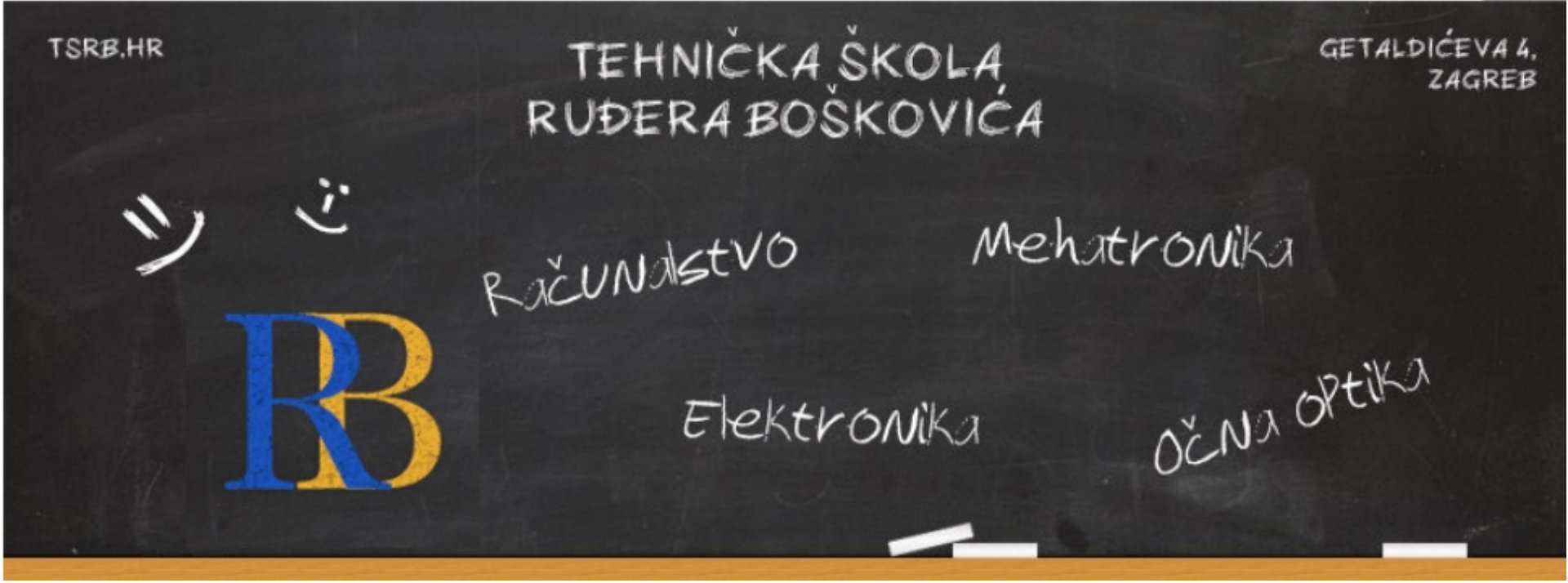


Liste za kontrolu pristupa

Računalne mreže_3.H

ACL

- Usmjernici, pored usmjeravanja podatkovnog prometa, omogućuju stvaranje **lista za kontrolu pristupa (engl. Access Control List - ACL)**
  - moguće je ograničiti ili potpuno onemogućiti pristup pojedinim uslugama te otežati izvođenje određenih vrsta mrežnih napada
- Zaštitni mehanizam koji sprječava neželjeni pristup mreži
- Predstavljaju osnovu mrežne sigurnosti na razini usmjernika
- Djeluju na principu filtriranja prometa

Zašto ACLs ?

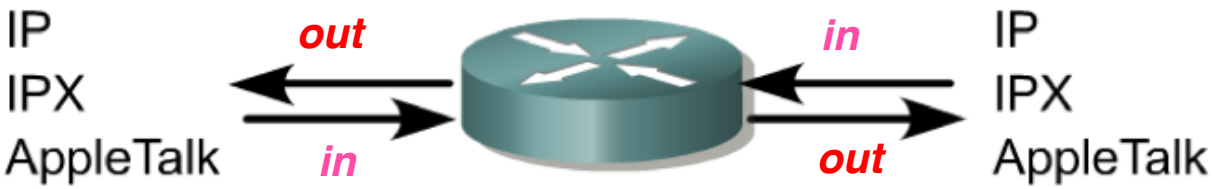
- smanjuju promet na mreži i povećavaju efikasnost mreže
- kontroliraju promet
- određuju koju vrstu prometa blokirati, a koju propustiti
- administrator (na zahtjev nadređenog) određuje u koji dio mreže klijent može ući

Kako ACLs rade?

- OS testira paket – provjeravajući redom uvjete od vrha liste prema dnu
- Ako je uvjet zadovoljen – odlučuje se da li će se paket odbaciti ili propustiti
  - Paket koji je jednom zadovoljio uvjet – više se ne provjerava
    - ostali uvjeti ACL se ignoriraju
  - Važan je raspored tvrdnji u ACL!
- Ako nije zadovoljen niti jedan uvjet paket je odbačen, jer na kraju ACL se podrazumijeva “zabrani sve” "deny any"

Pristupne liste (ACLs)

- Definiraju se
  - po protokolu, za smjer, po portu (interface)

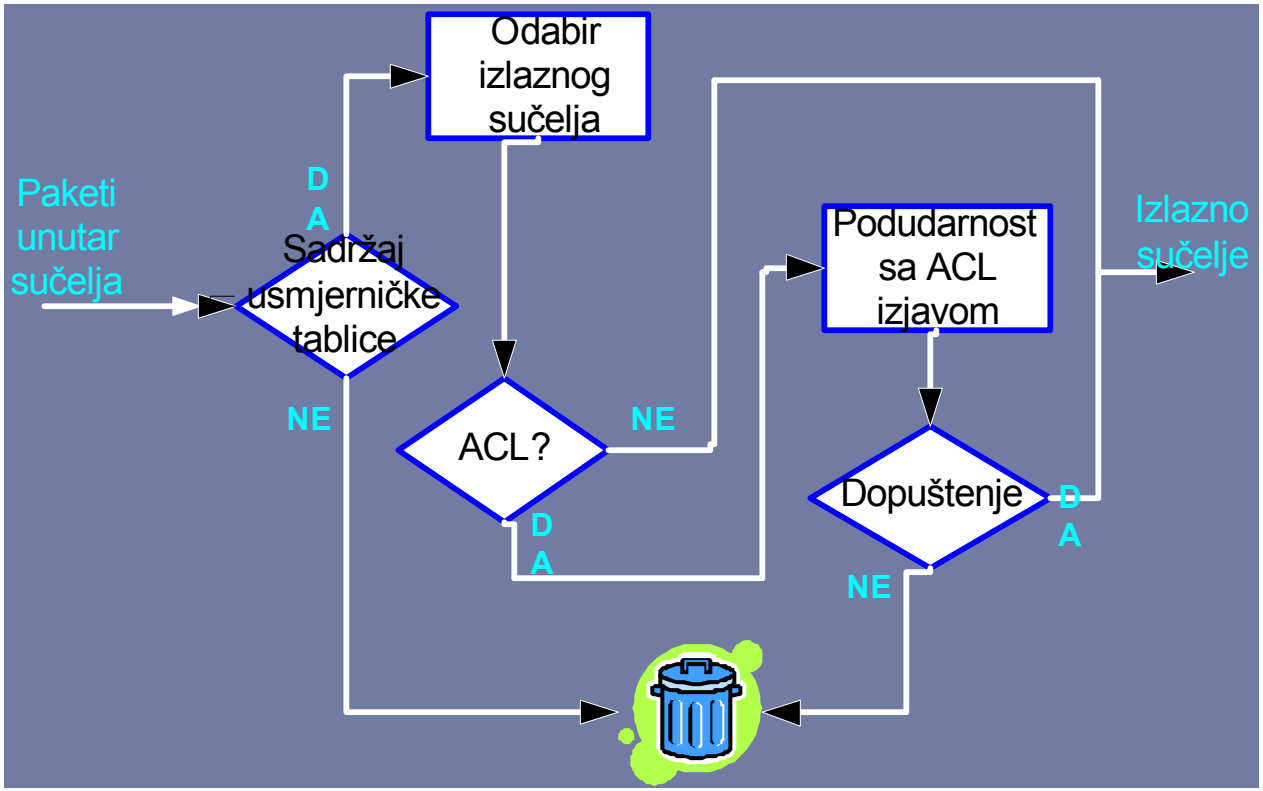


One list, per port, per direction, per protocol

With two interfaces and three protocols running, this router could have a total of 12 separate ACLs applied.

- ACL mogu djelovati na izlaznom ili ulaznom sučelju usmjernika

- Logika djelovanja ACL na izlaznom sučelju:



ACL

Osnovna podjela ACL lista:

- **Standardne** - filtriranje prometa samo na temelju izvorišne adrese zapisane u zaglavlju IP

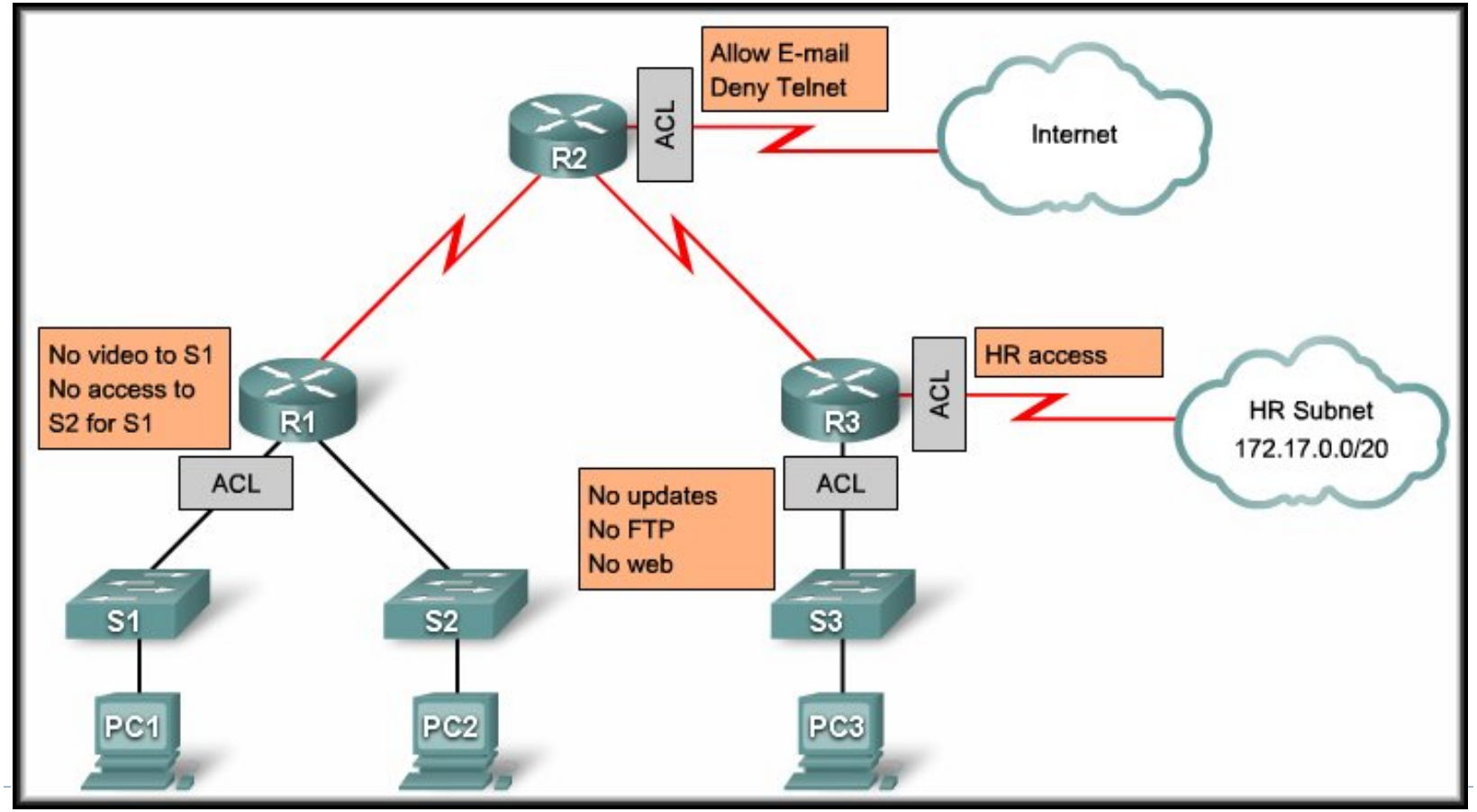
- **Proširene** – filtriranje prometa prema:
  - izvorišnoj IP adresi
  - odredišnoj IP adresi
  - Protokolu (IP, ICMP, OSPF, TCP, UDP i drugi)
  - podacima (brojevi TCP i UDP portova, TCP zastavice i ICMP poruke)

- Svaka lista predstavlja skupinu unosa koji definiraju pravila filtriranja
- unosi se grupiraju na temelju imena ili brojevne oznake
- Npr. za Cisco usmjernike, IP protokolu dodijeljeni rasponi brojevnih oznaka 1 do 99 i 1300 do 1999

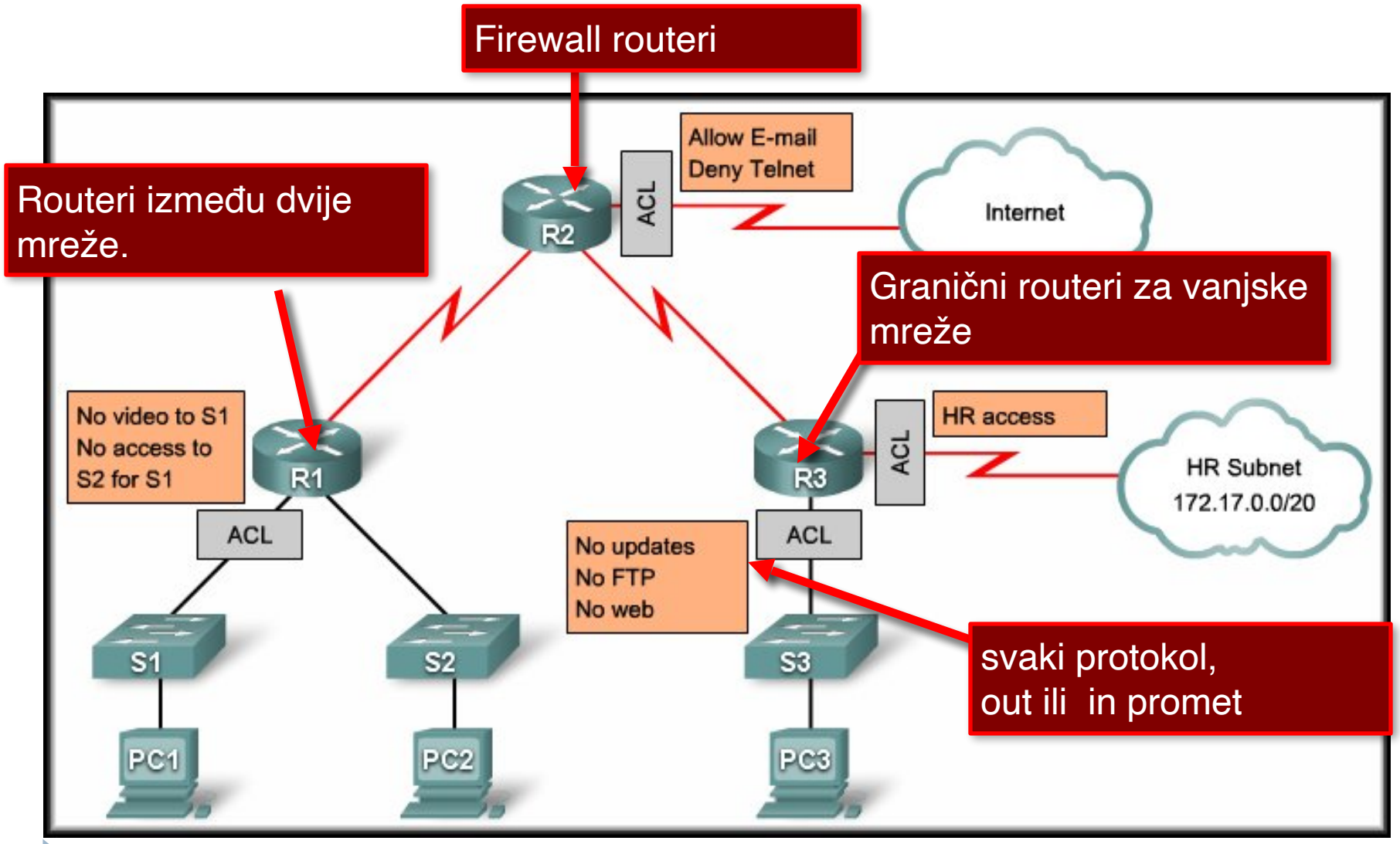
Višeznačne maske

- Višeznačne maske (engl. wildcard mask) - 32bitne vrijednosti
- inverzija subnet maske
- Pojedini bitovi određuju uzimaju li se odgovarajući bitovi IP adrese u obzir prilikom odluke o primjeni ACL unosa na promet s ili prema toj adresi
- npr. za 0.0.0.255 pravila filtriranja ACL liste primjenjuju na sve adrese čijih se gornjih 24 bita (gornja tri okteta) poklapaju s adresama u ACL unosima
  - Vrijednost donjeg okteta nije bitan (eng. don't care).

Primjer formiranja ACL



Primjer formiranja ACL



Stvaranje ACL liste

- Router#config
- Router(config)# access-list *ACL_# {permit | deny} source_IP_address [wildcard_mask] [log]*

- ACL_# - broj liste koji može biti iz raspona 1 do 99 ili 1300 do 1999
- {permit | deny} - akcija koja se poduzima u slučaju zadovoljenja uvjeta (omogućavanje ili onemogućavanje zatražene radnje)
- source_IP_address - izvorišna IP adresa
- [wildcard_mask] - višeznačna maska, ovaj parametar nije nužan
- [log] - posljednji parametar određuje stvara li se u slučaju zadovoljenja uvjeta dnevnički zapis

Vrste ACL:

- Standardna ACL – omogućavaju dozvolu ili zabranu prometa sa ishodišne IP adrese

- Primjer:
  - access-list 10 permit 192.168.30.0 0.0.0.255
  - omogućava sav promet sa mreže 192.168.30.0/24

- Važno: Premda to nije izričito navedeno podrazumijeva se da je sav drugi promet blokiran tom ACL (tzv.implicite deny any).

- Proširena ACL sadrži:
  - ishodišnu i odredišnu IP adresu
  - ishodišni i odredišni TCP/UDP port
  - vrstu ili broj protokola (za HTTP = 80)

- Primjer
  - access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
  - dopušta tcp promet s mreže 192.168.30.0/24 na odredišni port 80 (web)

ACL se numeriraju na slijedeći način:

- (1 do 99) i (1300 do 1999) - Standardne ACL
- (100 do 199) i (2000 do 2699) - Proširene ACL

- također se mogu i imenovati

- Osnovna pravila za razmještaj ACL:
  - Standardne ACL smjestiti što bliže odredištu
  - Proširene ACL smjestiti što bliže ishodištu prometa

Poništavanje ACL:

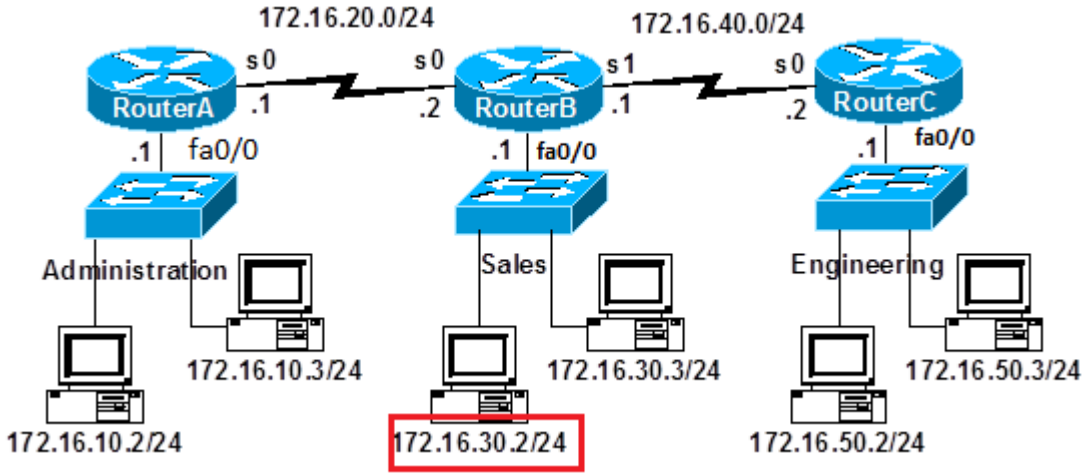
Router(config)#no access-list 10

Vježba - wildcard maska

```
RouterB(config)#access-list 10 permit  ?   ?
```

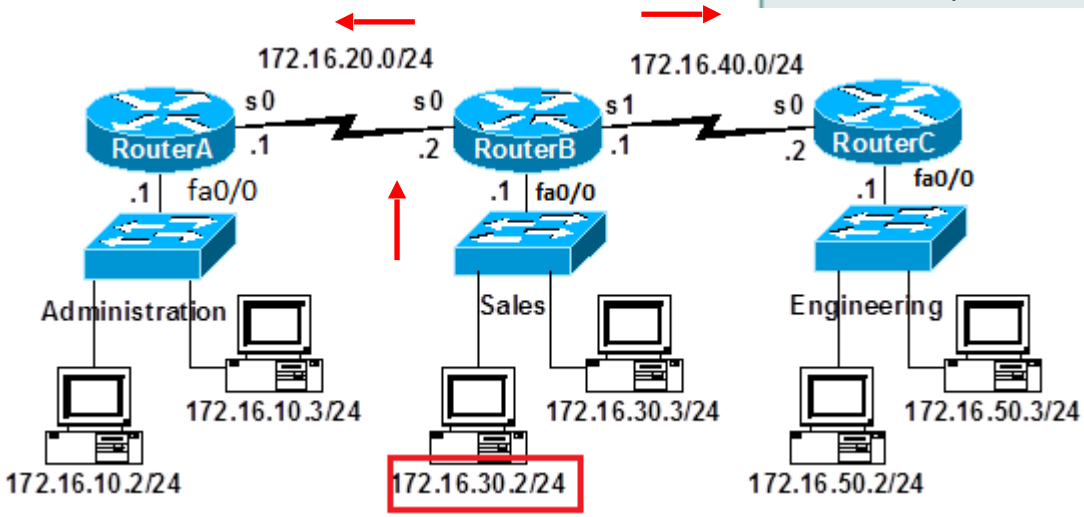
	Dopusti slijedeće mreže:	Adresa/wildcard maska
A	172.16.0.0 255.255.0.0	172.16.0.0 0.0.255.255
B	172.16.1.0 255.255.255.0	172.16.1.0 0.0.0.255
C	192.168.1.0 255.255.255.0	192.168.1.0 0.0.0.255
D	172.16.16.0 255.255.240.0	172.16.16.0 0.0.15.255
E	172.16.128.0 255.255.192.0	172.16.128.0 0.0.63.255
	Dopusti slijedeće hostove	
A	172.16.10.100	172.16.10.100 0.0.0.0
B	192.168.1.100	192.168.1.100 0.0.0.0
C	svi hostovi	0.0.0.0 255.255.255.255

Uči i riješi!



- Zadatak – kreiraj standardnu ACL uz uvjete:
  - Samo host 172.16.30.2 iz prodaje smije preko routera B izaći dalje u mrežu.
  - Niti jedan drugi host iz prodajnog dijela ne smije izaći iz mreže 172.16.30.0/24.

Protocol		Range
IP	(Standard IP)	1-99



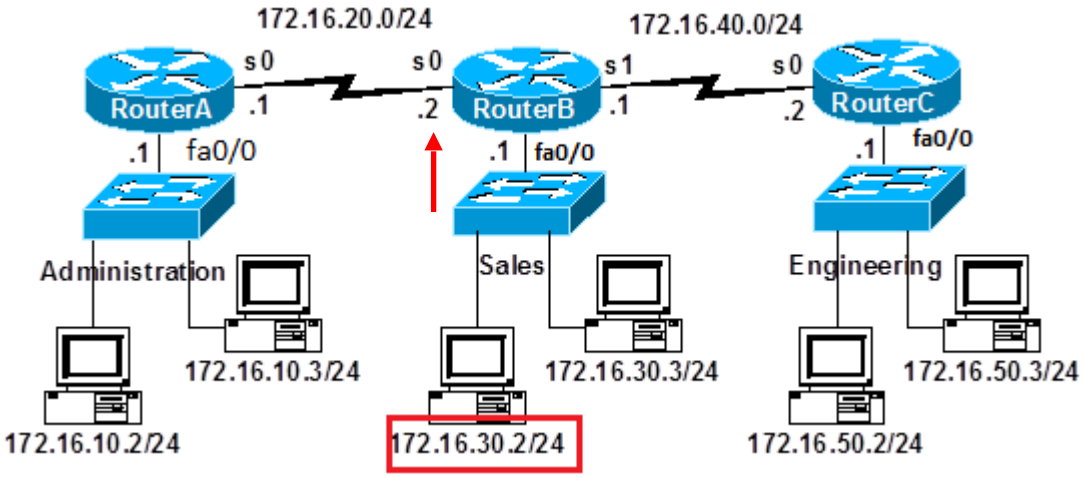
1. Korak : gdje je najbolje postaviti listu? Zašto?

```
Router(config)#access-list access-list-number
  {permit | deny} {test-conditions}
```

uvjet testiranja

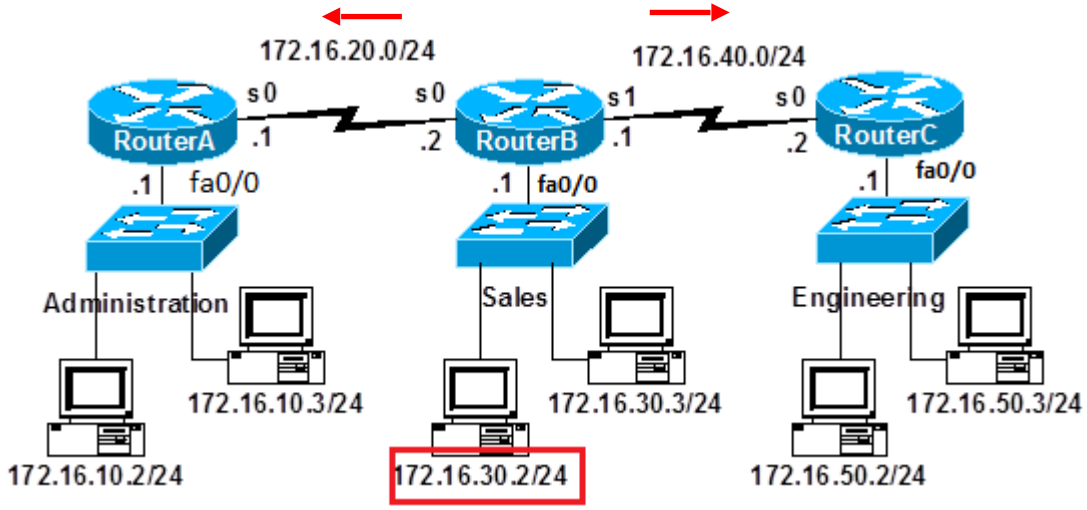
```
RouterB(config)#access-list 10 permit 172.16.30.2
Implicitni  "deny any" - postoji i ne treba pisati

RouterB(config)#access-list 10 deny 0.0.0.0 255.255.255.255
  - znači deny any - ne treba pisati
```

Postavljanje ACL na interface



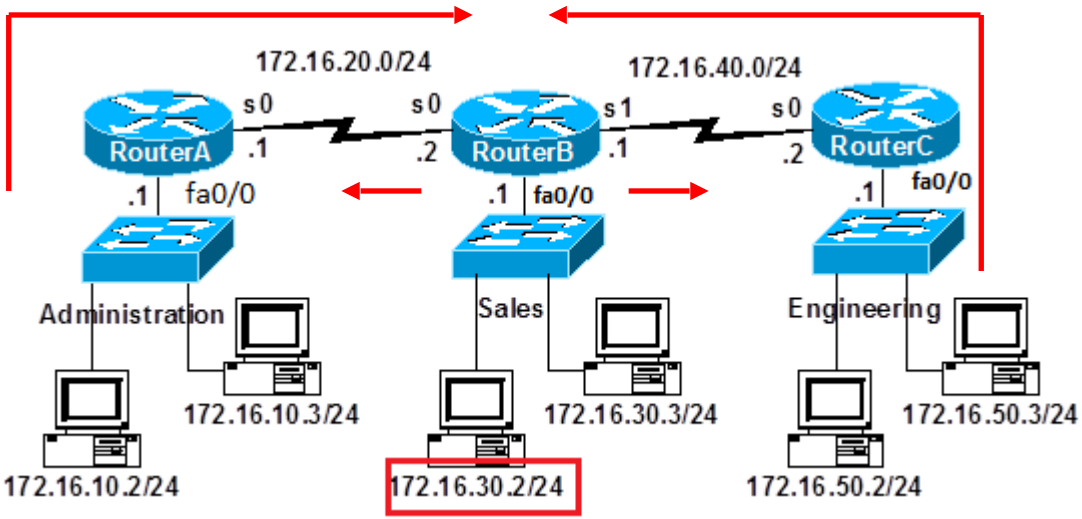

```
RouterB(config)#access-list 10 permit 172.16.30.2

RouterB(config)# interface fa0/0
RouterB(config-if)# ip access-group 10 in
```

Postavljanje liste na interface



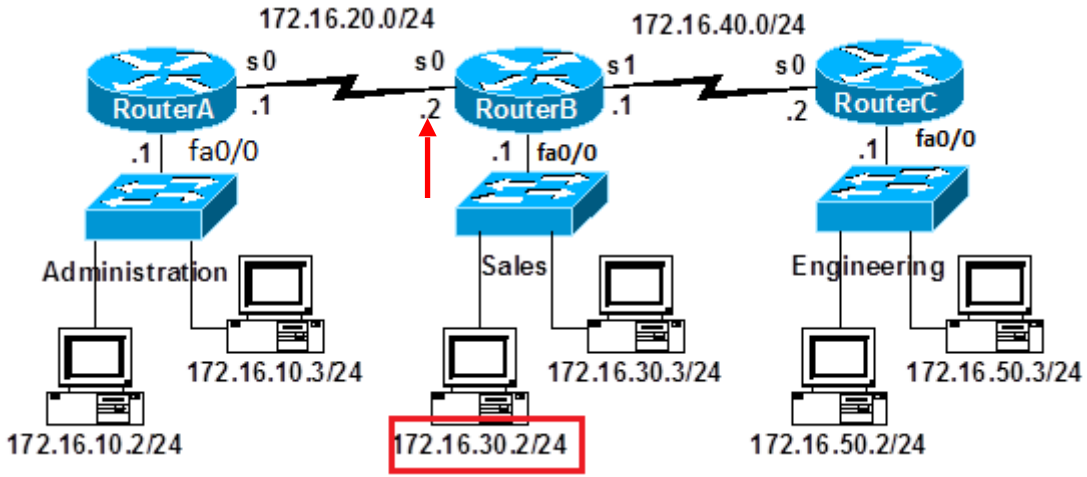
Ako ACL stavimo na izlazne interface

```
RouterB(config)#access-list 10 permit 172.16.30.2
RouterB(config)#access-list 10 deny 0.0.0.0 255.255.255.255
RouterB(config)# interface s 0
RouterB(config-if)# ip access-group 10 out
RouterB(config)# interface s 1
RouterB(config-if)# ip access-group 10 out
```



Zbog implicitnog deny any, ovako napisana lista brani i pakete iz Administracije prema Inženjeringu kao i pakete iz Inženjeringa u Administraciju .

```
RouterB(config)#access-list 10 permit 172.16.30.2
RouterB(config)#access-list 10 deny 0.0.0.0
  255.255.255.255 - deny any
RouterB(config)# interface s 0
RouterB(config-if)# ip access-group 10 out
RouterB(config)# interface s 1
RouterB(config-if)# ip access-group 10 out
```



Bolje je ACL postaviti na fa0/0 na routeru B

```
RouterB(config)#access-list 10 permit
  172.16.30.2
RouterB(config)#access-list 10 deny 0.0.0.0
  255.255.255.255 –deny any

RouterB(config)# interface fa0/0
RouterB(config-if)# ip access-group 10 in
```

Kreiranje ACLs

- Osnovna pravila
  - jedna lista po protokolu i po smjeru
  - **standard** ACL treba biti što bliže **cilju**
  - **proširena (extended)** ACL treba biti što bliže **izvoru**
  - **Filtriranje** mora ići od **određenijeg** prema **općenitijem**
  - **pažljivo !!!** s dodavanjem uvjeta ili brisanjem lista