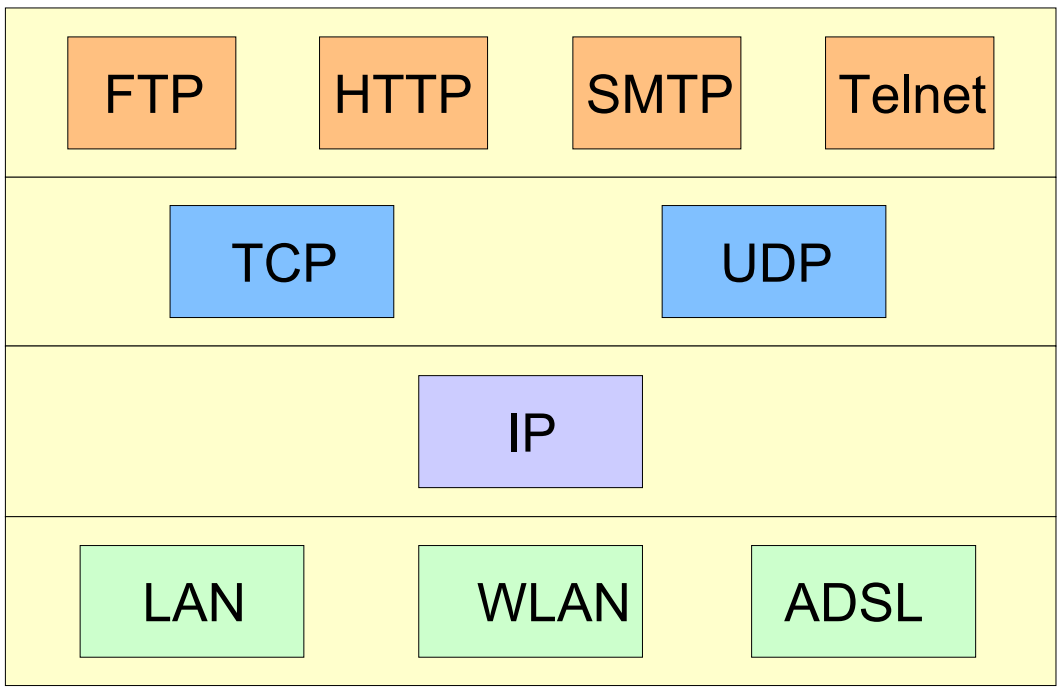
Ponovitev osnov protokola IP

- Protokol IP je protokol omrežnega sloja
  - IP v4
  - IP v6

OSI	TCP/IP
aplikacijski sloj	aplikacijski sloj
predstavitveni sloj	
sejni sloj	prenosni sloj
prenosni sloj	
omrežni sloj	omrežni sloj
povezovalni sloj	dostopovni sloj
fizični sloj	

Ponovitev osnov protokola IP

- Nekaj protokolov, ki so povezani s protokolom IP



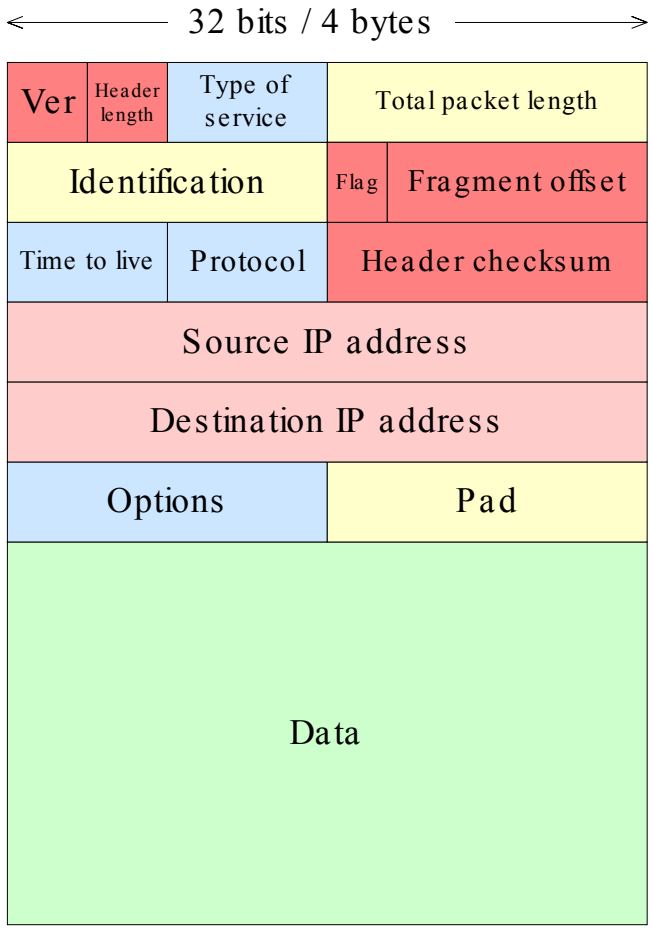
aplikacijski sloj

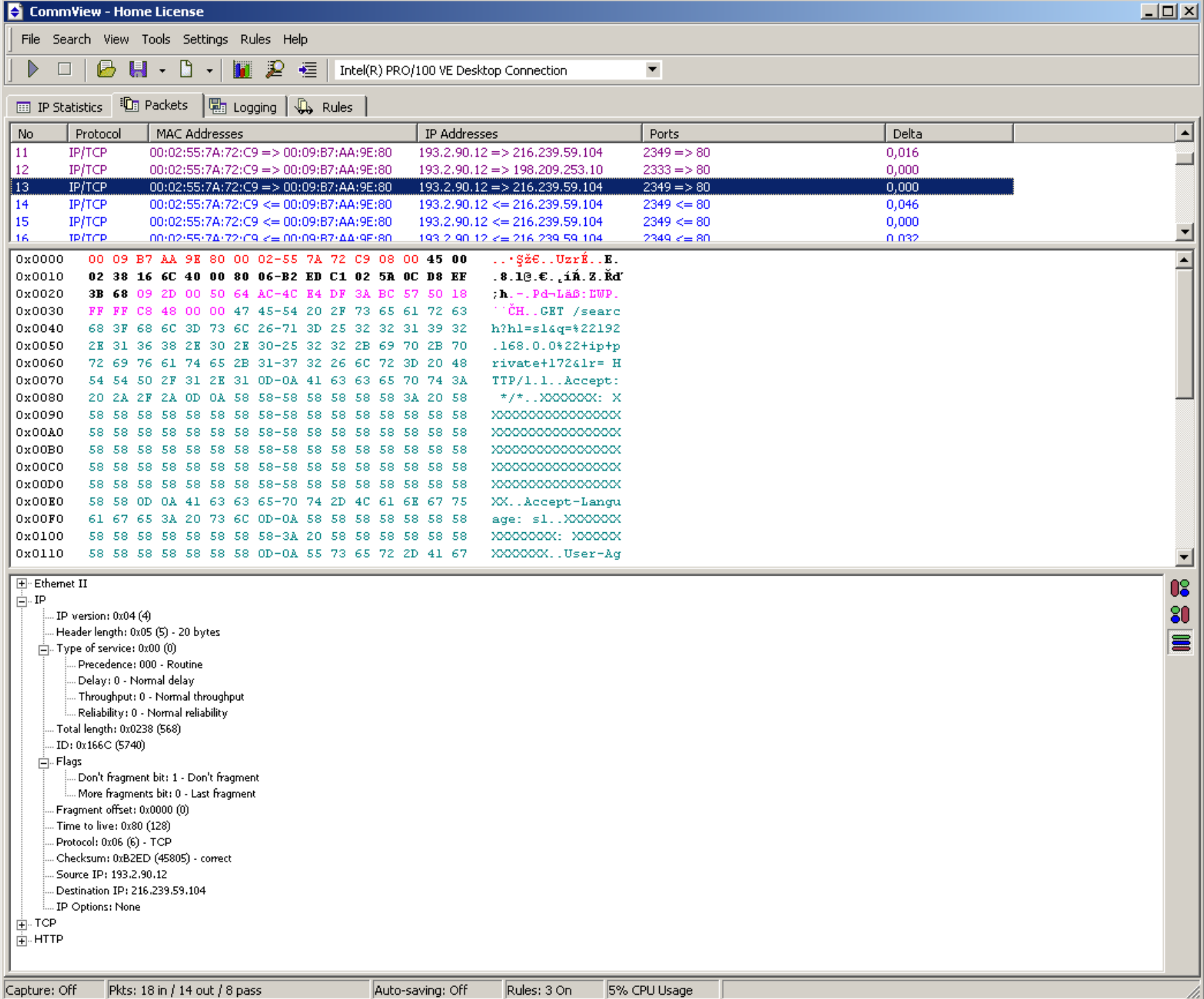
prenosni sloj

omrežni sloj

dostopovni sloj

Ponovitev osnov protokola IP




CommView - Home License
File Search View Tools Settings Rules Help
Intel(R) PRO/100 VE Desktop Connection
IP Statistics
Packets
Logging
Rules
No | Protocol | MAC Addresses | IP Addresses | Ports | Delta
11 | IP/TCP | 00:02:55:7A:72:C9 => 00:09:B7:AA:9E:80 | 193.2.90.12 => 216.239.59.104 | 2349 => 80 | 0,016
12 | IP/TCP | 00:02:55:7A:72:C9 => 00:09:B7:AA:9E:80 | 193.2.90.12 => 198.209.253.10 | 2333 => 80 | 0,000
13 | IP/TCP | 00:02:55:7A:72:C9 => 00:09:B7:AA:9E:80 | 193.2.90.12 => 216.239.59.104 | 2349 => 80 | 0,000
14 | IP/TCP | 00:02:55:7A:72:C9 <= 00:09:B7:AA:9E:80 | 193.2.90.12 <= 216.239.59.104 | 2349 <= 80 | 0,046
15 | IP/TCP | 00:02:55:7A:72:C9 <= 00:09:B7:AA:9E:80 | 193.2.90.12 <= 216.239.59.104 | 2349 <= 80 | 0,000
0x0000 00 09 B7 AA 9E 80 00 02-55 7A 72 C9 08 00 45 00
0x0010 02 38 16 6C 40 00 80 06-B2 ED C1 02 5A 0C D8 EF
0x0020 3B 68 09 2D 00 50 64 AC-4C E4 DF 3A BC 57 50 18
0x0030 FF FF C8 48 00 00 47 45-54 20 2F 73 65 61 72 63
0x0040 68 3F 68 6C 3D 73 6C 26-71 3D 25 32 32 31 39 32
0x0050 2E 31 36 38 2E 30 2E 30-25 32 32 2B 69 70 2B 70
0x0060 72 69 76 61 74 65 2B 31-37 32 26 6C 72 3D 20 48
0x0070 54 54 50 2F 31 2E 31 0D-0A 41 63 63 65 70 74 3A
0x0080 20 2A 2F 2A 0D 0A 58 58-58 58 58 58 58 3A 20 58
0x0090 58 58 58 58 58 58 58 58-58 58 58 58 58 58 58 58
0x00A0 58 58 58 58 58 58 58 58-58 58 58 58 58 58 58 58
0x00B0 58 58 58 58 58 58 58 58-58 58 58 58 58 58 58 58
0x00C0 58 58 58 58 58 58 58 58-58 58 58 58 58 58 58 58
0x00D0 58 58 58 58 58 58 58 58-58 58 58 58 58 58 58 58
0x00E0 58 58 0D 0A 41 63 63 65-70 74 2D 4C 61 6E 67 75
0x00F0 61 67 65 3A 20 73 6C 0D-0A 58 58 58 58 58 58 58
0x0100 58 58 58 58 58 58 58 58-3A 20 58 58 58 58 58 58
0x0110 58 58 58 58 58 58 58 0D-0A 55 73 65 72 2D 41 67
Ethernet II
IP
IP version: 0x04 (4)
Header length: 0x05 (5) - 20 bytes
Type of service: 0x00 (0)
Precedence: 000 - Routine
Delay: 0 - Normal delay
Throughput: 0 - Normal throughput
Reliability: 0 - Normal reliability
Total length: 0x0238 (568)
ID: 0x166C (5740)
Flags
Don't fragment bit: 1 - Don't fragment
More fragments bit: 0 - Last fragment
Fragment offset: 0x0000 (0)
Time to live: 0x80 (128)
Protocol: 0x06 (6) - TCP
Checksum: 0xB2ED (45805) - correct
Source IP: 193.2.90.12
Destination IP: 216.239.59.104
IP Options: None
TCP
HTTP
Capture: Off
Pkts: 18 in / 14 out / 8 pass
Auto-saving: Off
Rules: 3 On
5% CPU Usage

Naslavljanje v omrežjih IP

- Dolžina naslova
  - IPv4: 32 bitov (pribl. 10^{10} naslovov)
  - IPv6: 128 bitov (pribl. 10^{38} naslovov)
- Omrežna maska
  - je obvezni sestavni del naslova omrežja
  - pove število naslovov (pod)omrežja
  - maska ene naprave je 255.255.255.255
- Primeri
  - 10.2.0.0/24 = 10.2.0.0 255.255.255.0
  - 192.168.0.0/16 = 192.168.0.0 255.255.0.0
  - 213.9.10.64/26 = 213.9.10.64 255.255.255.192

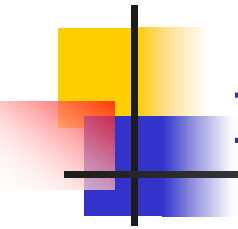
Vrste naslovov v omrežjih IP

- Zasebni naslovi
  - razred A

    10.0.0.0/8 = [10.0.0.0, 10.255.255.255]
  - razred B

    172.16.0.0/12 = [172.16.0.0, 172.31.255.255]
  - razred C

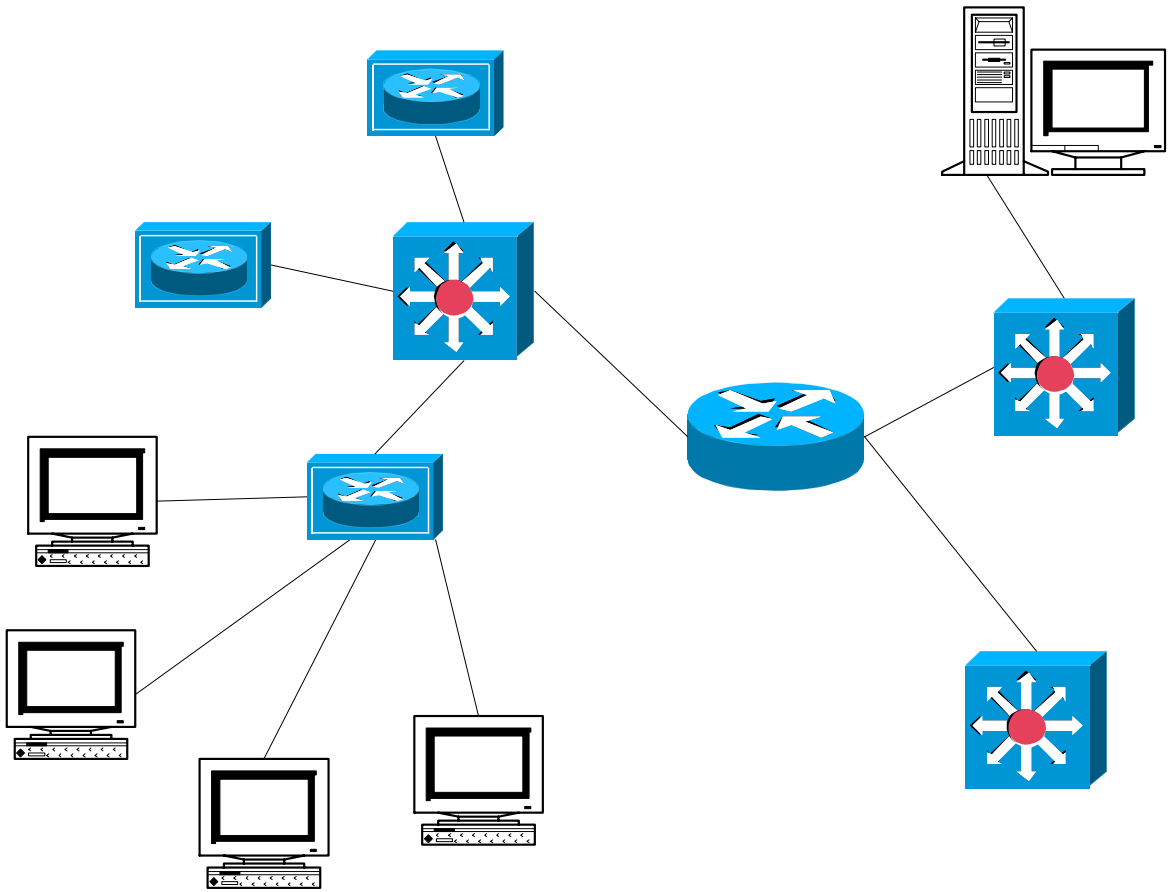
    192.168.0.0/16 = [192.168.0.0, 192.168.255.255]
- Javni naslovi



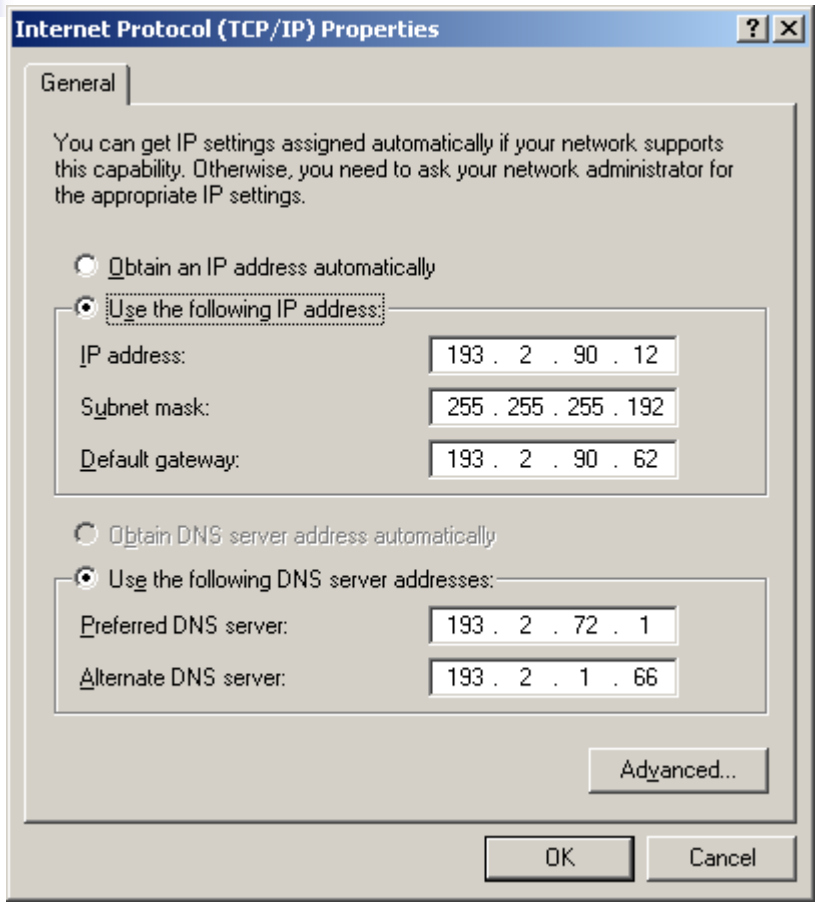
Internetno omrežje

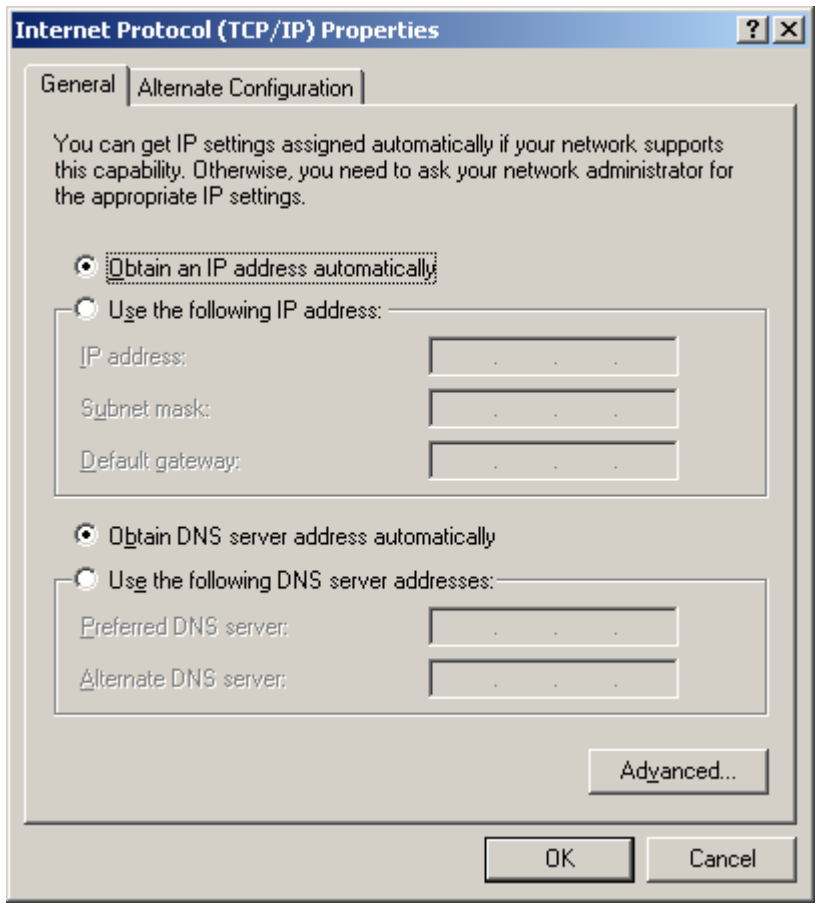
- Zgradba internetnega omrežja
  - dostopovno omrežje
  - hrbtenično omrežje
- Gradniki omrežij
  - usmerjevalniki (router)
  - stikala (switch)
  - dostopovni vozli (hub)
  - brezžične dostopovne točke (access point)

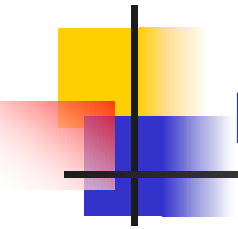
Primer zgradbe omrežja



Nastavitve odjemalca IP

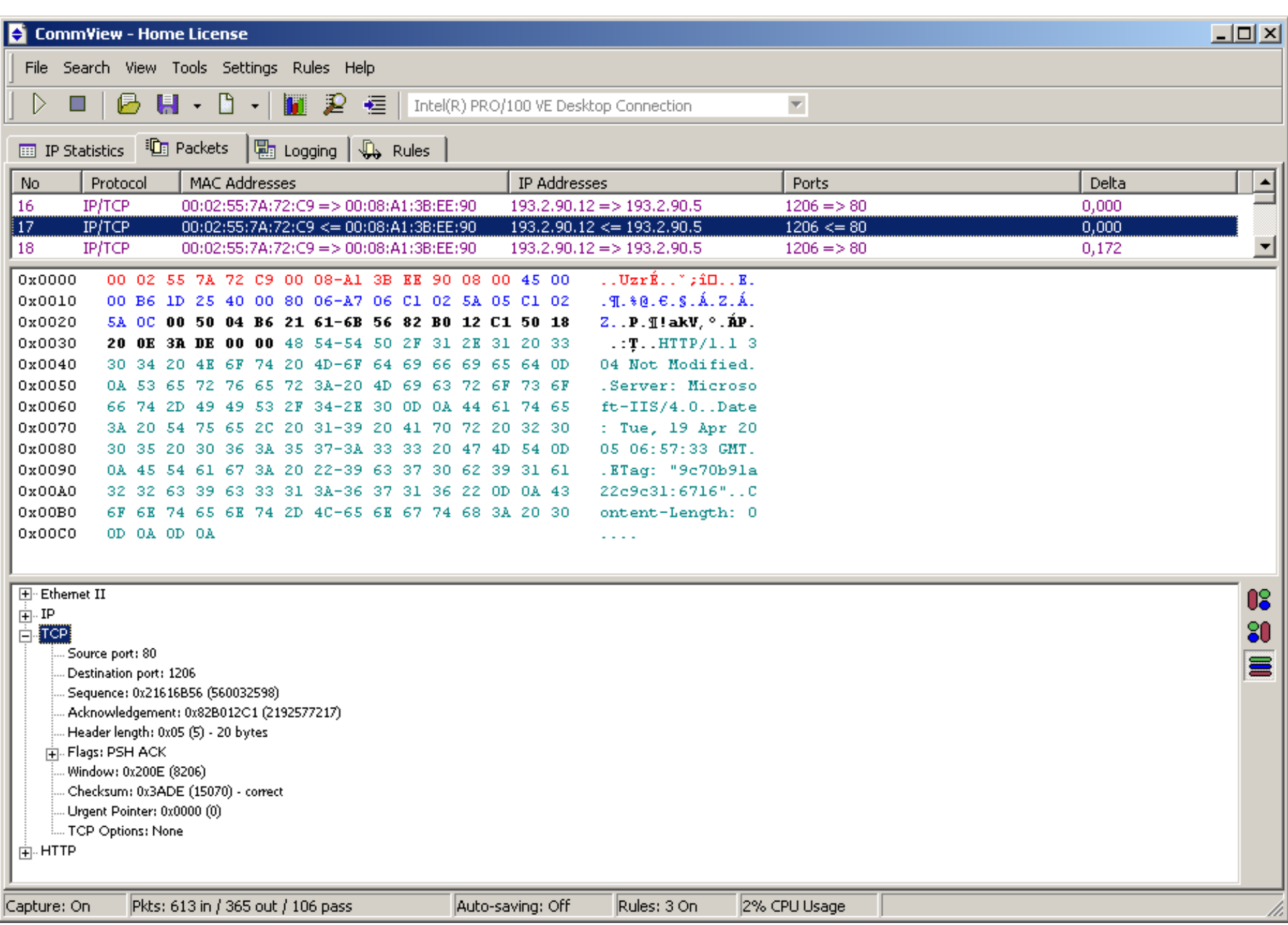






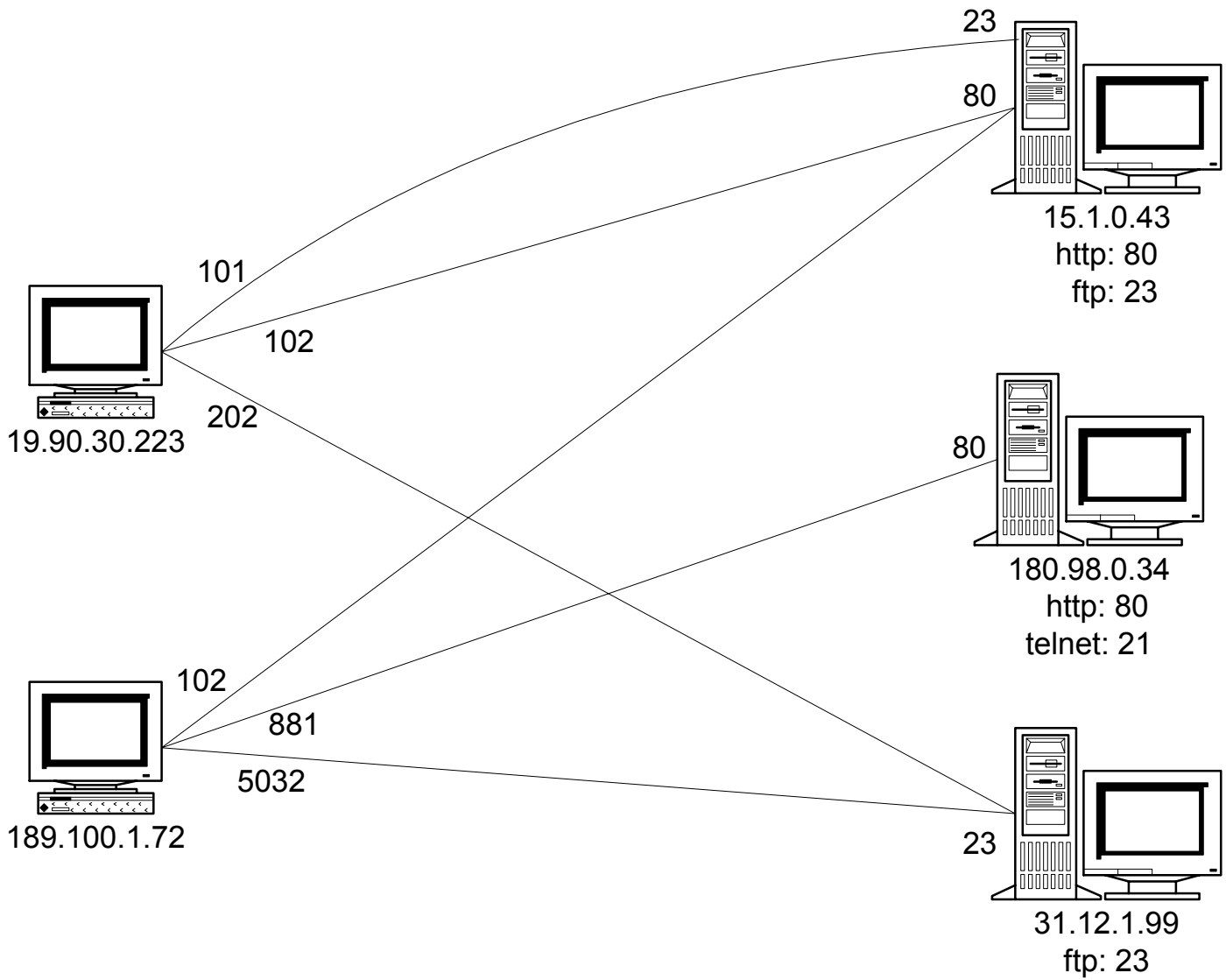
Protokola TCP in UDP

- TCP - Transmission Control Protocol
  - povezavno orientiran
  - zanesljiv
- UDP – User Datagram Protocol
  - nepovezavno orientiran
  - enostaven
- Povezava TCP
  - vzpostavitev povezave
  - prenos podatkov
  - rušenje povezave
- Povezava UDP
  - "Pošlji in upaj na najboljše"


CommView - Home License
File Search View Tools Settings Rules Help
Intel(R) PRO/100 VE Desktop Connection
IP Statistics
Packets
Logging
Rules
No | Protocol | MAC Addresses | IP Addresses | Ports | Delta
16 | IP/TCP | 00:02:55:7A:72:C9 => 00:08:A1:3B:EE:90 | 193.2.90.12 => 193.2.90.5 | 1206 => 80 | 0,000
17 | IP/TCP | 00:02:55:7A:72:C9 <= 00:08:A1:3B:EE:90 | 193.2.90.12 <= 193.2.90.5 | 1206 <= 80 | 0,000
18 | IP/TCP | 00:02:55:7A:72:C9 => 00:08:A1:3B:EE:90 | 193.2.90.12 => 193.2.90.5 | 1206 => 80 | 0,172
0x0000 00 02 55 7A 72 C9 00 08-A1 3B EE 90 08 00 45 00 ..UzrÉ..˘;îÐ..E.
0x0010 00 B6 1D 25 40 00 80 06-A7 06 C1 02 5A 05 C1 02 .¶.%@.€.§.Á.Z.Á.
0x0020 5A 0C 00 50 04 B6 21 61-6B 56 82 B0 12 C1 50 18 Z..P.¶!akV‚°.ÁP.
0x0030 20 0E 3A DE 00 00 48 54-54 50 2F 31 2E 31 20 33 .:Ţ..HTTP/1.1 3
0x0040 30 34 20 4E 6F 74 20 4D-6F 64 69 66 69 65 64 0D 04 Not Modified.
0x0050 0A 53 65 72 76 65 72 3A-20 4D 69 63 72 6F 73 6F .Server: Microso
0x0060 66 74 2D 49 49 53 2F 34-2E 30 0D 0A 44 61 74 65 ft-IIS/4.0..Date
0x0070 3A 20 54 75 65 2C 20 31-39 20 41 70 72 20 32 30 : Tue, 19 Apr 20
0x0080 30 35 20 30 36 3A 35 37-3A 33 33 20 47 4D 54 0D 05 06:57:33 GMT.
0x0090 0A 45 54 61 67 3A 20 22-39 63 37 30 62 39 31 61 .ETag: "9c70b91a
0x00A0 32 32 63 39 63 33 31 3A-36 37 31 36 22 0D 0A 43 22c9c31:6716"..C
0x00B0 6F 6E 74 65 6E 74 2D 4C-65 6E 67 74 68 3A 20 30 ontent-Length: 0
0x00C0 0D 0A 0D 0A ....
Ethernet II
IP
TCP
Source port: 80
Destination port: 1206
Sequence: 0x21616B56 (560032598)
Acknowledgement: 0x82B012C1 (2192577217)
Header length: 0x05 (5) - 20 bytes
Flags: PSH ACK
Window: 0x200E (8206)
Checksum: 0x3ADE (15070) - correct
Urgent Pointer: 0x0000 (0)
TCP Options: None
HTTP
Capture: On
Pkts: 613 in / 365 out / 106 pass
Auto-saving: Off
Rules: 3 On
2% CPU Usage

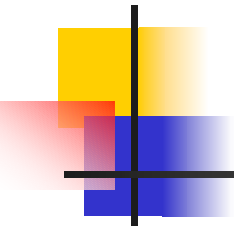
Naslavljanje aplikacije

- Naslov aplikacije na strežniku je sestavljen iz naslova IP in številke vrat (t.i. socket)
- Vrata (port)
  - izvorna (source) in ponorna (destination) vrata
  - vsaka aplikacija ima svoja vrata
- Nekaj primerov (well-known port numbers)
  - 80: protokol HTTP
  - 21: protokol FTP
  - 23: protokol Telnet
  - 110: POP3
- Izvorna vrata odjemalca imajo poljubno vrednost


23
80
15.1.0.43
http: 80
ftp: 23
101
102
202
19.90.30.223
80
180.98.0.34
http: 80
telnet: 21
102
881
5032
189.100.1.72
23
31.12.1.99
ftp: 23

Prevajanje omrežnih naslovov

- NAT – Network Address Translation
  - običajno del usmerjevalnika
  - pretvori zasebne naslove v javne ter obratno
- Zagotavljanje varnosti s kombinacijo požarnega zidu in prevajanja naslovov

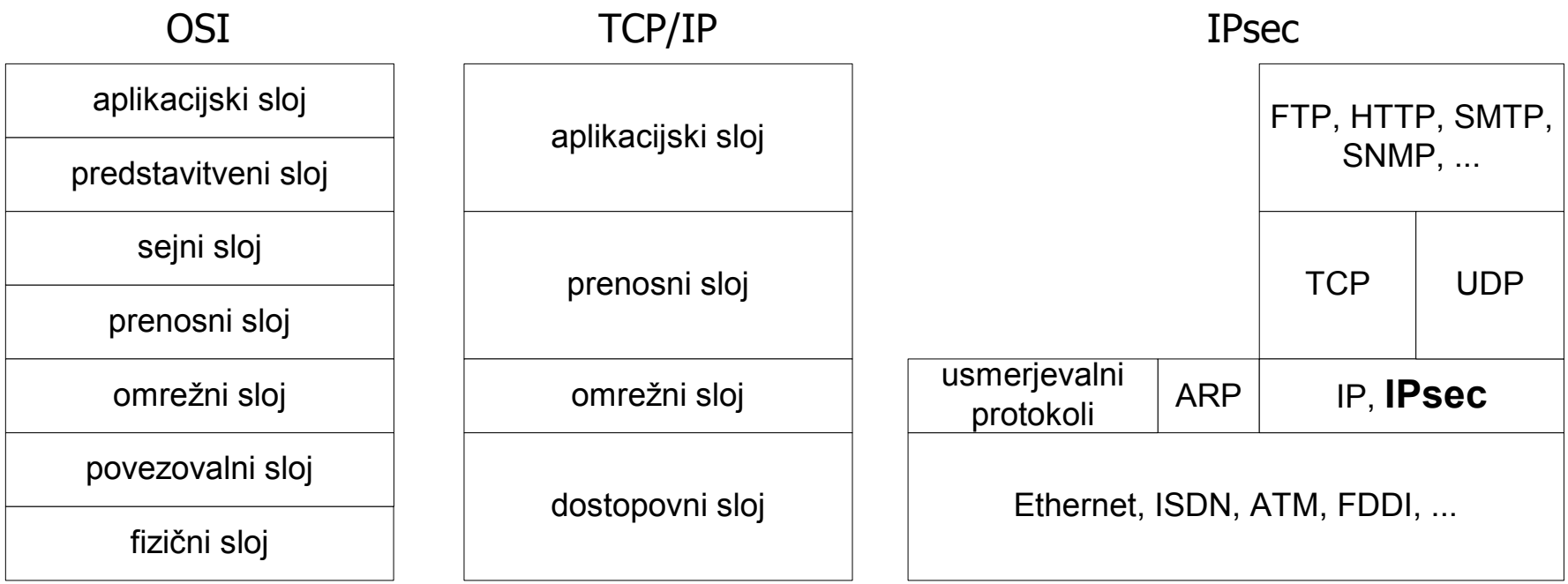


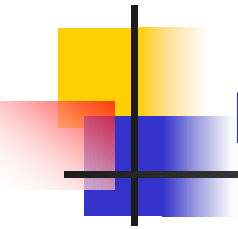
Uvod v IPsec

- Zaščita IP paketov
  - protokoli varnosti (AH, ESP)
  - avtentikacijski algoritmi
  - šifrirni algoritmi
- Del standarda IPv6
- Združljivost z IPv4

Uvod v IPsec

- IPsec je protokol omrežnega sloja



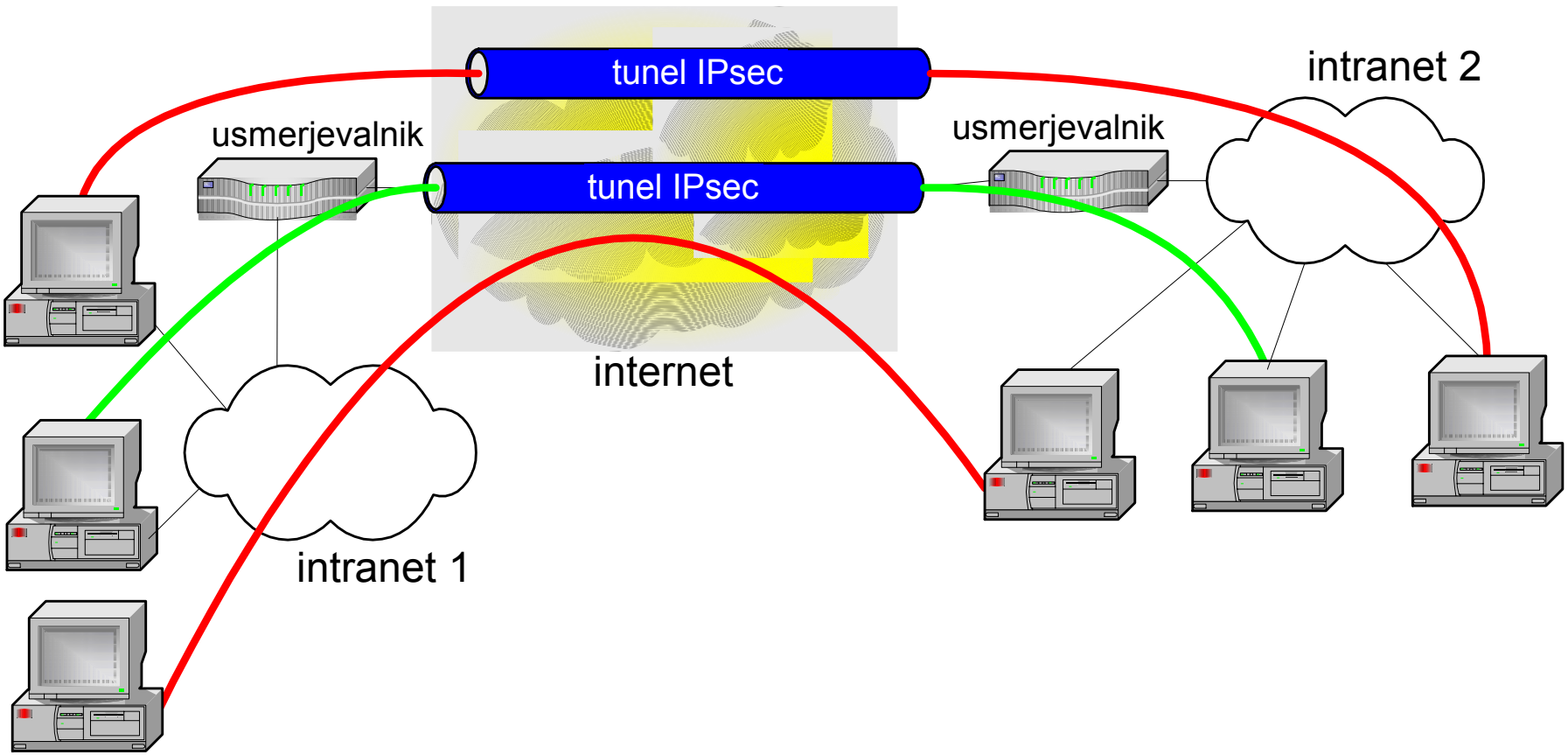


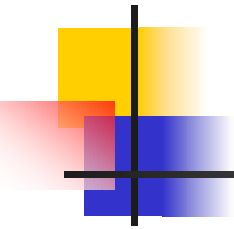
Možnosti uporabe

- Varna povezava poljubnih IPsec naprav
- Varna povezava lokalnih omrežij
- Gradnja navideznih zasebnih omrežij
- Varen dostop oddaljenih uporabnikov
- Varen dostop mobilnih uporabnikov

Načini uporabe

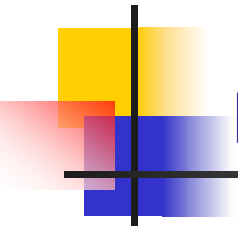
- Transportni način prenosa
- Tunelski način prenosa





Delovanje protokola IPsec

- Navidezno povezavno orientiran
- Vzpostavljanje povezav
  - ročna vzpostavitev
  - protokol Internet Key Exchange (IKE)

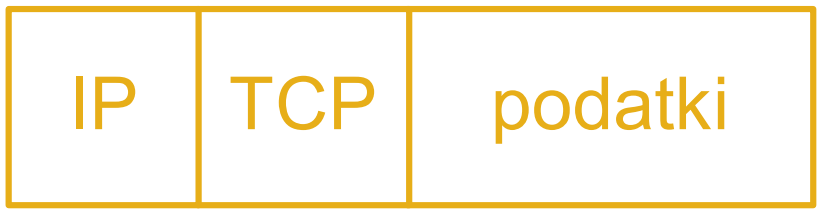


Protokola varnosti

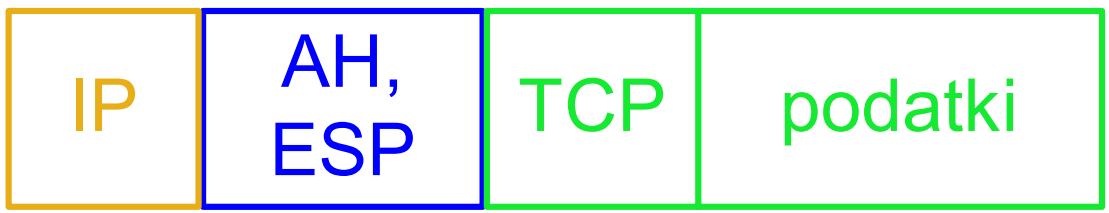
- Authentication Header – AH
  - avtentikacija glave IP
  - avtentikacija podatkov
- Encapsulating Security Payload – ESP
  - avtentikacija podatkov
  - šifriranje podatkov

Prenosna načina

- Originalni paket IP



- Paket IPsec v transportnem načinu prenosa



- Paket IPsec v tunelskem načinu prenosa