Nastavni predmet:	**RAČUNALNE MREŽE**
Vježba:	Liste pristupa (ACL) na usmjerniku
Cilj vježbe:	Uvježbati postupke konfiguracije dinamičkog rutinga. Naučiti primjenu standardne liste pristupa.

Sven Grgić i Maja Markovac

PRIPREMA ZA VJEŽBU

U pismenoj formi odgovori na slijedeća pitanja:

1. Koji slojevi OSI modela omogućavaju filtriranje prometa?
   Mrežni sloj
2. Koje su mogući kriteriji za propuštanje (ili zabranu) prolaska paketima?
   Kriteriji mogu biti točnost izvorišne i odredišne IP adrese, protokol ili po podacima u paketu.
3. Kako funkcionira standardna lista pristupa?
   Funkcionira tako što filtira promet na temelju izvorišne IP adrese.
4. Kako se dobiva wildcard maska? Primjer.
   Wildcard se dobiva tako što se invertira subnet maska u binarnom obliku te se pretvori natrag u decimalni oblik.
   Na primjer mrežna maska 255.255.255.252 je u binarnom 11111111.11111111.11111111.11111100. Kad se to invertira (jedinice u nule, nule u jedinice) dobije se sljedeće: 00000000.00000000.00000000.00000011 što je u decimalnom zapisu: 0.0.0.3 i to je wildcard maska.
5. Koje elemente sadrži proširena ACL?

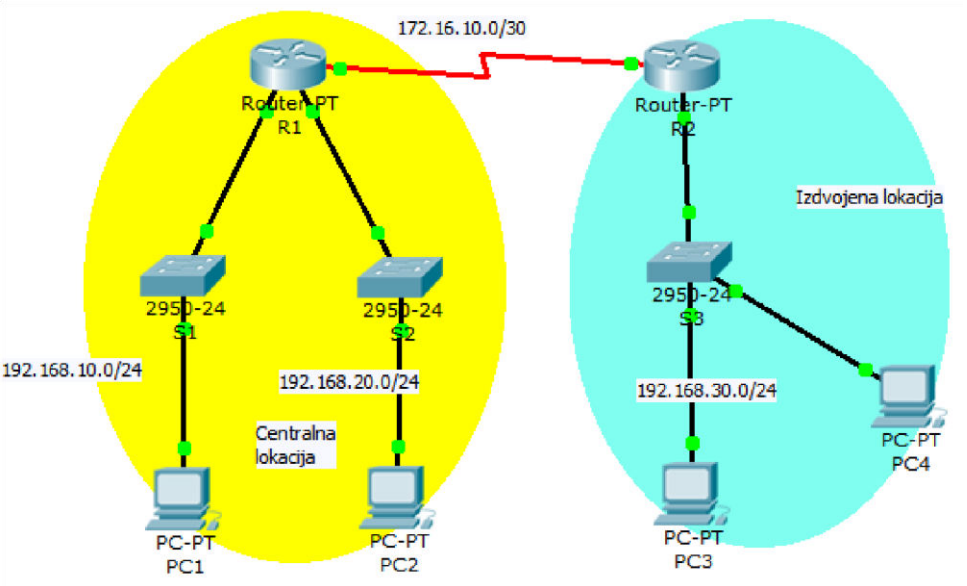
   Sadrži dodatno filtriranje i to prema izvorišnoj IP adresi, odredišnoj IP adresi, protokolu (IP, ICMP, OSPF, TCP, UDP i drugi) i podacima (brojevi TCP i UDP portova, TCP zastavice i ICMP poruke).

Situacija:

Uprava tvrtke je odlučila primjeniti određena ograničenja unutar svoje mreže kako bi se povećao stupanj sigurnosti i zaštite podataka. Administrator je prepustio tehničarima da konfiguriraju liste pristupa ACL te da konfiguraciju prethodno isprobaju na simulatoru.

Zahtjevi su slijedeći:
Konfigurirati ACL prema slijedećim zahtjevima:

a) *Računalima na mreži 192.168.10.0/24 je dozvoljen pristup mreži na izdvojenoj lokaciji ali ne na mrežu 192.168.20.0/24*
b) *Računalima sa mreže 192.168.30.0/24 omogućen je pristup svim mrežama.Izuzetak je računalo sa IP adresom 192.168.30.128 (PC3) koje nema dozvolu izlaska iz mreže*



IZVOĐENJE VJEŽBE

Zabilješke, skice i topologije, te odgovore na postavljena pitanja zapisati u bilježnicu.

Uređaj	Oznaka sučelja	Adresa sučelja	Mrežna maska	Tip serijskog sučelja	Default gateway
R1	Fa 0/0	192.168.10.1	255.255.255.0		
	Fa 0/1	192.168.20.1	255.255.255.0		
	S2/0	172.16.10.1	255.255.255.252	DCE	
R2	Fa 0/0	192.168.30.1	255.255.255.0		
	S2/0	172.16.10.2	255.255.255.252	DTE	
PC1		192.168.10.10	255.255.255.0		192.168.10.1
PC2		192.168.20.10	255.255.255.0		192.168.20.1
PC3		192.168.30.10	255.255.255.0		192.168.30.1
PC4		192.168.30.128	255.255.255.0		192.168.30.1

Zadaci:

1. Spoji uređaje prema zadanoj topologiji i izvrši temeljnu konfiguraciju usmjernika. Preklopnici su u defaultnoj konfiguraciji te ih nije potrebno konfigurirati.

2. Izvrši konfiguraciju sučelja usmjernika i računala prema podacima iz tablice.

3. Konfiguriraj RIPv1 protokol na usmjernicima.

   - **Što bi se dogodilo kada ovaj (ili neki drugi) ruting protokol ne bi bio konfiguriran?**

4. Izvrši provjeru povezanosti između računala PC1 do PC4.

5. Ukoliko je provjera bila uspješna, pristupi konfiguriranju liste pristupa na usmjerniku R1, na slijedeći način:

a) Listom pristupa pod rednim brojem 10, na usmjerniku R1 onemogući promet sa mreže 192.168.10.0 na mrežu 192.168.20.0 : **R1(config)#access-list 10 deny 192.168.10.0 0.0.0.255**

b) Istom listom omogući promet na mrežu 192.168.20.0 sa bilo koje druge mreže: **R1(config)#access-list 10 permit any**

c) Odredi da se promet filtrira na portu koji je najbliži odredištu **R1(config)#interface fa 0/1**

d) Definiraj da će se filtriranje provesti na izlazu toga porta **R1(config-if)#ip access-group 10 out**

   - **Što u instrukciji pod a) predstavlja dio 0.0.0.255?**
   - **Koja je oznaka porta koji je najbliži mreži 192.168.20.0?**
   - **Kojim je rednim brojevima numeriraju standardne ACL?**

6. Provjeri učinkovitost liste pristupa koju si konfigurirao, slanjem ICMP paketa.

   - **Da li ACL odrađuje funkciju na način kako si očekivao?**
   - **Ako se javio problem, opiši kako se on očituje.**
   - **Kod traženja odgovora iskoristi slanje ICMP paketa sa računala uz pomoć naredbenog retka, ali isto tako iz Simulacijskog moda, korak po korak.**

7. Konfiguracija druge liste pristupa na usmjerniku R2.

a) Listom pristupa pod rednim brojem 20 onemogući da računalo sa IP adresom 192.168.30.128 šalje podatke izvan LAN-a: **R2(config)#access-list 20 deny 192.168.30.128**

b) Istom listom pristupa omogući da ostala računala u toj mreži mogu slobodno prometovati izvan LAN-a:
R2(config)#access-list 20 permit any

c) Odredi da se promet filtrira na portu koji je najbliži polazištu:
R2(config)#interface fa 0/0

d) Definiraj da će se filtriranje provesti na ulazu toga porta
R2(config-if)#ip access-group 20 in

8. Provjeri učinkovitost liste pristupa koju si konfigurirao, slanjem ICMP paketa.

- **Radi li konfigurirana lista pristupa na očekivani način?**
- **Provjeri može li se ova ACL primijeniti tako da filtrira promet na izlaznom portu.**
  - **Koji je način bolji i zašto?**

Nakon obavljenih zadataka u ovoj vježbi učenik će samostalno (ili uz manju pomoć zabilješki):

- Učinkovito na simulatoru konfigurirati usmjernike i usmjernički protokol RIPv1.
- Konfigurirati standardnu listu pristupa.
- Praćenjem prometa u mreži dijagnosticirati moguće probleme te ih otkloniti.

Provjera znanja:

1. Točni odgovori na postavljena pitanja po zadacima – 1 bod
2. Temeljnu konfiguracija usmjernika i RIPv1 protokola – 1 bod
3. Konfigurirati standardnu listu pristupa sa zabranom prometa između dviju mreža na istom usmjerniku – 1 bod
4. Konfigurirati i pozicionirati listu pristupa koja zabranjuje vanjski promet sa ili na određeno računalo – 1 bod
5. Praćenje prometa između mreža na kojima je filtriranje omogućeno, dijagnosticiranje greške i njezino otklanjanje – 1 bod.