokol tunela – L2TP
  - Transportni protokol – UDP/IP
- Koristi se UDP port 1701
- L2TP formira tunel između LAC (L2TP-Access-Concentrator) i LNS (L2TP-Network-Server)
- Ima mogućnost kreiranja više tunela sa više PPP sesija kroz jedan logički tunel



Tuneliranje [23]

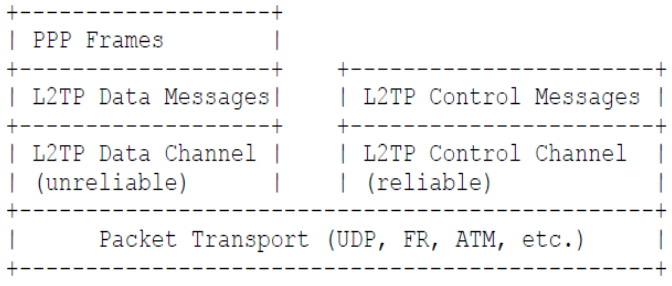
- Layer Two Tunneling Protocol – L2TP – RFC 2661

L2TP scenario:



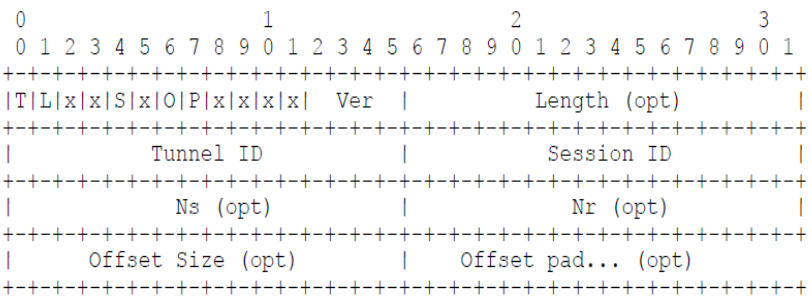
Tuneliranje [24]

- Layer Two Tunneling Protocol – L2TP – RFC 2661
- L2TP tunel je sesija sa dva toka saobraćaja, ne postoje odvojeni upravljački kanal i kanal tunela.
- Razlikuju se tipovi poruka:
  - Kontrolne poruke
    - uspostava, upravljanje i raskid tunela
    - imaju mehanizam koji obezbeđuje garanciju isporuke
  - Poruke za prenos podataka
    - Ne postoji mehanizam koji obezbeđuje garanciju isporuke



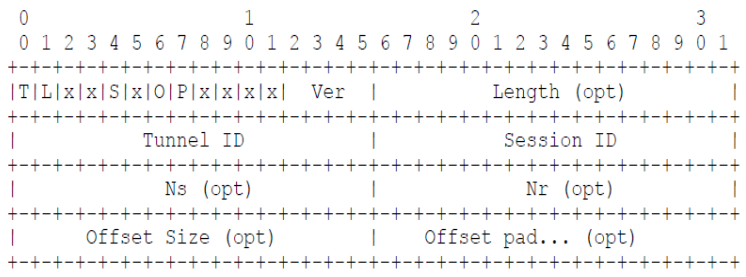
Tuneliranje [25]

- Layer Two Tunneling Protocol – L2TP – RFC 2661
- L2TP zaglavlje – i za kontrolne i za upravljačke poruke
- Razlikuju se u opcionim poljima



Tuneliranje [26]

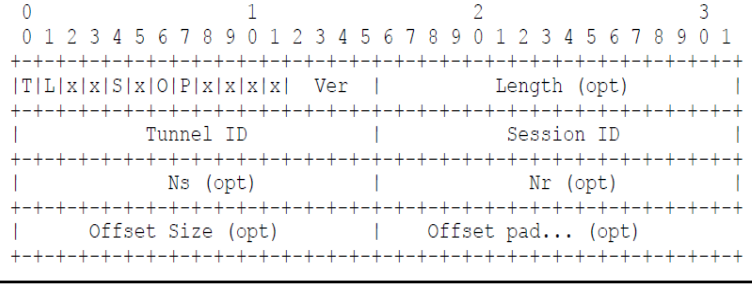
- Type (T) bit - type of message. 0 data message, 1 control message.
- Length (L), ukazuje na prisutnost Length polja. Uvek 1 za kontrolne poruke.
- x bits – za buduće namene, moraju biti 0
- Sequence (S) – ukazuju na prisutnost Ns i Nr polja. Uvek 1 za kontrolne poruke.
- Offset (O) – ukazuju na prisutnost Offset Size polja. Uvek 0 za kontrolne poruke.
- Priority (P) – definiše prioritet. Uvek 0 za kontrolne poruke.
- Ver - verzija L2TP data message header – L2TP koristi oznaku 2, L2F koristi oznaku 1.
- Length – totalna dužina poruke u oktetima



Tuneliranje [27]

- Tunnel ID - oznaka tunela (veza izmedju kontrolnih poruka i poruka za prenos podataka) Lokalnog tipa, svaka strana postavlja svoj. Tunnel ID se razmenjuje tokom uspostave tunela

- Session ID - oznaka sesije unutar tunela. Lokalnog tipa, Session ID se razmenjuje tokom uspostave sesije.
- Ns - sequence number
- Nr - očekivani broj kontrolne poruke za prijem – mehanizam garancije isporuke
- Offset Size – ukazuje na kraj zaglavlja, tačnije na kraj opcionog polja Offset pad



Tuneliranje [28]

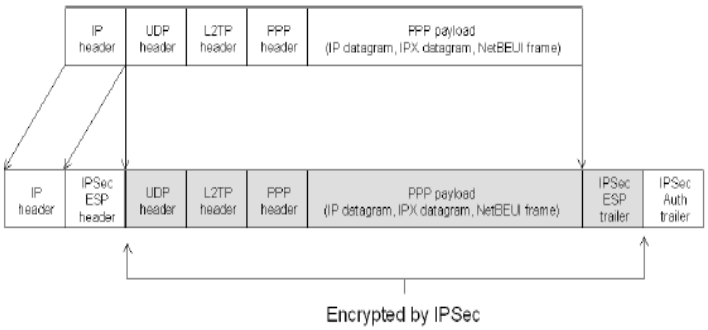
- Layer Two Tunneling Protocol – L2TP – RFC 2661
- Kontrolne poruke
  - uspostava, upravljanje i raskid tunela
  - imaju mehanizam koji obezbeđuje garanciju isporuke
- Tipovi kontrolnih poruka
  - Upravljanje uspostavom i raskidom tunela
  - Upravljanje pozivima
  - Izveštaj o greškama
  - Upravljanje PPP sesijom

Tuneliranje [29]

- Layer Two Tunneling Protocol – L2TP – RFC 2661
- Poruke za prenos podataka
  - Enkapsuliraju PPP frejmove
  - Nema garancije isporuke (ne postoji retransmisija u slučaju gubitka paketa)
  - Opciona numeracija paketa (Sequence numbers)
    - najčešće za detekciju gubitka paketa
  - Ne postoji mehanizam uz pomoć koga se može izbeći fragmentacija

Tuneliranje [30]

- Layer Two Tunneling Protocol – L2TP – RFC 2661
- End-toEnd sa visokim nivoom zaštite postiže se u kombinaciji sa IPSec – om

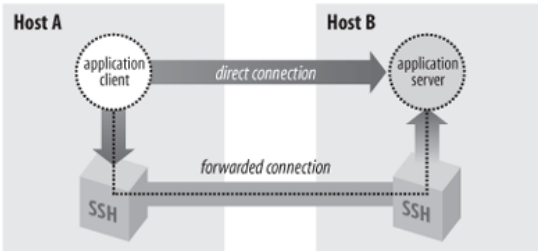


Tuneliranje [31]

- SSH Tuneliranje
- Koristi se za kriptovanje TCP sesija u kojima se prenose nekriptovani aplikativni podaci.
- port forwarding

```
ssh –L lport:rhost:rport rhost
```

- Tunelirani protokol – TCP
- Tunel protokol – SSH
- Transportni protokol - TCP



Tuneliranje [32]

SSL

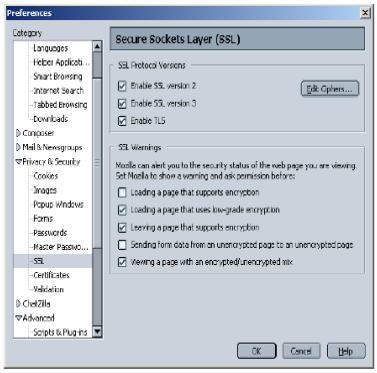
- komunikacioni protokol razvijen sa ciljem da podrži
  - kriptografsku bezbednost
  - interoperabilnost
    - implementacije različitih proizvođača
  - proširivost
    - različitim kriptografskim algoritmima
  - relativnu efikasnost
    - optimizuje zauzeće procesora i mrežni protok
    - keširanjem komunikacionih parametara za uspostavljene veze

- SSL = Secure Sockets Layer
  - prozvod Netscape-a
  - SSL v2: prva prihvaćena verzija
    - imala je bezbednosnih nedostataka
  - SSL v3: de facto standard od 1996.
    - nikad nije zvanično standardizovan

Tuneliranje [33]

TLS

- TLS = Transport Layer Security
  - standardizacija SSL protokola u okviru IETF
  - RFC 2246
  - podrška u savremenim browserima



Tuneliranje [34]

TLS

- dva sloja
  - Record Protocol
  - Handshake Protocol / Alert Protocol / Change Cipher Spec Protocol
- TLS Record Protocol
  - oslanja se na TCP i daje podršku za protokole višeg nivoa
  - koristi simetrične algoritme za šifrovanje
  - prenos poruka obuhvata i proveru integriteta pomoću hash funkcija
- TLS Handshake Protocol
  - autentifikacija klijenta i servera i dogovor oko korišćenih algoritama i ključeva
  - provera identiteta pomoću asimetričnih algoritama
  - dogovor oko session ključa je siguran od prisluškivanja
  - postupak dogovaranja obezbeđuje detekciju man-in-the-middle napada

Tuneliranje [35]

- **SSL/TLS Tuneliranje**
- **Jedna od metoda je upotreba *port-forwarding* kao kod SSH tuneliranja**
- **Upotreba SSL/TLS u kombinaciji sa tunelima između virtuelnih mrežnih interfejsa – često se naziva SSL/TLS tuneliranje**

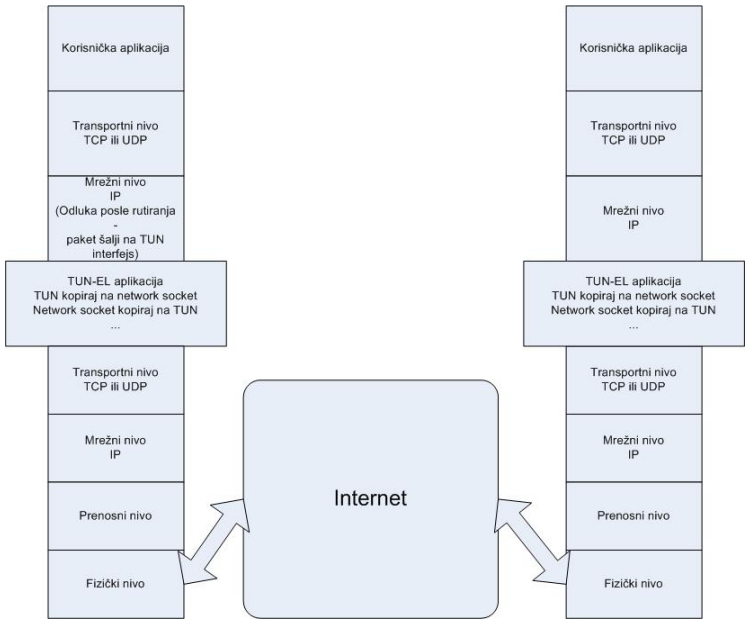
Tuneliranje [36]

- Virtuelni mrežni interfejsi – TUN & TAP
- Posmatramo ih kao Point-to-Point ili Ethernet interfejse, koji umesto da primaju pakete sa "žice", pakete primaju od korisničkih aplikacija, takođe. umesto da pakete šalju na "žicu", pakete prosleđuju korisničkoj aplikaciji.
- Korisnički program pristupa TUN & TAP interfejsima kao klasičnom fajlu i može da čita, iz njih, i zapisuje, u njih, pakete.
- TUN – Point-to-Point interfejs
- TAP – Ethernet interfejs
- TUN & TAP interfejs, sa stanovišta rutiranja i filtriranja saobraćaja, imaju isti tretman kao i klasični interfejsi.

Tuneliranje [37]

- Virtuelni mrežni interfejsi – TUN & TAP
- Jednostavan tunel:
  - TUN-EL aplikacija koja bite sa TUN-a kopira na *network socket* i bite sa *network socketa* kopira na TUN. Sve dodatne funkcije su dozvoljene (nalazimo se na aplikativnom nivou :)
  - Dve tačke koje koriste TUN-EL , uz dogovor o IP adresama i portovima na kojima TUN-EL sluša i na koje TUN-EL šalje, mogu kreirati tunel sa sledećim osobinama:
    - Transportni protokol: TCP ili UDP
    - Protokol tunela: aplikacija TUN-EL
    - Tunelirani protokol: IP

Tuneliranje [38]



VPN [1]

- **VPN – Virtual Private Network**
- **VPN – jedna od definicija:**
  - **Privatna mreža za prenos podataka koja se realizuje preko javne infrastrukture upotrebom tuneliranja i mehanizama zaštite podataka.**
- **VPN se koristi za realizaciju WAI (wide area intranet) i za realizaciju extranet-a.**

VPN [2]

VPN nije novost

- Za realizaciju WAI i extranet-a do sada su se koristile tradicionalne metode:
  - Postavljanje privatne komunikacione infrastrukture
  - Iznajmljivanje komunikacione infrastrukture, odnosno iznajmljivanje prenosnih puteva, od komunikacionih provajdera, na ekskluzivno korišćenje (iznajmljene linije, Frame Relay ...)
  - Kombinacija gore navedenih metoda
- Odnos korisnika prema upotrebi iznajmljene infrastrukture je isti kao prema privatnoj infrastrukturi.
- Korisniku, provajder, garantuje da niko drugi nema prava na upotrebu iznajmljene infrastrukture.
- Korisniku, provajder, garantuje za zadovoljenje očekivanih karakteristika komunikacione infrastrukture
- Korisniku je omogućeno da sam kreira logičku arhitekturu i politiku zaštite
- Cena iznajmljivanja komunikacione infrastrukture je visoka i može dodatno da raste:
  - sa porastom geografske udaljenosti tačaka koje se povezuju
  - sa porastom kapaciteta
  - sa iznajmljivanjem infrastrukture od dva ili više provajdera (nema globalnog provajdera)
  - ...

VPN [3]

- Internet:
  - Javna infrastruktura
  - Briše se pojam zavisnosti od geografske udaljenosti, cena se vezuje za najbližu pristupnu tačku – gotovo uvek u "lokalu"
  - Viši kapaciteti, viša cena – ali radimo uvek u "lokalu"
- Odlična alternativa klasičnim komunikacionim sistemima za javnu infrastrukturu nad kojom gradimo VPN
- Teži se da se postigne isti nivo servisa koji je dostignut upotrebom klasičnih komunikacionih sistema.

VPN [4]

- **Tipovi VPN-a:**
  - **Trusted VPN – ekskluzivnost, garancija karakteristika (QoS). Realizuju se putem unapred odredjenih putanja sa definisanim karakteristikama kroz mrežu jednog ili više ugovorom vezanih provajdera. Provajder/i garantuju putanje i njihove karakteristike. Servis koji se pruža od strane provajdera i potpuno je transparentan u odnosu na korisnika.**
  - **Secure VPN – koristi se kriptozaštita da bi se ostvarila: autentifikacija, integritet, poverljivost, neporecivost. Nema zavisnosti od provajdera. Omogućava se pristup klasifikovanih korisnika – klasifikovanim privatnim servisima sa bilo koje tačke Interneta.**
  - **Hybrid VPN – omogućava se paralelno korišćenje oba tipa VPN, u potpunosti ili delimično.**

VPN [5]

- **Tehnologije za realizaciju VPN-a (po preporuci VPN Consortiuma):**
  - **Trusted VPN:**
    - **ATM**
    - **Frame Relay**
    - **L2 MPLS**
    - **L3 MPLS/BGP**
  - **Secure VPN:**
    - **IPsec**
    - **IPsec/GRE**
    - **IPsec/L2TP**
    - **SSL/TLS**
  - **Hybrid VPN – bilo koja kombinacija gore navedenih**

VPN [6]

- **Manje službena, ali česta podela:**
  - **Site-to-site VPN:**
    - **IPsec**
    - **IPsec/GRE**
    - **MPLS**
    - **SSL/TLS**
  - **DialUp VPN (Remote access VPN):**
    - **IPsec/L2TP**
    - **PPTP**
    - **SSL/TLS**

IPSec overview

IPSec is a framework of security protocols and algorithms used to secure data at the network layer.

Prior to the IPSec standard, Cisco implemented its proprietary Cisco Encryption Technology (CET) to provide protection at the packet level.

RFC 2401 describes the general framework for this architecture. The framework provides data integrity, authentication, and confidentiality, as well as security association and key management.

IPSec consists of two protocols.

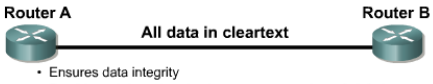
IPSec Framework	Choice 1	Choice 2
IPSec protocol	ESP	ESP +AH
Encryption	DES	3DES
Authentication	MD5	SHA
Diffie -Hellman	DH1	DH2

IPSec overview

The first protocol is Encapsulating Security Payload (ESP). It encapsulates the data, but does not provide protection to the outer headers. ESP encrypts the payload for data confidentiality.

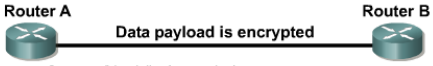
The second protocol is Authentication Header (AH). The AH protocol provides protection to the entire datagram by embedding the header in the data. The AH verifies the integrity of the IP datagram. AH and ESP use symmetric secret key algorithms, although public key algorithms are feasible.

Authentication Header



- Ensures data integrity
- Provides origin authentication - ensures packets definitely came from peer router
- Uses keyed-hash mechanism
- Does NOT provide confidentiality (no encryption)
- Provides optional replay protection

Encapsulating Security Payload



- Data confidentiality (encryption)
- Limited traffic flow confidentiality
- Data integrity
- Optional data origin authentication
- Anti-replay protection
- Does not protect IP header

IPSec overview

The advantages of IPSec are:

- Easy deployment
  - -No change to intermediate systems such as service provider backbones are required
  - -No change to existing applications are required
  - -IPSec gateways enable managed services
- Scalability
  - -Scales to Service Provider levels
  - -Internet Key Exchange (IKE) for Internet
- Security Association and Key Management Protocol (ISAKMP)
  - -Interoperability with Public Key Infrastructure (PKI)
- Certificate Authorities
  - Windows 2000 Certificate Services are recommended for less than 100 devices
  - VeriSign, Entrust, Baltimore are recommended for greater than 100 device Fast deployment/provisioning
  - -VPN links are up in minutes
- Cost-effective
  - -Implemented in existing routers/CPEs
  - -Implemented in end-host software
- High-performance
  - -QoS integration is possible
  - -Dedicated crypto hardware is inexpensive

Authentication header

The IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams, and to provide protection against replays.

AH, defined in RFC 2402, provides authentication for as much of the IP header as possible, as well as for upper level protocol data. However, some IP header fields may change in transit. The value of these fields may not be predictable by the sender, when the packet arrives at the receiver. The values of such fields cannot be protected by AH.

AH is defined as IP protocol 51.

AH may be applied alone, in combination with the IP ESP, or in a nested fashion through the use of tunnel mode.

Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host.

Authentication header

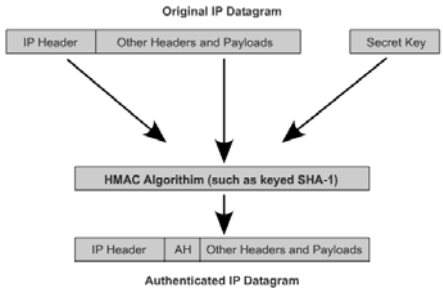
ESP may be used to provide the same security services, and it also provides a confidentiality, or encryption, service. The primary difference between the authentication services provided by ESP and AH is the extent of the coverage. Specifically, ESP does not protect any IP header fields unless ESP encapsulates those fields, or the fields are in tunnel mode.

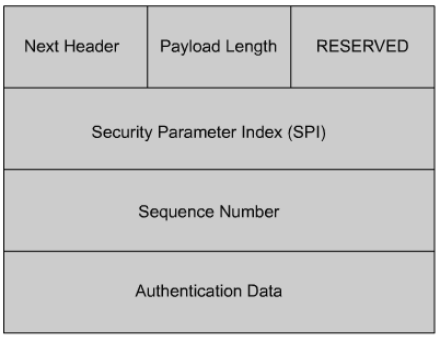
AH provides the packet authentication, integrity assurance, and replay detection/protection via sequence numbers. However, no confidentiality or encryption is provided.

The following are reasons to use AH even though ESP seems to do all the security services. First, AH requires less overhead than ESP. Second, AH is never export-restricted. Finally, AH is mandatory for IPv6 compliance.

Authentication header

The AH header structure is:
•A 32-bit Security Parameter Index (SPI) value shows the Security Association (SA) used for this packet
•A 64-bit sequence number prevents packet replay
•Authentication data is a HMAC value of the packet





Encapsulating security payload

ESP, defined in RFC 2406, is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service, and limited traffic flow confidentiality by defeating traffic flow analysis.

The set of services provided depends on options selected at the time of security association establishment and on the placement of the implementation.

Confidentiality may be selected independent of all other services. However, use of confidentiality without integrity authentication, either in ESP or separately in AH, may subject traffic to certain forms of active attacks that could undermine the confidentiality service.

ESP is defined as IP protocol 50.

Data origin authentication and connectionless integrity are joint services and are offered as an option in conjunction with optional confidentiality.

The anti-replay service may be selected only if data origin authentication is selected. Its election is solely at the discretion of the receiver. Although the default calls for the sender to increment the sequence number used for anti-replay, the service is effective only if the receiver checks the sequence number.

Encapsulating security payload

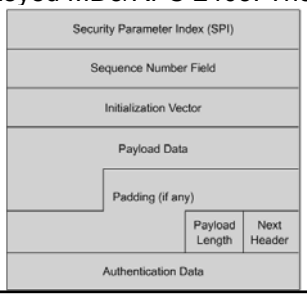
Traffic flow confidentiality requires selection of tunnel mode. Traffic flow confidentiality is most effective if implemented at a security gateway where traffic aggregation may be able to mask true source-destination patterns.

Note that although both confidentiality and authentication are optional, at least one of them must be selected.

One of the most important values ina a ESP header is the Security Parameters Index (SPI) that allows the router to keep track to the current security association between two IPSec devices.

Encryption is done with DES or 3DES. Optional authentication and integrity are provided with HMAC, keyed SHA-1/RFC 2404, or keyed MD5/RFC 2403. There are two different key types contained in the SA:

- Encryption session keys
- HMAC session keys



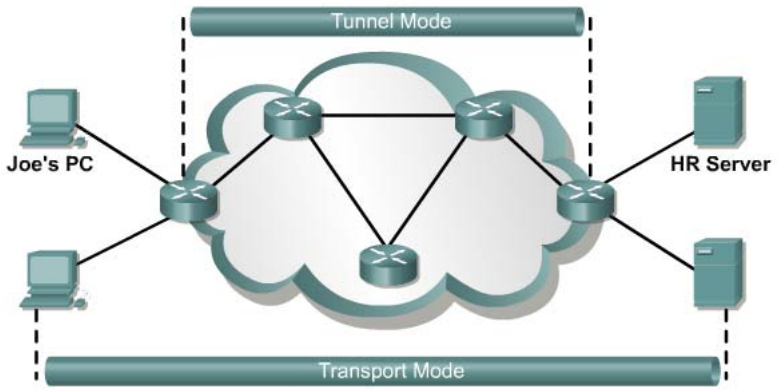
IPSec modes

ESP and AH can be applied to IP packets in two different ways, transport mode and tunnel mode.

In transport mode, security is provided only for the transport layer and above. Transport mode protects the payload of the packet but leaves the original IP address in the clear. The original IP address is used to route the packet through the Internet. In transport mode, each end host does IPSec encapsulation of its own data, host-to-host. Therefore, IPSec has to be implemented on end-hosts. The application endpoint must also be the IPSec endpoint.

Tunnel mode provides security for the whole original IP packet. The original IP packet is encrypted. Next, the encrypted packet is encapsulated in another IP packet. The outside IP address is used to route the packet through the Internet. In tunnel mode, IPSec gateways provide IPSec services to other hosts in peer-to-peer tunnels. End-hosts are not aware of IPSec being used to protect their traffic. IPSec gateways provide transparent protection of the traffic of other hosts over untrusted networks.

IPSec modes

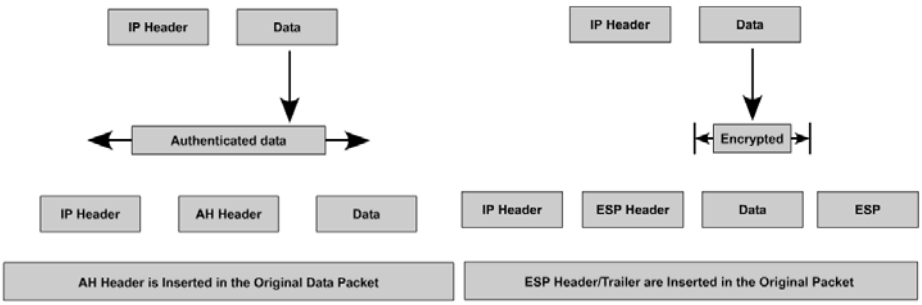


Transport mode

In transport mode, the AH header normally adds 24 bytes to each packet.

In transport mode, the ESP header/trailer normally adds up to 37 bytes to each packet.

Using both AH and ESP in tunnel mode can add up to 61 bytes to each packet.

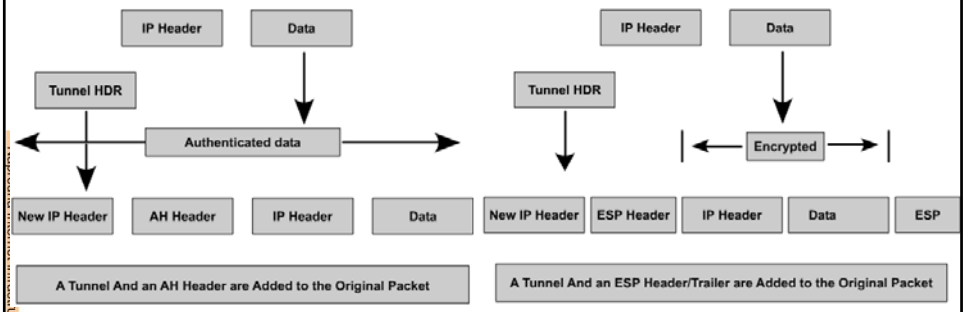


Tunnel mode

In tunnel mode, the tunnel IP and AH headers add 44 bytes to each packet.

In tunnel mode, the tunnel IP and ESP headers and trailer add up to 57 bytes to each packet.

Using both AH and ESP in tunnel mode can add up to 101 bytes to each packet.



IPSec security associations

IPSec Security Associations (SAs) represent a policy contract between two peers or hosts, and describe how the peers will use IPSec security services to protect network traffic.

SAs contain all the security parameters needed to securely transport packets between the peers or hosts, and practically define the security policy used in IPSec.

Establishment of SAs is a prerequisite for IPSec traffic protection to work. When relevant SAs are established, IPSec refers to them for all parameters needed to protect a particular traffic flow.

SAs always contain unidirectional, or one-way, specifications.

SAs are also encapsulation protocol specific. There is a separate SA for each encapsulation protocol, AH and ESP, for a given traffic flow.

If two hosts A and B are communicating securely using both AH and ESP, then each host builds separate SAs, inbound and outbound, for each protocol.

VPN devices store all their active SAs in a local database called the SA database (SADB).

IPSec security associations

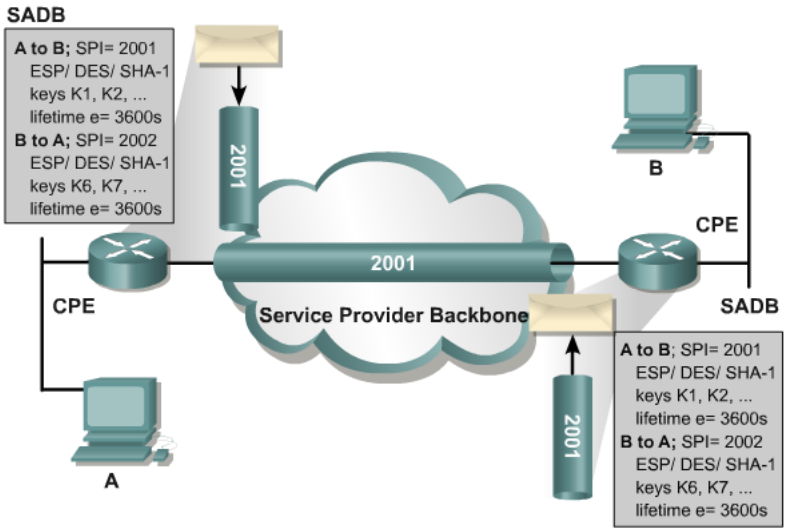
An SA contains the following security parameters :
•Authentication/encryption algorithm, key length and other encryption parameters, such as key lifetime, used with protected packets
•Session keys for authentication, or HMACs, and encryption, which can be entered manually or negotiated automatically with the help of the IKE protocol, fed to the algorithms
•A specification of network traffic to which the SA will be applied, such as all IP traffic or only TELNET sessions
•IPSec AH or ESP encapsulation protocol and tunnel or transport mode

The Security Parameters Index (SPI) is a 32-bit number that identifies each established SA.

The SPI uniquely identifies a particular SA in the SADB.

SPIs are written into IPSec packet headers to locate the appropriate SA on the receiving system.

IPSec security associations



Five steps of IPSec

The goal of IPSec is to protect the desired data with the necessary security and algorithms. The operation of IPSec can be broken down into five primary steps:

1.Interesting traffic initiates the IPSec process. Traffic is deemed interesting when a packet triggers an access list that defines traffic to be protected.

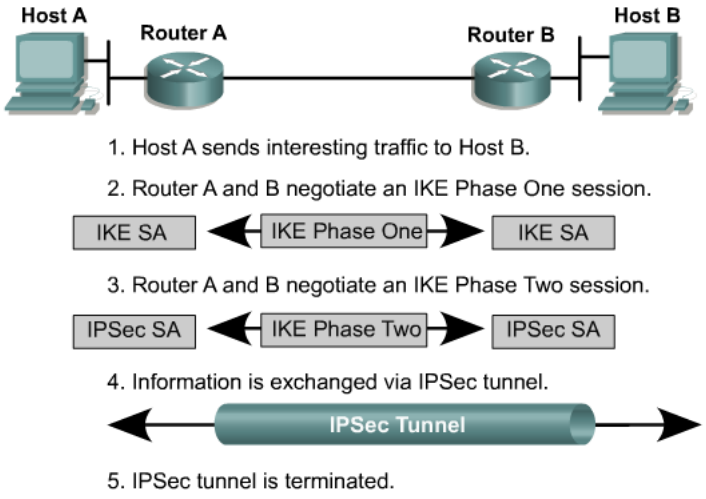
2.During IKE Phase One, IKE authenticates IPSec peers and negotiates IKE SAs, setting up a secure communications channel for negotiating IPSec SAs in phase two.

3.During IKE Phase Two, IKE negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers. These security parameters are used to protect data and messages exchanged between endpoints.

4.During the data transfer phase, data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.

5.During IPSec tunnel termination, IPSec SAs terminate through deletion or by timing out.

Five steps of IPSec



IKE

Internet Key Exchange (IKE) enhances IPSec by providing additional features and flexibility. It makes IPSec easier to configure.

IKE, defined in RFC 2409, is a hybrid protocol which implements the Oakley key exchange and SKeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework.

ISAKMP is defined in RFC 2408. ISAKMP, Oakley, and SKeme are security protocols implemented by IKE.

IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations.

IKE Mode configuration allows a gateway to download an IP address, and other network level configuration, to the client as part of an IKE negotiation. Using this exchange, the gateway gives IP addresses to the IKE client to be used as an inner IP address encapsulated under IPSec. This provides a known IP address for the client, which can be matched against IPSec policy.

IKE

IKE provides the following benefits:
•Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers
•Allows administrators to specify a lifetime for the IPSec security association
•Allows encryption keys to change during IPSec sessions
•Allows IPSec to provide anti-replay services
•Permits certification authority (CA) support for a manageable, scalable IPSec implementation
•Allows dynamic authentication of peers

One of the most important factors in the IKE SA negotiation is the mutual authentication of peers. Each peer must be sure that it is talking to the correct peer, before negotiating traffic protection (IPsec) policies with it. This mutual authentication is accomplished via IKE's two-way authentication methods. IKE provides three defined methods for two-way authentication:
•Authentication using a pre-shared secret
•Authentication using RSA encrypted nonces
•Authentication using RSA signatures

IKE

The component technologies implemented for use by IKE are:

DES-The Data Encryption Standard (DES) is used to encrypt packet data. IKE implements the 56-bit DES-CBC with Explicit IV standard.

3DES-168-bit encryption. 3DES in simple terms is DES performed 3 three times on the same data. The strength of 3DES is approximately twice the strength of DES.

CBC- Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPSec packet.

Diffie-Hellman- A public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE to establish session keys. 768-bit and 1024-bit Diffie-Hellman groups are supported.

MD5- (HMAC variant)-Message Digest 5 (MD5) is a hash algorithm used to authenticate packet data. HMAC is a variant that provides an additional level of hashing.

SHA- (HMAC variant)- Secure Hash Algorithm (SHA) is a hash algorithm used to authenticate packet data. HMAC is a variant that provides an additional level of hashing.

IKE phases

The events within an IKE session happen in following order:

In IKE Phase One (main or aggressive mode) the peers will:
•Negotiate an IKE protection suite
•Authenticate each other
•Exchange keying material to protect the IKE session
•Establish the IKE SA

Then in IKE Phase Two (quick mode) peers:
•Negotiate IPsec policies
•Exchange keying material of IPsec SAs
•Establish IPsec SAs

IKE Phase One

IKE Phase One runs in main or aggressive mode.

The mode used is implementation and situation dependent.

The purpose of IKE Phase One is the negotiation of an IKE protection suite, the authentication of peers, the exchange of keying material to protect the IKE session, and finally the establishment of an IKE SA, which defines the parameters of the secure IKE channel.

The IKE main mode is the first mode that negotiates protection suites between peers.

ISAKMP uses six messages to establish the IKE SA. These messages include SA negotiation, a Diffie-Hellman key exchange, and the authentication of peers.

IKE main mode hides the identity of IKE peers from eavesdroppers, and can use the protocol's negotiation capabilities to the fullest.

IKE Phase One

Like the IKE main mode, the IKE aggressive mode negotiates protection suites between peers.

The major difference between the main and the aggressive mode is that the aggressive mode takes half the number of messages as the main mode and consequently offers less negotiating flexibility for the IKE session protection.

The initiating peer proposes a list of policies, and the responder accepts a policy or rejects the offers with no further negotiation of protection details.

The aggressive mode does protection suite negotiation, authentication of peers, and generates keying material as the main mode does, but because of limited capabilities it does not provide peer identity protection (For example, an eavesdropper can determine the identity of negotiating peers).

Because only three messages are needed to establish IKE SA, an IKE aggressive mode exchange is also much faster than an IKE main mode exchange.

It is used mainly when security policies are well known on both peers, and there is no need to use the full IKE negotiation capabilities to establish an IKE SA as quickly as possible.

IKE Phase Two

IKE Phase Two is used to negotiate and establish SAs of other protocols (IPsec's AH and ESP, IP PCP (payload compression protocol), etc).

Phase Two needs an established IKE SA (produced in IKE Phase One to protect the IKE session) to operate, and only operates in one defined mode, the quick mode.

The IKE initiator presents a list of (IPsec) policy proposals and the IKE responder chooses an acceptable proposal according to its locally defined policy. When the policy between peers is agreed upon, the keying material is agreed upon, and IPsec SAs are established.

IKE quick mode is quite fast, with almost no noticeable delay associated with it and if no Perfect Forward Secrecy (PFS) functionality is used with IPsec.

Once an IKE SA is in place (established via Main Mode or Aggressive Mode), only quick mode exchanges are used to negotiate additional IPsec SAs or to rekey established IPsec SAs, which are about to expire.

IPSec in Cisco IOS software