

ACCESS CONTROL LISTS

Dr Dušan Stefanović CCNA, CCNA Security,CCNP

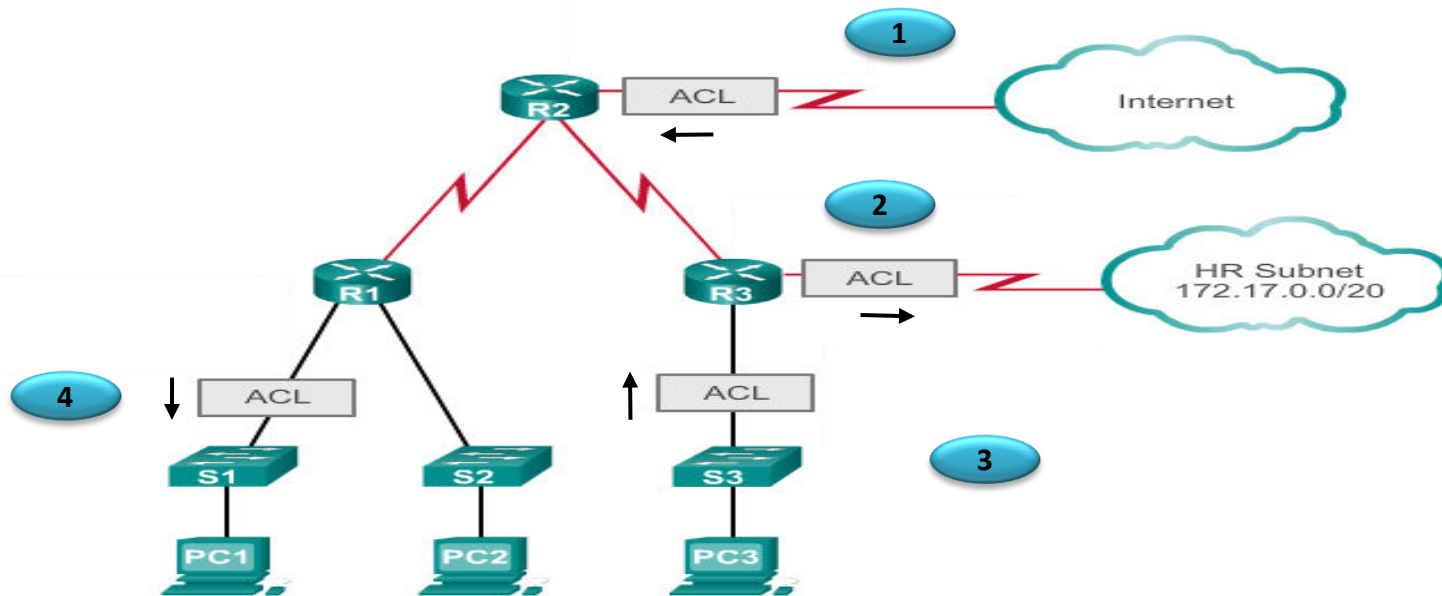


ECDL
European Computer
Driving Licence



ETS AUTHORIZED
TOEFL iBT CENTER

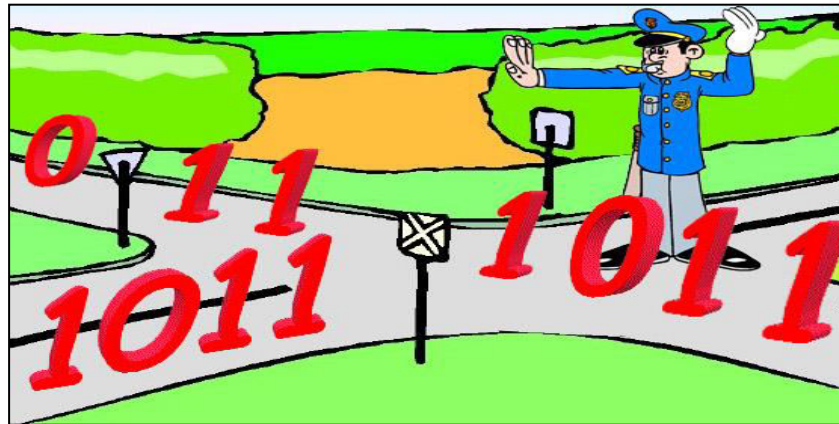
ACCESS CONTROL LISTS (ACL)



- Podrazumevano, ruter ne filtrira saobraćaj.
- Kada se ACL primeni na interfejs:
 - nadgleda mrežni saobraćaj
 - određuje da li paket može da se prosledi (filtrira saobraćaj)

ACCESS CONTROL LISTS (ACL)

- Ruter na osnovu pravila (filter rules) može da prosleđuje(permit) ili odbacuje(deny) pakete.
 - Filtriranjem paketa kontroliše se pristup mreži:
 - analiziraju se dolazni(incoming) i odlazni(outgoing) paketi
 - propuštaju se ili odbacuju paketi na osnovu definisanog kriterijuma
- ACL je lista sastavljena od **permit** ili **deny** iskaza, koji su poznati kao **access control entries (ACEs)** ili **ACL** iskazi



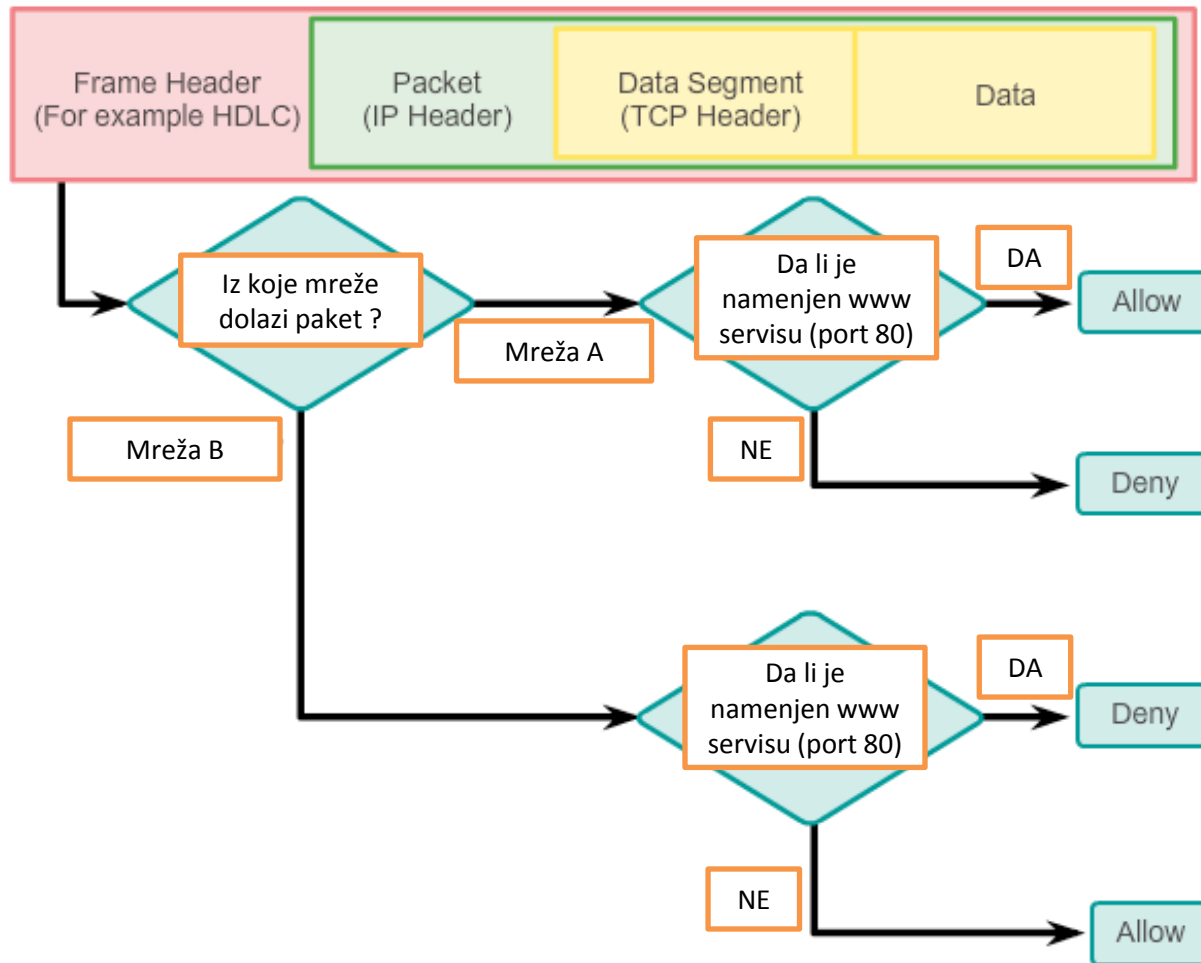
FILTRIRANJE PAKETA

- ACL određuje da li će ruter dozvoliti ili zabraniti dalje prosleđivanje paketa na osnovu sledećih kriterijuma:
 - **Izvorišna (source) IP adresa**
 - **Odredišna (destination) IP adresa**
 - **IP protokola (ICMP, TCP, UDP, EIGRP, ...)**
 - **TCP/UDP izvorišni port**
 - **TCP/UDP odredišni port**
- Filtriranje paketa izvršava se na Sloju 3 (Network) i sloju 4 (Transport)

Packet filtering works at Layer 3 and Layer 4



PAKET FILTERING PRIMER



ACCESS CONTROL LISTS (ACL)



Dolazna (inbound) ACL filtrira pakete koji dolaze na definisani interfejs i pre nego što su paketi rutirani na izlazni (outbound) interfejs

Odlazna (outbound) ACL filtrira pakete koji su prošli kroz rutingu tabelu

VRSTE ACL

● Standardne ACL

- Mogu da dozvole (**permit**) ili zabrane(**deny**) saobraćaj gledajući samo Izvorišnu(Source) IP adresu!

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

● Extended ACL

- Mogu da dozvole(**permit**) ili zabrane(**deny**) saobraćaj za:
 - Tip protokola (IP, ICMP, EIGRP, OSPF, TCP, UDP, ...)
 - Izvorišna IP adresa
 - Izvorišni TCP ili UDP portovi
 - Odredišna IP adresa
 - Odredišni TCP ili UDP portovi

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```



ECDL
European Computer
Driving Licence



ETS AUTHORIZED
TOEFL iBT CENTER

IMENOVANE I NEIMENOVANE ACL

Numbered ACL:

Broj identifikuje tip ACL
(1 – 99) i (1300 i 1999): Standard IP ACL
(100 – 199) i (2000 i 2699): Extended IP ACL

Named ACL:

- ACL lista se identifikuje na osnovu imena
- Ime sadrži alfanumeričke karaktere
 - Predlaže se da ime sadrži velika slova
 - Nesme da sadrži razmak
 - Unosi mogu naknadno da se brišu i dodaju



WILDCARD MASK

- Standard i Extended ACL obe koriste wildcard mask-u.
 - Wildcard mask i subnet maska se razlikuju na način na koji mečuju binarnu 1 i binarnu 0.
- Wildcard mask-a koristi sledeća pravila kojim se mečuje binarna 0 i binarna 1:
 - Wildcard mask bit 0 - Match odgovarajuću bit vrednost u adresi
 - Wildcard mask bit 1 - Ignore odgovarajuću bit vrednost u adresi



ODREĐIVANJE WILDCARD MASKE

- Želimo da dozvolimo pristup svim korisnicima u mreži 192.168.3.0 /24
 - Oduzme se subnet maska (255.255.255.0) od subnet maske 255.255.255.255.

$$\begin{array}{r} 255.255.255.255 \\ - \underline{255.255.255.000} \\ \hline 000.000.000.255 \end{array}$$

```
access-list 1 permit 192.168.3.0 0.0.0.255
```



ECDL
European Computer
Driving Licence



ETS AUTHORIZED
TOEFL iBT CENTER

ODREĐIVANJE WILDCARD MASKE

- Želimo da dozvolimo pristup svim korisnicima u mreži 192.168.3.32 /28
 - Oduzme se subnet maska (255.255.255.240) od subnet maske 255.255.255.255

$$\begin{array}{r} 255.255.255.255 \\ -255.255.255.240 \\ \hline 000.000.000.15 \end{array}$$

```
access-list 1 permit 192.168.3.32 0.0.0.15
```



ECDL
European Computer
Driving Licence



ETS AUTHORIZED
TOEFL iBT CENTER

ACCESS CONTROL LISTS (ACL)

```
access-list 1 permit 192.168.1.1 0.0.0.0
```

	Dekadni prikaz	Binarni prikaz
IP Adresa	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.0	00000000.00000000.00000000.00000000
Rezultat	192.168.1.1	11000000.10101000.00000001.00000001

- **Host** ključna reč može se koristiti za zamenu 0.0.0.0 wildcard maske.
 - Ova maska označava da svi biti u IPv4 adresi moraju da se mečuju tj. jedan host se samo mečuje

```
access-list 1 permit host 192.168.1.1
```



ECDL
European Computer
Driving Licence



ETS AUTHORIZED
TOEFL iBT CENTER

ACCESS CONTROL LISTS (ACL)

```
access-list 1 permit 0.0.0.0 255.255.255.255
```

	Dekadni prikaz	Binarni prikaz
IP Adresa	0.0.0.0	00000000.00000000.00000000.00000000
Wildcard Maska	255.255.255.255	11111111.11111111.11111111.11111111
Rezultat	0.0.0.0	00000000.00000000.00000000.00000000

- **Any** ključna reč može da se koristi za zamenu 255.255.255.255 wildcard maske.
 - Ova maska označava da ni jedan bit u IPv4 adresi ne mora da se mečuje.

```
access-list 1 permit any
```



PRIMENA ACL

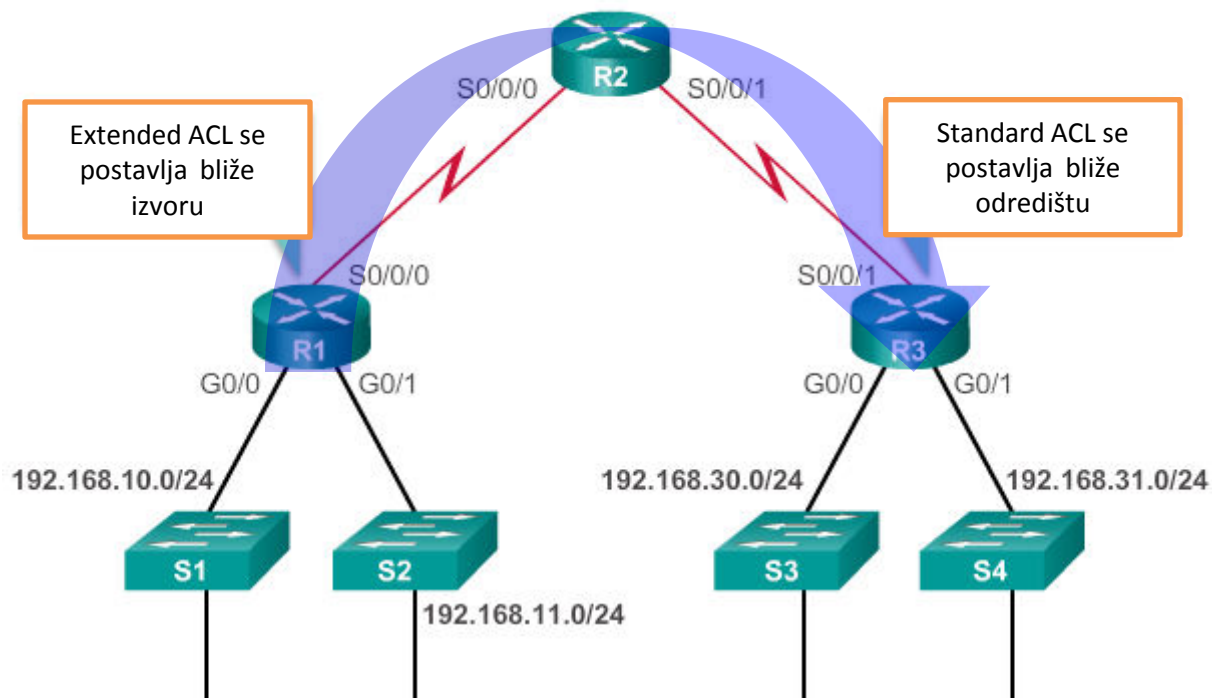


Jedna ACL lista po interfejsu, smeru i protokolu

Na dva interfejsa i dva Layer 3 protokola, mogu da se konfigurisu 8 nezavisnih ACL lista

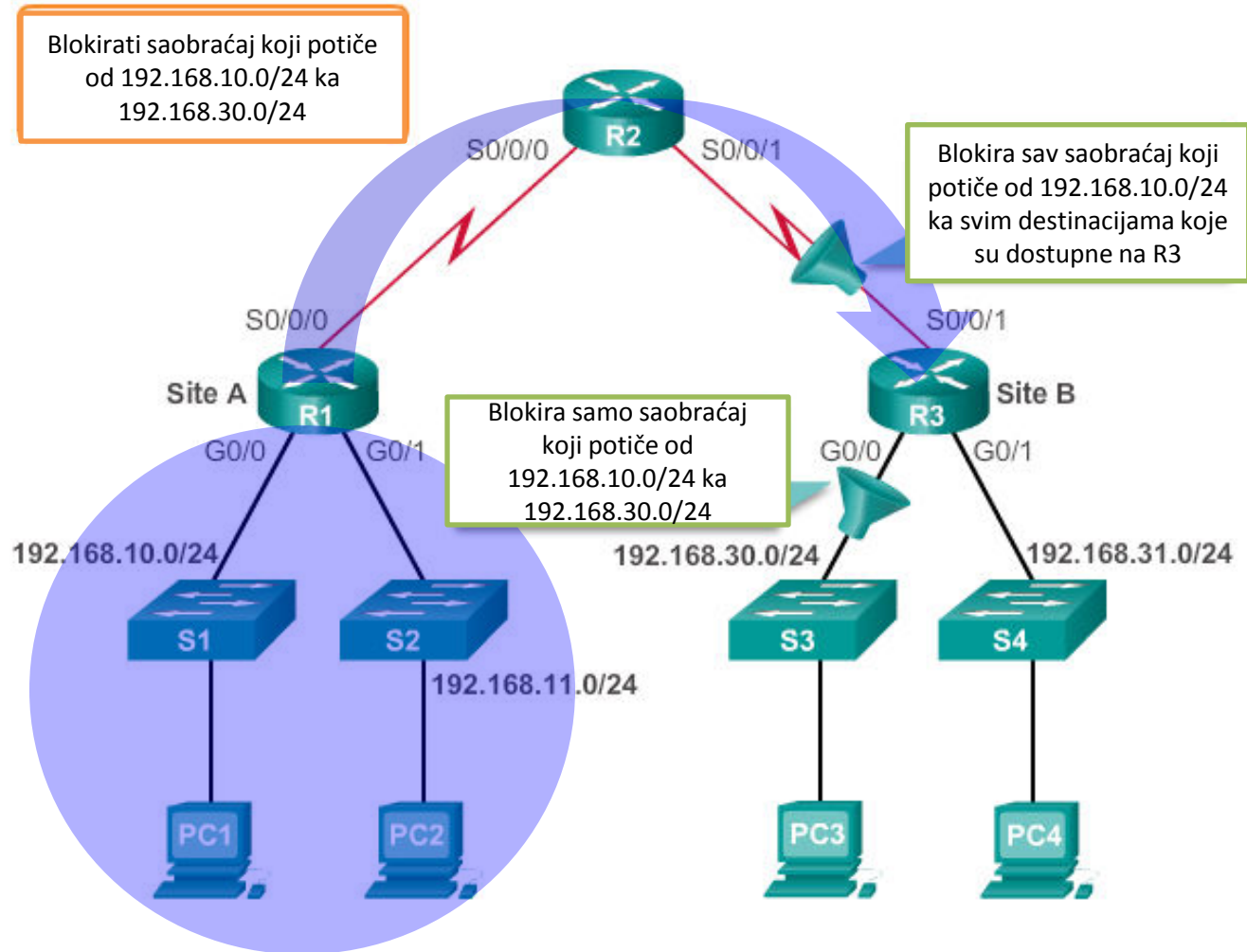
Jedna ACL lista po protokolu (IPv4 ili IPv6)
Jedna ACL lista po smeru (IN ili OUT)
Jedna ACL lista po interfejsu (FastEthernet 0/0)

ACCESS CONTROL LISTS (ACL)

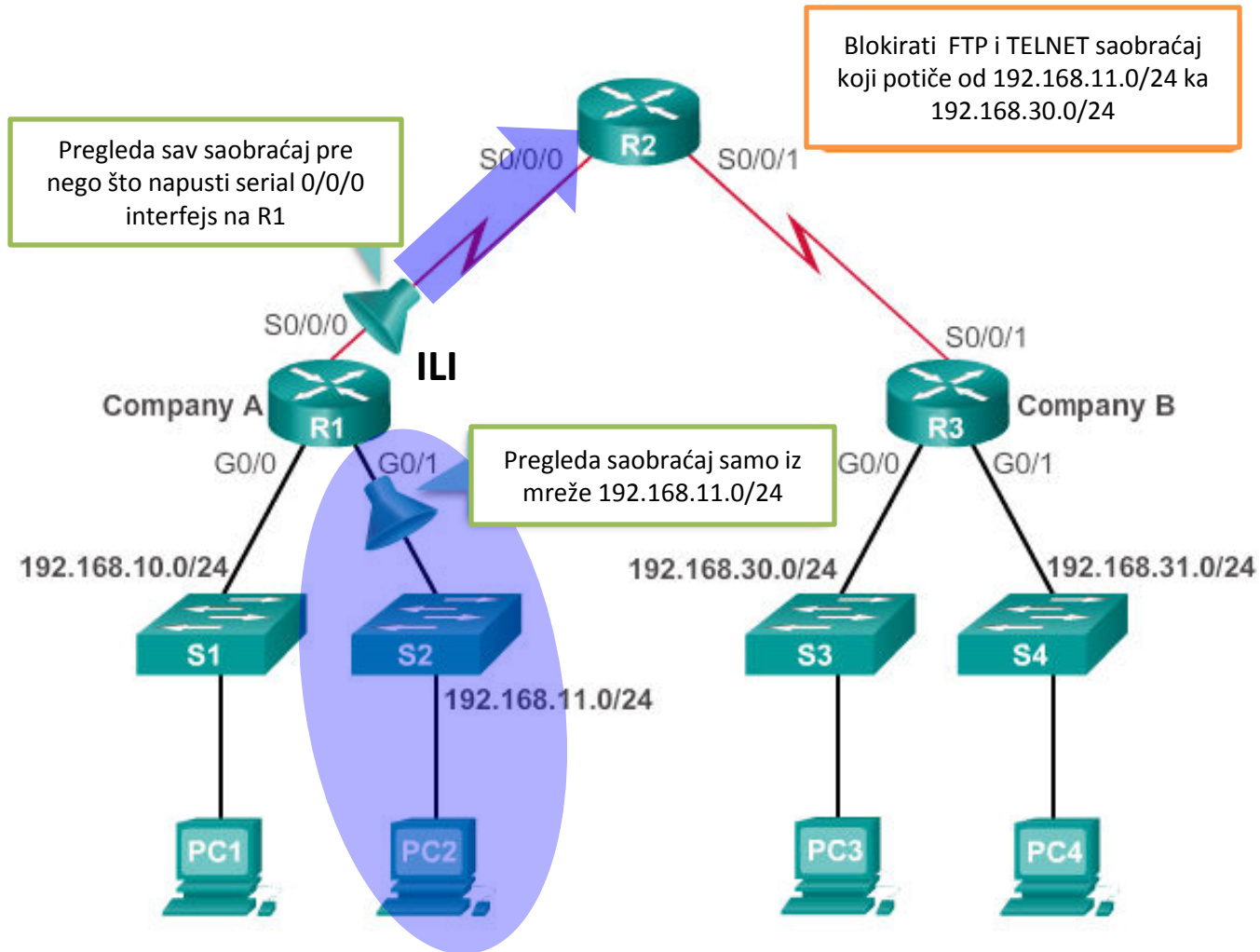


- **Extended ACL** – Neželjeni saobraćaj se filtrira što bliže izvorišnoj mreži.
- **Standard ACLs** - Neželjeni saobraćaj se filtrira što bliže odredišnoj mreži, jer sadrži samo izvorišnu adresu.

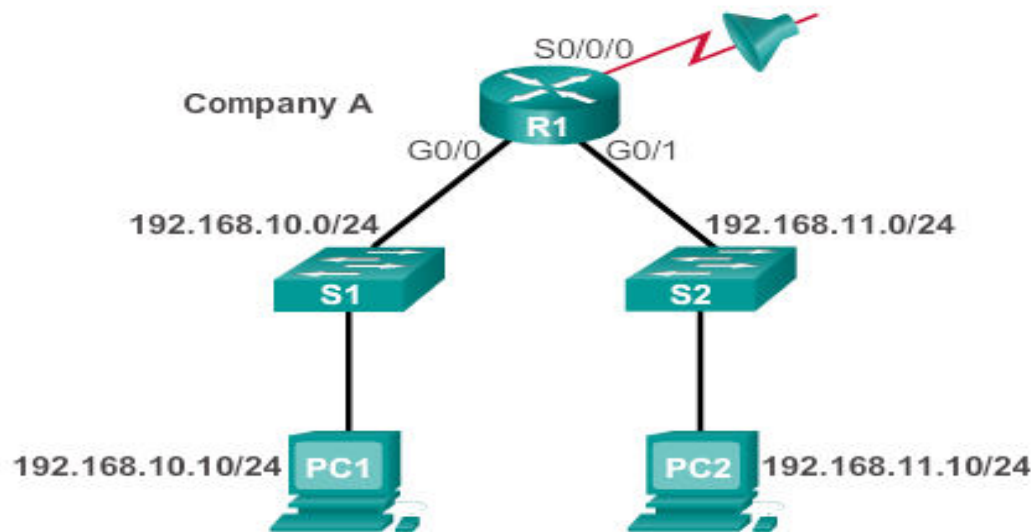
STANDARDNA ACL PRIMENA



EXTENDED ACL PRIMENA



KORACI U KREIRANJU ACL



1. Kreiranje ACL liste.

- Iz globalnog konfiguracionog moda dodajemo iskaze na osnovu kojih se sprovodi filtriranje.

2. Primena ACL liste na interfejs.

- Mod za konfiguraciju interfejsa.
- Identifikacija ACL liste i smer u kome se radi filtriranje.

KREIRANJE STANDARDNE ACL

```
RTR(config)# access-list ACL# {permit|deny} {test-conditions }  
access-list    5    permit    172.34.54.34 0.0.0.0
```

ACL-# je jedinstven identifikator. Broj identifikuje vrstu ACL liste.

permit | **deny** su termini na osnovu kojih se paket koji odgovara tom unosu odbacuje ili prosleđuje.

permit: paket se ne filtrira.

deny: paket se filtrira.

remark: unos komentara za ACL listu



PRIMENA ACL LISTE NA INTERFEJS

```
RTR(config-if)# {protocol} access-group list-# {in|out}
```

```
ip access-group 5 out
```

- **in** | **out** definiše da li je ACL za dolazni ili odlazni saobraćaj.
 - **in** znači da se paket pregleda čim stigne na interfejs, pre odluke o rutiranju.
 - **out** znači da se paket pregleda pre nego što napusti interfejs, nakon odluke o rutiranju.
- “**out**” je podrazumevana vrednost.
 - Outbound ACL je efikasnija i preporučuje se.
 - Inbound ACL proverava svaki paket.

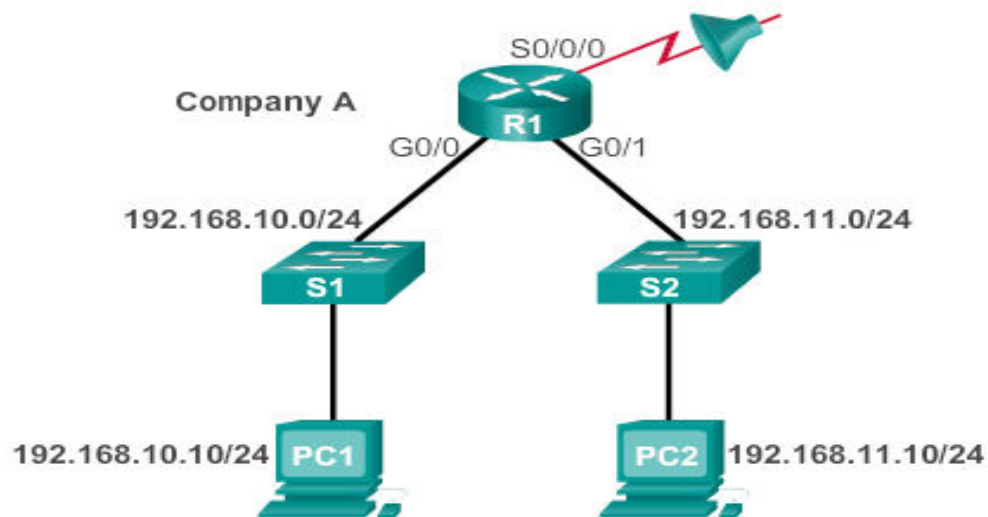


ECDL
European Computer
Driving Licence



ETS AUTHORIZED
TOEFL iBT CENTER

IMPLICITNA ZABRANA



Podrazumevano, na kraju svake ACL liste je implicitna zabrana (**implied deny**). Svaki paket koji se ne mećuje u definisanom iskazu biće odbaćen

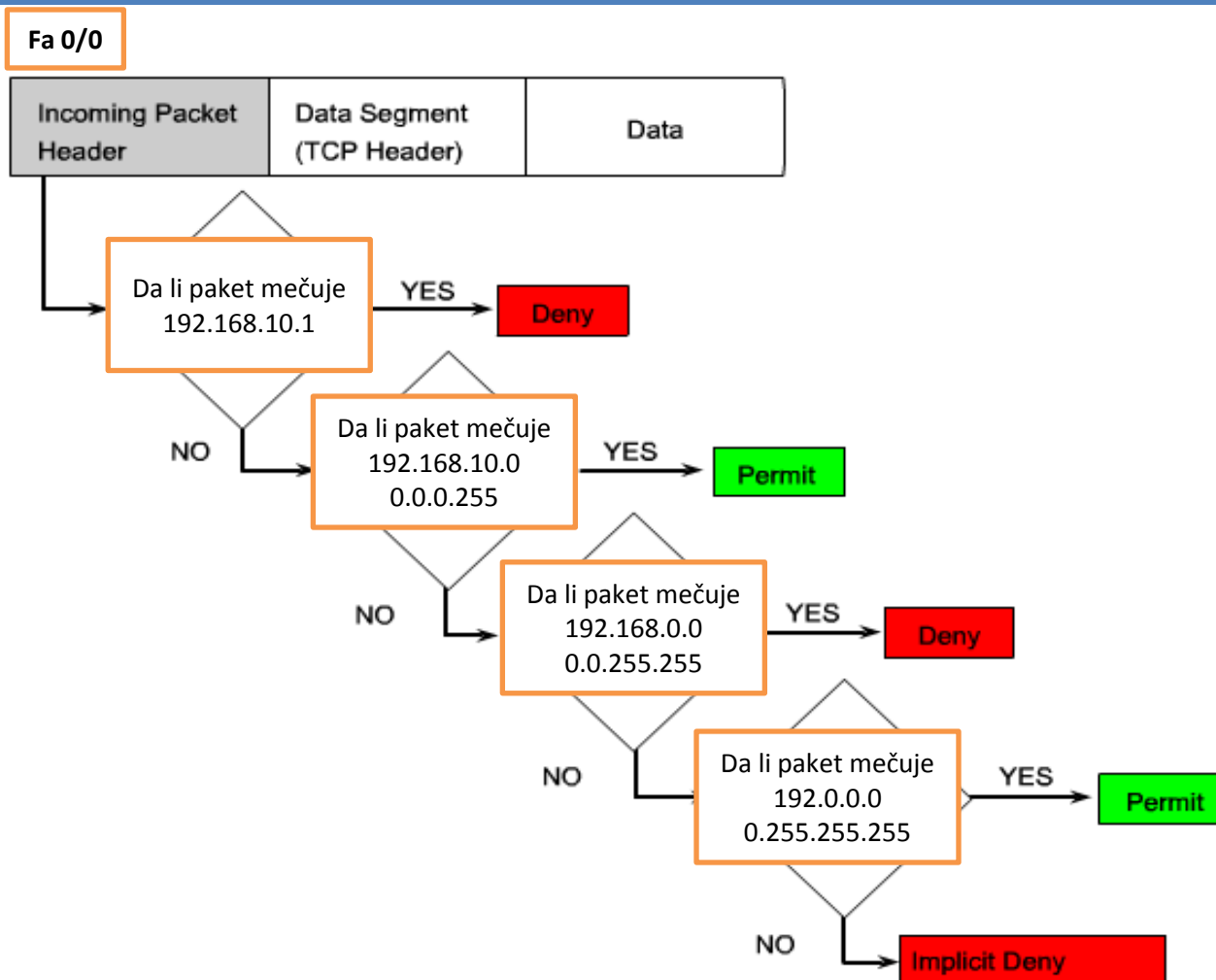
```
R1 (config) # access-list 1 permit ip 192.168.10.0 0.0.0.255
```

ili

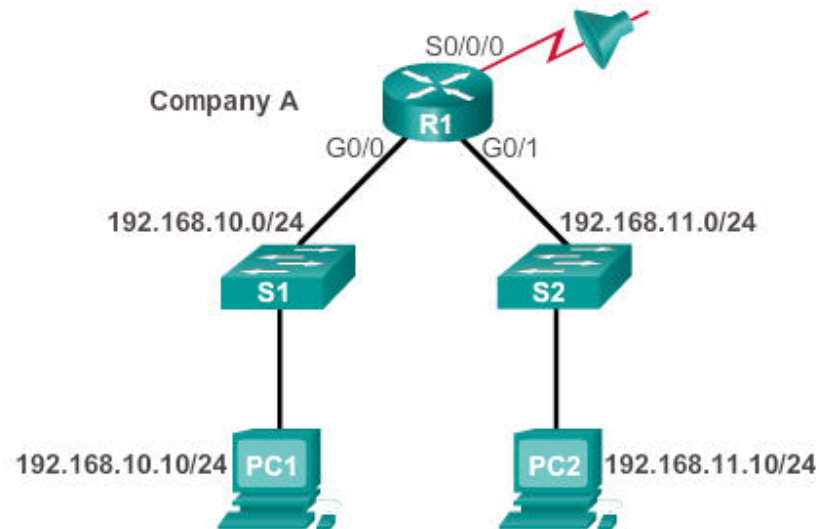
```
R1 (config) # access-list 2 permit ip 192.168.10.0 0.0.0.255
```

```
R1 (config) # access-list 2 deny any
```

ALGORITAM RADA STANDARDNE ACL LISTE

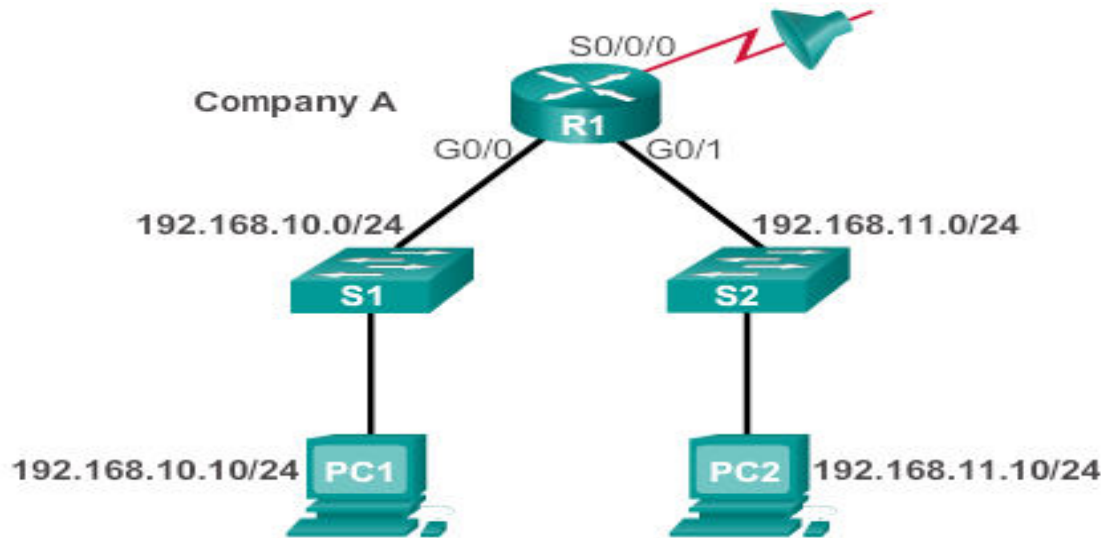


UKLANJANJE ACL LISTE



```
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)# exit
R1# show access-lists
Standard IP access list 10
    10 permit 192.168.10.0, wildcard bits 0.0.0.255
R1# conf t
R1(config)# no access-list 10
```

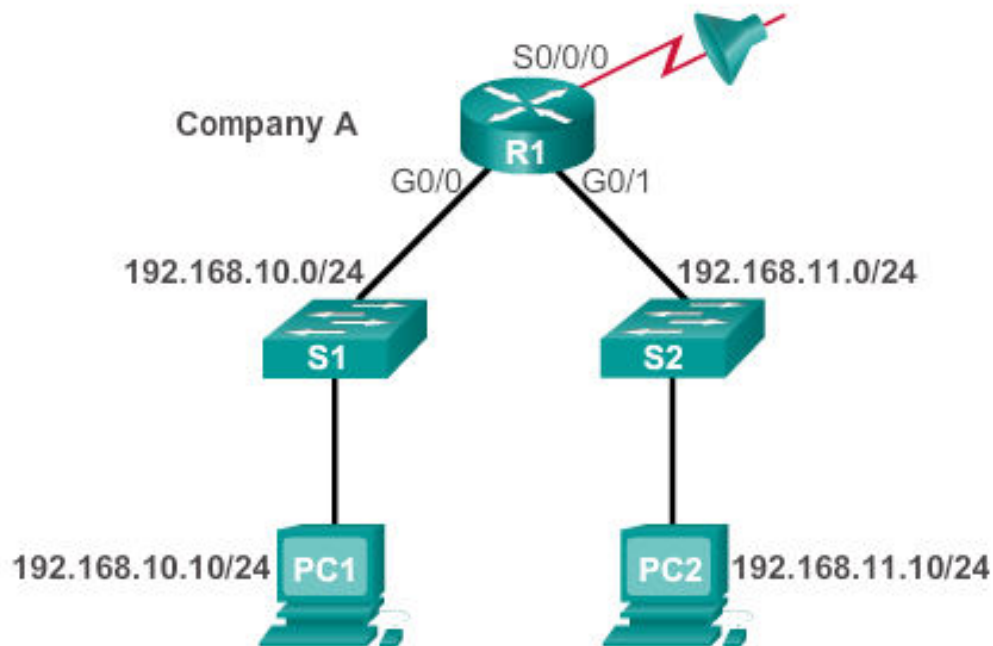
Komentari - remark



```
R1(config)# access-list 10 remark Permit hosts from the 192.168.10.0 LAN
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)# exit
```

```
R1# show running-config | include access-list 10
access-list 10 remark Permit hosts from the 192.168.10.0 LAN
access-list 10 permit 192.168.10.0 0.0.0.255
```

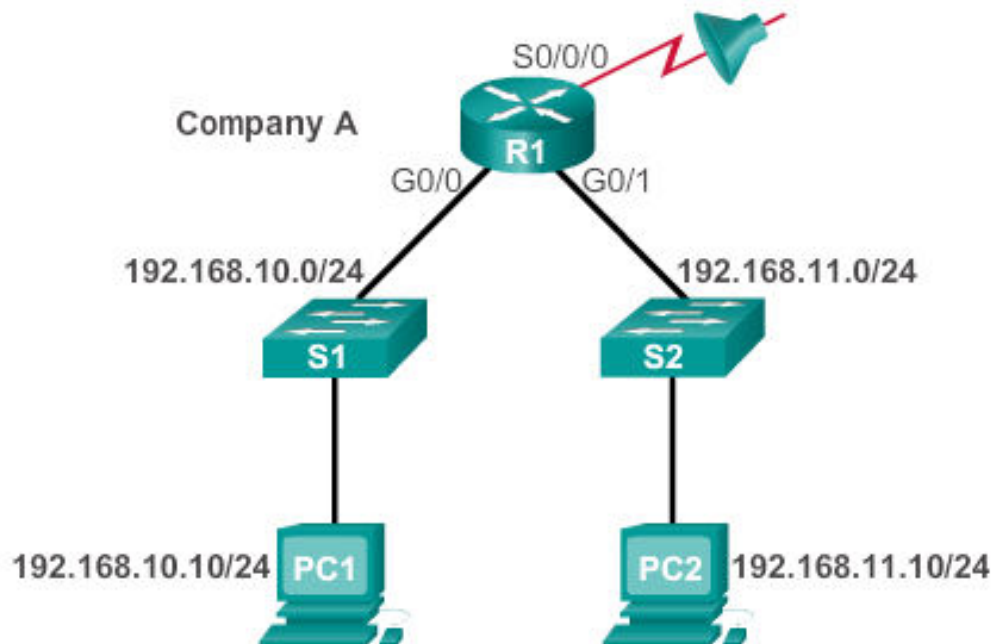

REDOSLED IZVRŠENJA ISKAZA



ACL 3: Host iskaz je u konfliktu sa prethodnim iskazom

```
R1 (config) # access-list 3 deny 192.168.10.0 0.0.0.255  
R1 (config) # access-list 3 permit host 192.168.10.10
```

REDOSLED IZVRŠENJA ISKAZA



Preporuka: Prvo se unese određeniji tj. specifičniji iskazi

```
R1 (config) # access-list 4 permit host 192.168.10.10  
R1 (config) # access-list 4 deny 192.168.10.0 0.0.0.255  
R1 (config) #
```

PRIMENA ACL LISTE

Korak 1: Konfiguracija ACL liste

```
R1 (config) # access-list 1 permit 192.168.10.0 0.0.0.255
```

Korak 2: Izbor interfejsa na kome se primenjuje ACL

```
R1 (config) # interface serial 0/0/0
```

Korak 3: Primena ACL na interfejs

```
R1 (config-if) # ip access-group 1 out
```

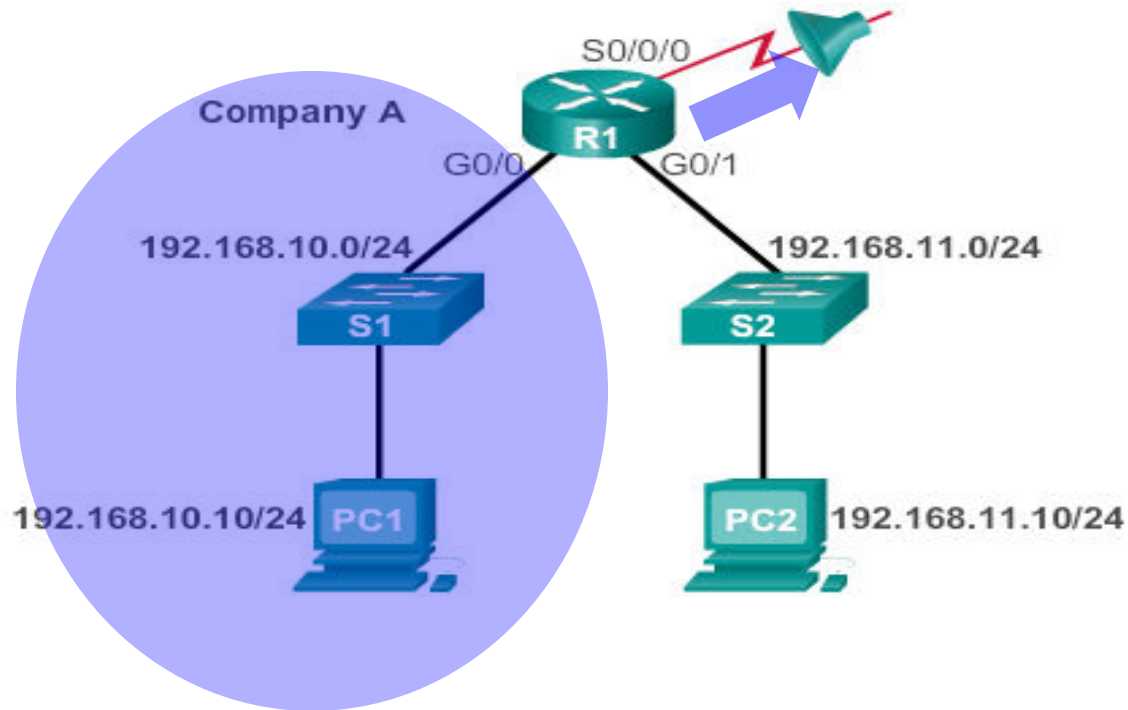


ECDL
European Computer
Driving Licence



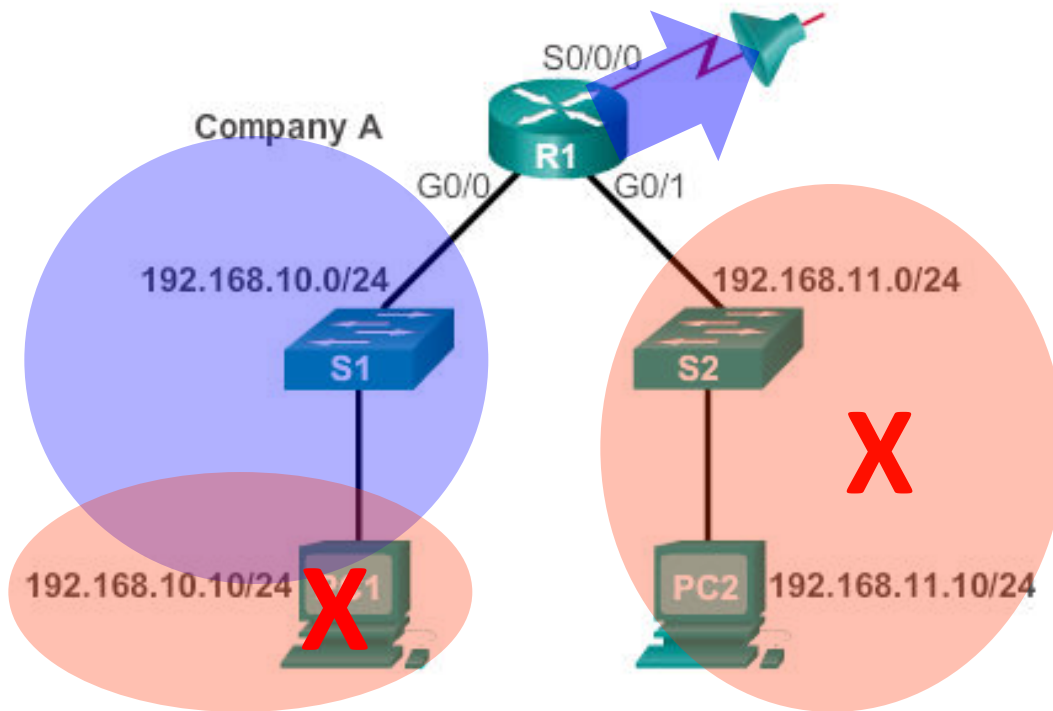
ETS AUTHORIZED
TOEFL iBT CENTER

PRIMER 1



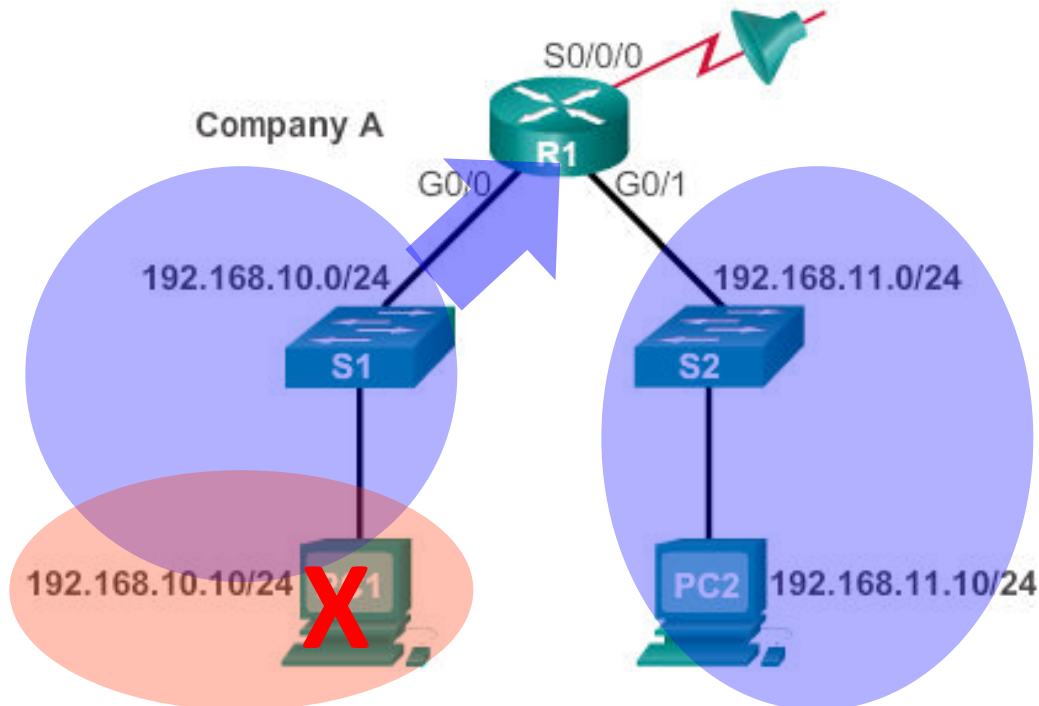
```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255  
R1(config)# interface s0/0/0  
R1(config-if)# ip access-group 1 out
```

PRIMER 2



```
R1 (config) # access-list 1 deny host 192.168.10.10  
R1 (config) # access-list 1 permit 192.168.10.0 0.0.0.255  
R1 (config) # interface s0/0/0  
R1 (config-if) # ip access-group 1 out
```

PRIMER 3



```
R1 (config) # access-list 1 deny host 192.168.10.10  
R1 (config) # access-list 1 permit any  
R1 (config) # interface g0/0  
R1 (config-if) # ip access-group 1 in
```

IMENOVANA ACL

```
Router(config)# ip access-list [standard | extended] name
```

Naziv imenovane ACL liste mora da bude jedinstveno na ruteru i ne može da počne brojem

```
Router(config-std-nacl)# [permit | deny | remark] {source  
[source-wildcard]} [log]
```

```
Router(config-if)# ip access-group name [in | out]
```



ECDL
European Computer
Driving Licence



ETS AUTHORIZED
TOEFL iBT CENTER

ACCESS CONTROL LISTS (ACL)

PRIMER 1 – Neimenovana ACL

```
R1 (config) # access-list 1 remark Ne dozvoli guest radne stanice
R1 (config) # access-list 1 deny host 192.168.10.10
R1 (config) # access-list 1 remark Dozvoli ostale uredaje iz 192.168.x.x mreža
R1 (config) # access-list 1 permit 192.168.0.0 0.0.255.255
R1 (config) # interface s0/0/0
R1 (config-if) # ip access-group 1 out
R1 (config-if) #
```

PRIMER 2 – Imenovana ACL

```
R1 (config) # ip access-list standard NO_ACCESS
R1 (config-std-nacl) # remark Ne dozvoli pristup sa LAB radne stanice
R1 (config-std-nacl) # deny host 192.168.11.10
R1 (config-std-nacl) # remark Dozvoli pristup sa ostalih uredaja
R1 (config-std-nacl) # permit any
R1 (config-std-nacl) # interface G0/0
R1 (config-if) # ip access-group NO_ACCESS out
R1 (config-if) #
```



ECDL
European Computer
Driving Licence



ETS AUTHORIZED
TOEFL iBT CENTER

MODIFIKACIJA NEIMENOVANE ACL

Konfiguracija

```
R1 (config) # access-list 1 deny host 192.168.10.99  
R1 (config) # access-list 1 permit 192.168.0.0 0.0.255.255
```

Korak 1

```
R1# show access-lists 1  
Standard IP access list 1  
    10 deny    192.168.10.99  
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
```

Korak 2

```
R1 (config) # ip access-list standard 1  
R1 (config-std-nacl) # no 10  
R1 (config-std-nacl) # 10 deny host 192.168.10.10  
R1 (config-std-nacl) # end
```

Korak 3

```
R1# show access-lists  
Standard IP access list 1  
    10 deny    192.168.10.10  
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
```



MODIFIKACIJA IMENOVANE ACL

```
R1# show access-lists
```

```
Standard IP access list NO_ACCESS
```

```
10 deny 192.168.11.10
```

```
20 permit 192.168.11.0, wildcard bits 0.0.0.255
```

```
R1(config)# ip access-list standard NO_ACCESS
```

```
R1(config-std-nacl)# 15 deny host 192.168.11.11
```

```
R1# show access-lists
```

```
Standard IP access list NO_ACCESS
```

```
10 deny 192.168.11.10
```

```
15 deny 192.168.11.11
```

```
20 permit 192.168.11.0, wildcard bits 0.0.0.255
```



VERIFIKACIJA ACL

```
R1# show ip interface g0/0
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.10.1/24
<output omitted>
  Outgoing access list is NO_ACCESS
  Inbound access list is not set
<output omitted>
```

```
R1# show access-lists
Standard IP access list NO_ACCESS
  15 deny    192.168.11.11
  10 deny    192.168.11.10
  20 permit  192.168.11.0, wildcard bits 0.0.0.255
R1#
```



ACL STATISTIKA

```
R1#show access-lists
```

```
Standard IP access list 1
```

```
10 deny 192.168.10.10 (8 match(es))
```

```
20 permit 192.168.0.0, wildcard bits 0.0.255.255
```

```
Standard IP access list NO_ACCESS
```

```
15 deny 192.168.11.11
```

```
10 deny 192.168.11.10 (4 match(es))
```

```
20 permit 192.168.11.0, wildcard bits 0.0.0.255
```

```
R1#clear access-list counters 1
```

```
R1#show access-lists
```

```
Standard IP access list 1
```

```
10 deny 192.168.10.10
```

```
20 permit 192.168.0.0, wildcard bits 0.0.255.255
```

```
Standard IP access list NO_ACCESS
```

```
15 deny 192.168.11.11
```

```
10 deny 192.168.11.10 (4 match(es))
```

```
20 permit 192.168.11.0, wildcard bits 0.0.0.255
```

Brisanje broja
mečovanih paketa.

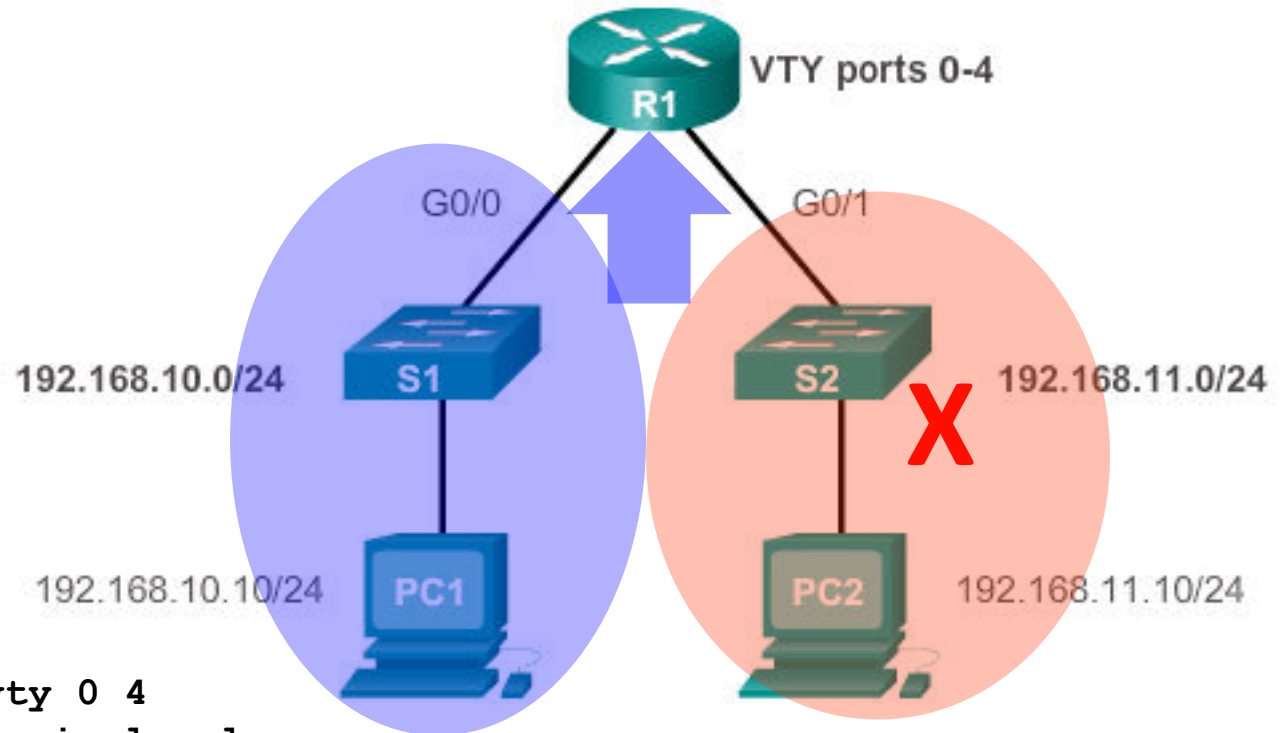


ECDL
European Computer
Driving Licence



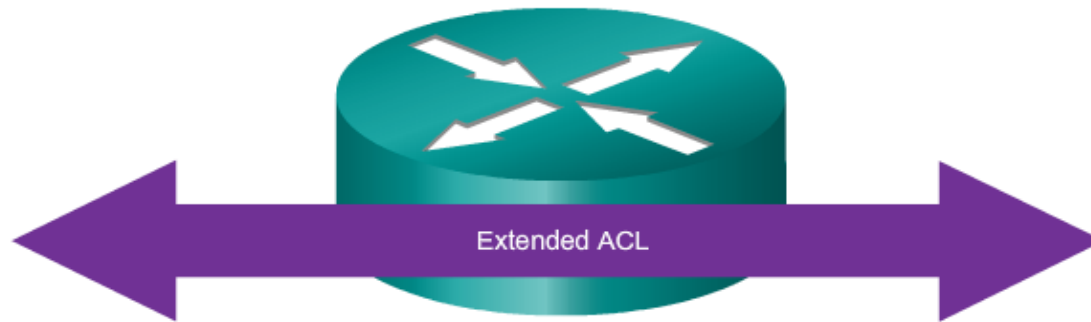
ETS AUTHORIZED
TOEFL iBT CENTER

BEZBEDAN PRISTUP PREKO VTY LINIJA



```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# access-class 21 in
R1(config-line)# exit
R1(config)# access-list 21 permit 192.168.10.0 0.0.0.255
R1(config)# access-list 21 deny any
```

EXTENDED ACL



Extended ACLs can filter on:

- IZVORIŠNA ADRESA
- ODREDIŠNA ADRESA
- PROTOKOL
- PORT

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

ACCESS CONTROL LISTS (ACL)

- Extended ACL se koriste češće od standardnih ACL jer obezbeđuju veći stepen kontrole nad podacima koje želimo da filtriramo.
- Extended ACL filtriranje radi na osnovu source i destination IP adrese.
- Ono što ih čini posebnim je filtriranje na osnovu protokola:
 - (IP, TCP, UDP, ICMP, EIGRP, ...)
 - Source port
 - Destination port



SINTAKSA EXTENDED ACL

Extended ACLs filtriranje vrši na osnovu **Protokola** i **Odredišne IP** adrese

Izbor **Protokola** dodaje različite opcije.

access-list	ist-#	permit deny remark	Protocol	Izvor		Odredište	
				IP	Wildcard	IP	Wildcard
	100-199		IP TCP UDP	any		any	
	2000 to 2699		ICMP EIGRP OSPF	host		host	

Opcije su različite u zavisnosti koji protokol je izabran.



Imena portova / Brojevi portova

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

Port/protokol nakon odredišne adrese
odnose se na odredišni port

- **Bitno:**

- Nemaju svi protokoli zadat naziv porta
- Broj porta uvek radi.
- SSH i HTTPS nemaju ime porta i zadaju se prema broju porta (22 and 443)



Extended IP ACL Primeri

- IP se odnosi na ceo protokolski stek, u tom slučaju brojevi portova ne mogu da se definišu.

```
access-list 101 permit ip any any
```

Dozvoljava sve pakete

```
access-list 101 deny ip any host 10.1.1.1
```

Filtrira sve pakete sa bilo koje odredišne adrese koji su namenjeni host-u 10.1.1.1.

```
access-list 101 deny ip host 10.1.1.1 any
```

Filtrira sve pakete sa host-a 10.1.1.1 ka bilo kojoj odredišnoj adresi



ECDL
European Computer
Driving Licence



ETS AUTHORIZED
TOEFL iBT CENTER

Extended TCP ACL Primeri

```
access-list 101 deny tcp any any eq telnet
```

Filtrira telnet saobraćaj sa bilo kog IP uređaja ka bilo kom IP uređaju.

```
access-list 101 deny tcp any host 10.1.1.1 eq 23
```

Zabranjuje telnet saobraćaj sa bilo kog izvora ka 10.1.1.1.

```
access-list 101 deny tcp any host 10.1.1.1 eq telnet
```



ECDL
European Computer
Driving Licence



ETS AUTHORIZED
TOEFL iBT CENTER

Extended TCP ACL Primeri

Port/protokol nakon izvorišne adrese odnosi se na izvorišni port

```
access-list 101 deny tcp any eq telnet any
```

Bilo kom TCP paketu kojem je source port 23 nije dozvoljen pristup bilo kom odredištu.

Port/protokol nakon odredišne adrese odnosi se na odredišni port

```
access-list 101 permit tcp 192.168.32.0 0.0.31.255 any eq 20  
access-list 101 permit tcp 192.168.32.0 0.0.31.255 any eq 21
```

FTP paketima iz mreža 192.168.32.0 do 192.168.63.0 je dozvoljen pristup ka bilo kom odredištu.

FTP zahteva da oba porta budu dozvoljena.

- Port 20 = ftp- kanal za podatke
- Port 21 = ftp (komandni kanal)

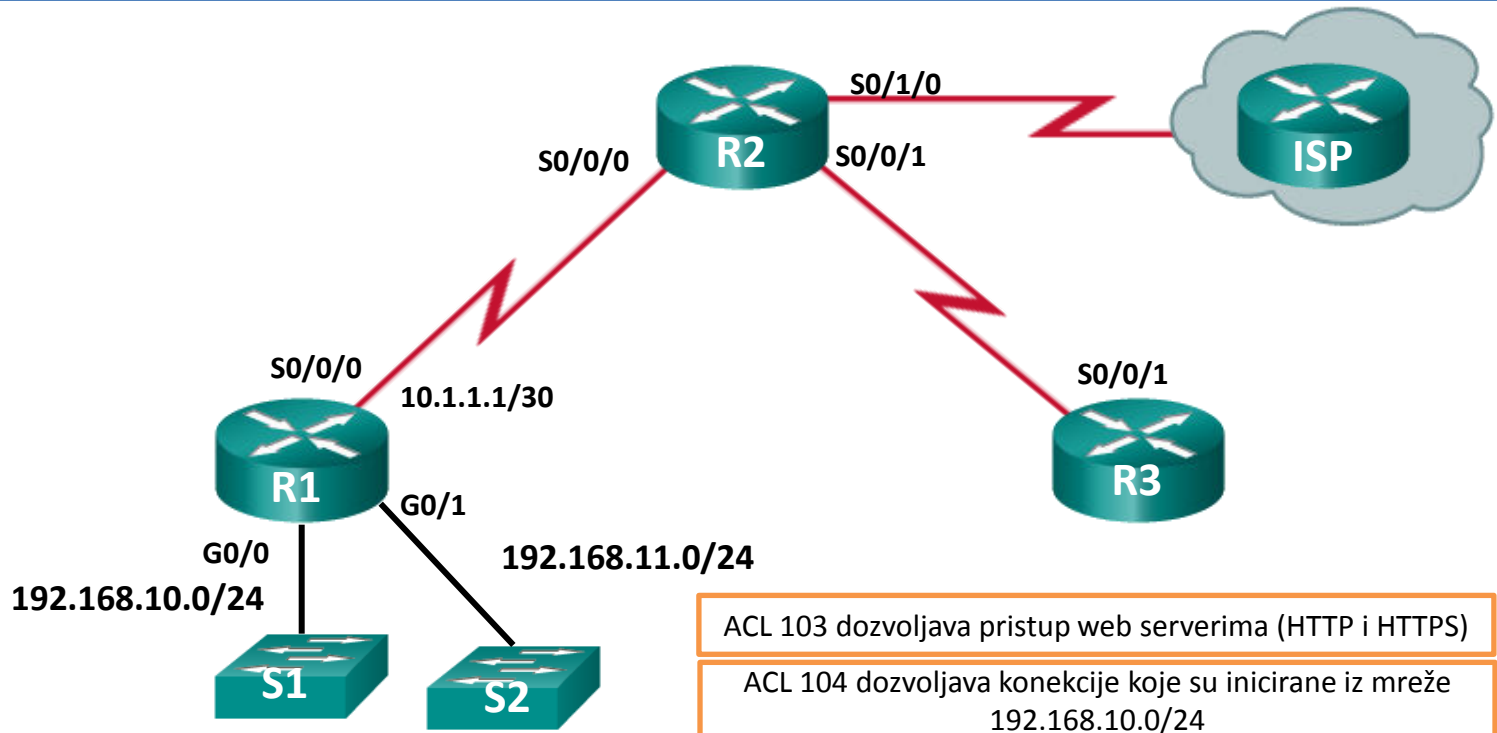


ECDL
European Computer
Driving Licence



ETS AUTHORIZED
TOEFL iBT CENTER

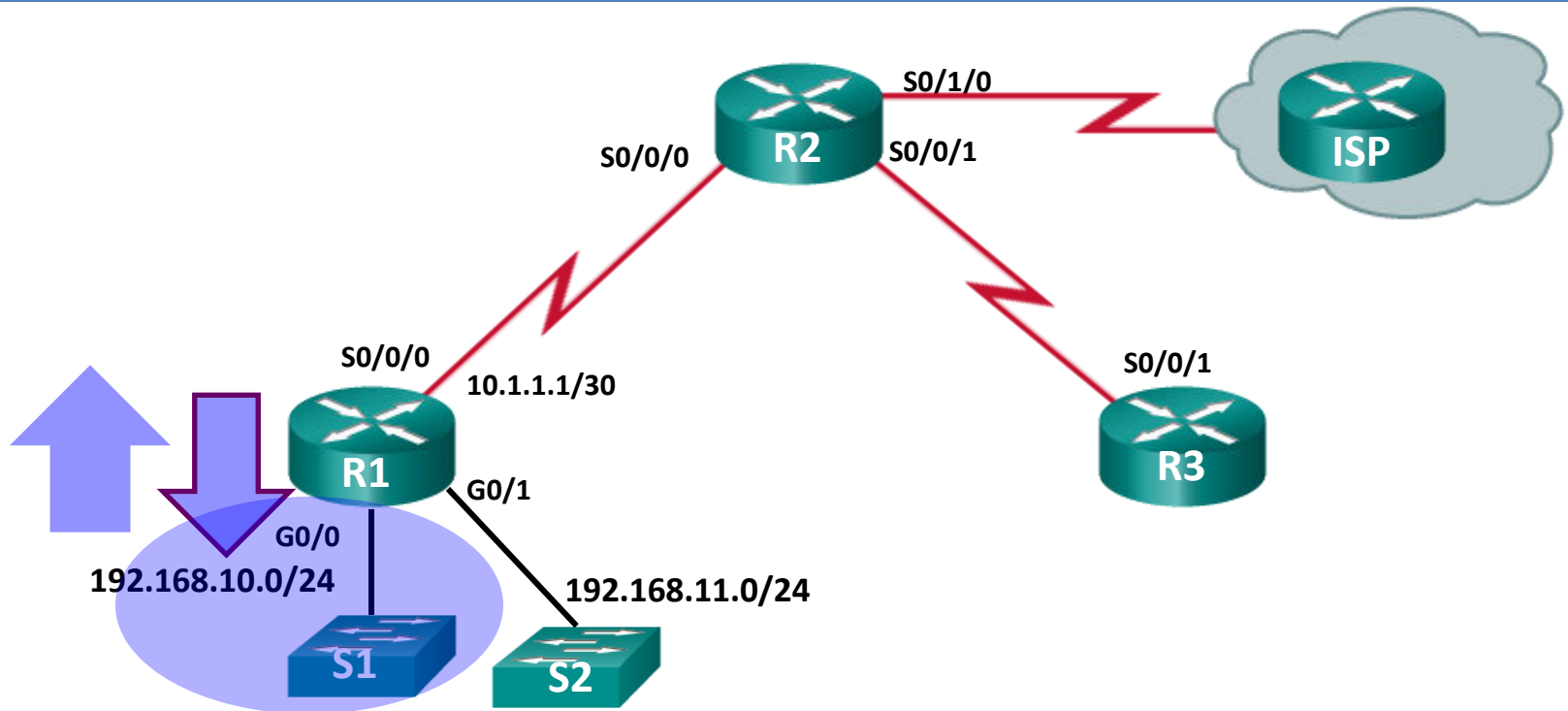
KONFIGURACIJA EXTENDED ACL



```
R1 (config) #access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1 (config) #access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1 (config) #access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
```

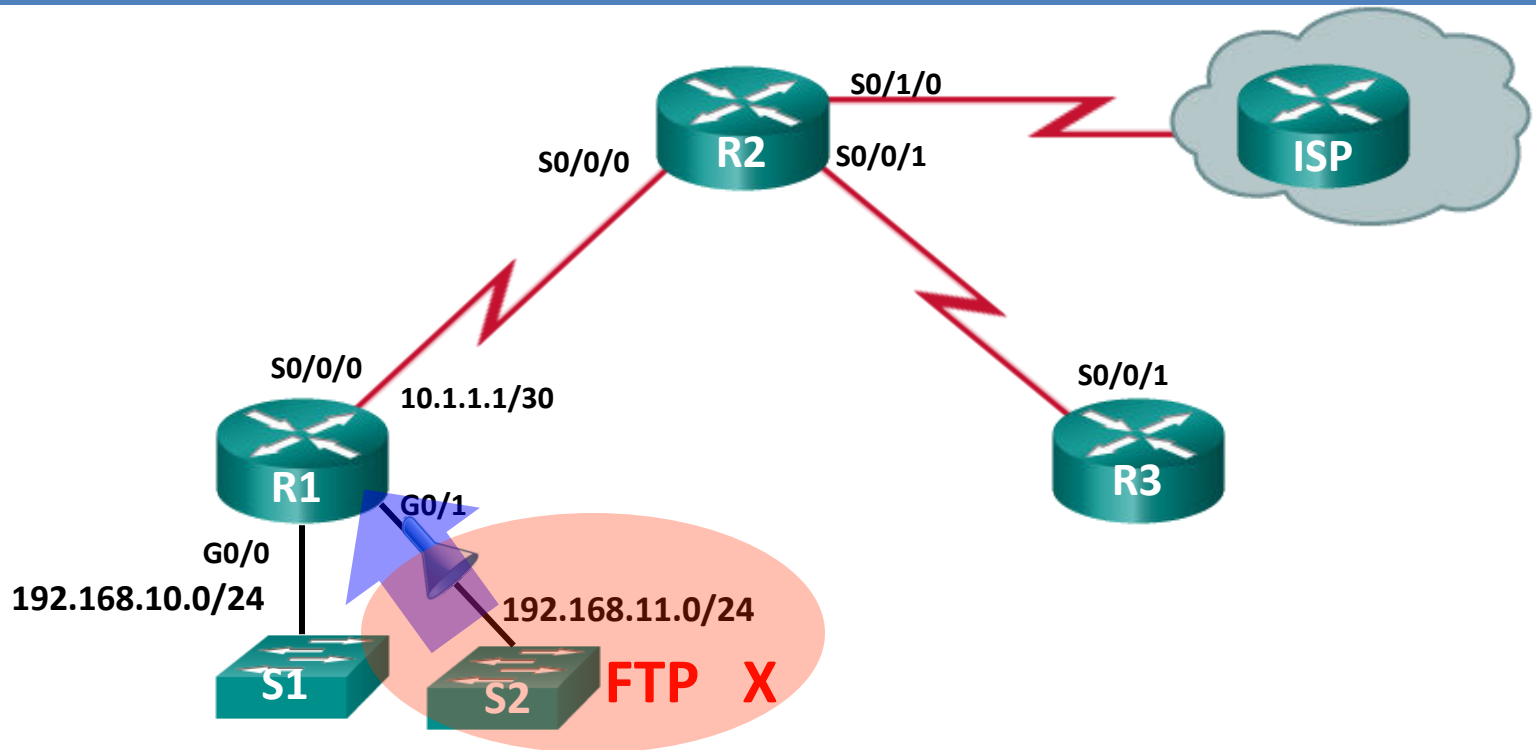
Established parametar dozvoljava samo povratni saobraćaj koji je odgovor na saobraćaj koji je iniciran iz 192.168.10.0/24 mreže.

PRIMENA EXTENDED ACL NA INTERFEJS



```
R1(config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)# access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)# interface g0/0
R1(config-if)# ip access-group 103 in
R1(config-if)# ip access-group 104 out
```

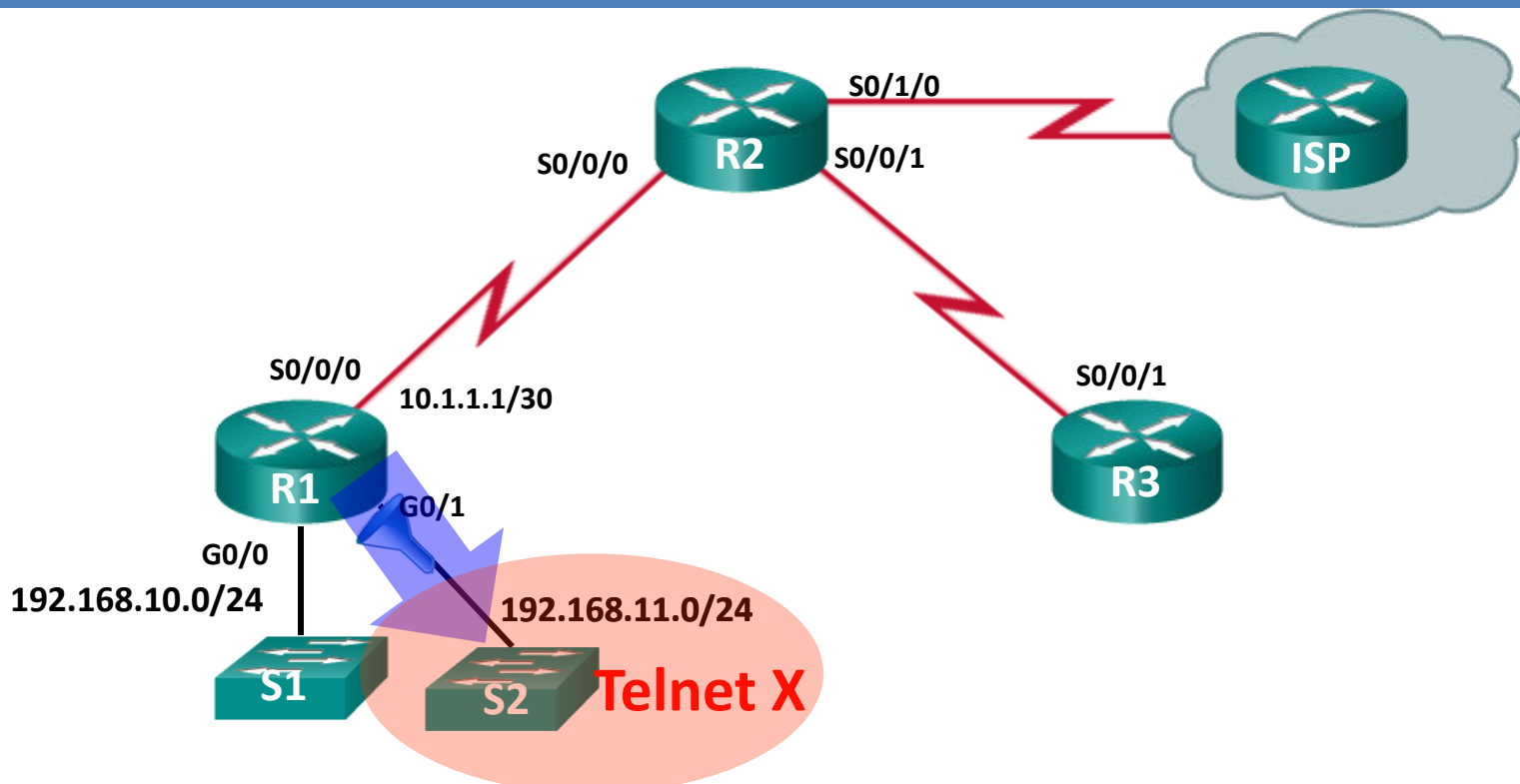
ZABRANA SAMO FTP SAOBRAĆAJA



```
R1(config)#access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0 0.0.0.255 eq ftp
R1(config)#access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0 0.0.0.255 eq ftp-data
R1(config)#access-list 101 permit ip any any

R1(config)# nterface g0/1
R1(config-if# ip access-group 101 in
```

ZABRANA SAMO TELNET SAOBRAĆAJA



```
R1 (config) # access-list 102 deny tcp 192.168.11.0 0.0.0.255 any eq 23
R1 (config) # access-list 102 permit ip any any

R1 (config) # interface g0/1
R1 (config-if) # ip access-group 102 out
```


ACL REŠAVANJE PROBLEMA #2

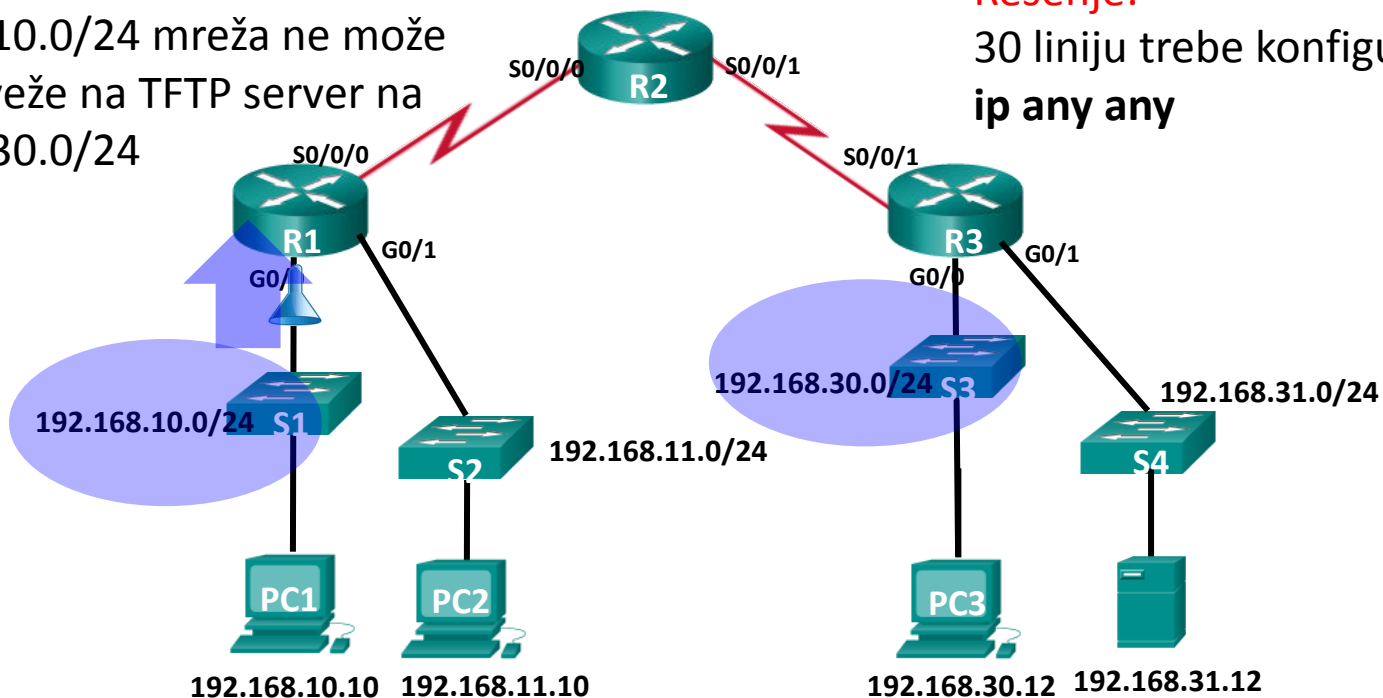
```
R1# show access-lists 120
Extended IP access list 120
 10 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
 20 deny tcp 192.168.10.0 0.0.0.255 host 192.168.31.12 eq smtp
 30 permit tcp any any
```

Problem:

192.168.10.0/24 mreža ne može da se poveže na TFTP server na 192.168.30.0/24

Rešenje:

30 liniju trebe konfigurisati ip any any



ACL REŠAVANJE PROBLEMA #3

```
R1# show access-lists 130
```

```
Extended IP access list 130
```

```
10 deny tcp any eq telnet any
```

```
20 deny tcp 192.168.11.0 0.0.0.255 host 192.168.31.12 eq smtp
```

```
30 permit tcp any any (12 match(es))
```

Problem:

Iz 192.168.11.0/24 mreže se ne sme koristiti Telnet ka 192.168.30.0/24.

Rešenje:

10 liniju treba konfigurirati deny tcp any any eq telnet

