LV15: Liste pristupa (ACL) na usmjerniku

Priprema za vježbu

1. Koji slojevi OSI modela omogućavaju filtriranje prometa?

Slojevi OSI modela koji omogućavaju filtriranje prometa su 3. (Sloj mrežne veze) i 4. (Transportni sloj).

2. Koje su mogući kriteriji za propuštanje (ili zabranu) prolaska paketima?

Mogući kriteriji za propuštanje ili zabranu prolaska paketima uključuju IP adrese izvora i odredišta, portove, protokole, i sadržaj paketa.

3. Kako funkcionira standardna lista pristupa?

Standardna lista pristupa (ACL) funkcionira tako da definira dozvoljene ili zabranjene vrste prometa na temelju određenih kriterija, kao što su IP adrese, portovi ili protokoli. Ove liste se primjenjuju na ulazne ili izlazne sučelja usmjerničkih uređaja (routera) i omogućuju ili blokiraju prolazak paketa na temelju definiranih pravila.

4. Kako se dobiva wildcard maska? Primjer.

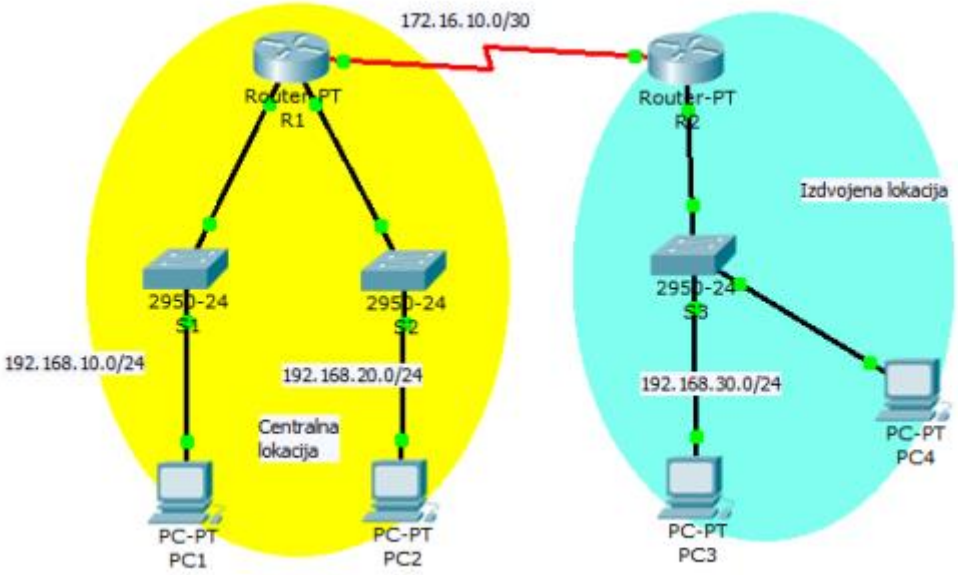
Wildcard maska se dobiva invertiranjem obične mrežne maske. Primjer, ako je obična mrežna maska 255.255.255.0, wildcard maska će biti 0.0.0.255.

5. Koje elemente sadrži proširena ACL?

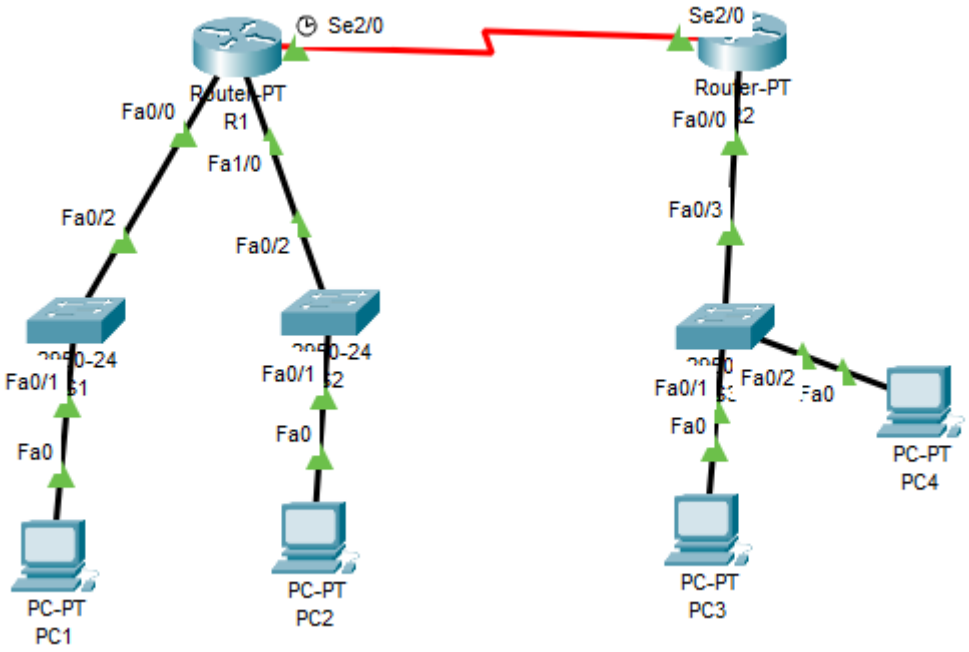
Proširena ACL (Access Control List) uključuje dodatne elemente u usporedbi s standardnom ACL. To može uključivati dodatne kriterije poput sadržaja paketa, dodatnih protokola ili dodatnih atributa IP adresa.

Izvođenje vježbe

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



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.

R1:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown
```

```
Router(config)#interface fastethernet 1/0
Router(config-if)#ip address 192.168.20.1 255.255.255.0
Router(config-if)#no shutdown
```

```
Router(config-if)#exit
Router(config)#interface serial 2/0
Router(config-if)#ip address 172.16.10.1 255.255.255.252
Router(config-if)#no shutdown
```

R2:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.30.1 255.255.255.0
Router(config-if)#no shutdown
```

```
Router(config-if)#exit
Router(config)#interface serial 2/0
Router(config-if)#ip address 172.16.10.2 255.255.255.252
Router(config-if)#no shutdown
```

3. Konfiguriraj RIPv1 protokol na usmjernicima. - Što bi se dogodilo kada ovaj (ili neki drugi) ruting protokol ne bi bio konfiguriran?

Nebi bila uspostavljena veza između računala

R1:

```
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 172.16.10.0
```

Network Address
172.16.0.0
192.168.10.0
192.168.20.0
192.168.30.0

R2:

```
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 172.16.10.0
```

Network Address
172.16.0.0
192.168.10.0
192.168.20.0
192.168.30.0

4. Izvrši provjeru povezanosti između računala PC1 do PC4.

```
C:\>ping 192.168.30.128

Pinging 192.168.30.128 with 32 bytes of data:

Request timed out.
Reply from 192.168.30.128: bytes=32 time=1ms TTL=126
Reply from 192.168.30.128: bytes=32 time=7ms TTL=126
Reply from 192.168.30.128: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.30.128:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 7ms, Average = 3ms
```

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 :

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(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:

```
Router(config-router)#exit
Router(config)#access-list 10 permit any
```

c) Odredi da se promet filtrira na portu koji je najbliži odredištu

```
Router(config)#interface fa 1/0
```

d) Definiraj da će se filtriranje provesti na izlazu toga porta

```
Router(config-if)#ip access-group 10 out
```

Što u instrukciji pod a) predstavlja dio 0.0.0.255?

Wildcard mrežna maska

Koja je oznaka porta koji je najbliži mreži 192.168.20.0?

Fa 1/0

Kojim je rednim brojevima numeriraju standardne ACL?

Od 1 do 99 ili od 1300 do 1999

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

Da li ACL odrađuje funkciju na način kako si očekivao?

Da

Ako se javio problem, opiši kako se on očituje.

Ne može komunicirati sa mrežom 192.168.20.0

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:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(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:

```
Router(config)#access-list 20 permit any
```

c) Odredi da se promet filtrira na portu koji je najbliži polazištu:

```
Router(config)#interface fa 0/0
```

d) Definiraj da će se filtriranje provesti na ulazu toga porta

```
Router(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?

Da radi

Provjeri može li se ova ACL primijeniti tako da filtrira promet na izlaznom portu.

Ne može se promjeniti jer mu je onemogučen izlaz iz lokalne mreže