Matija Kovač i Petar Pavić 3.C

LV15 – Liste pristupa (ACL) na usmjerniku

PRIPREMA ZA VJEŽBU

1. Koji slojevi OSI modela omogućavaju filtriranje prometa?

Filtriranje prometa obično se provodi na OSI slojevima 3 (mrežni sloj) i 4 (transportni sloj), iako se može provoditi i na slojevima 5 (sesijski sloj) i 7 (aplikacijski sloj) ovisno o specifičnim zahtjevima i implementaciji.

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

Kriteriji za propuštanje ili blokiranje prolaska paketima mogu uključivati adresne informacije (npr. IP adresa izvorišta ili odredišta), vrstu prometa (npr. HTTP, FTP), portove (za TCP/UDP), te dodatne informacije kao što su QoS oznake ili specifični podaci u zaglavljima paketa.

3. Kako funkcionira standardna lista pristupa?

Standardna lista pristupa (ACL) funkcionira tako da omogućava ili blokira prolazak prometa na temelju zadanih pravila. Svako pravilo definira određene kriterije (npr. IP adresa izvorišta, odredišta, ili vrsta prometa) i akciju koja se treba poduzeti (npr. dopustiti ili blokirati promet koji zadovoljava te kriterije).

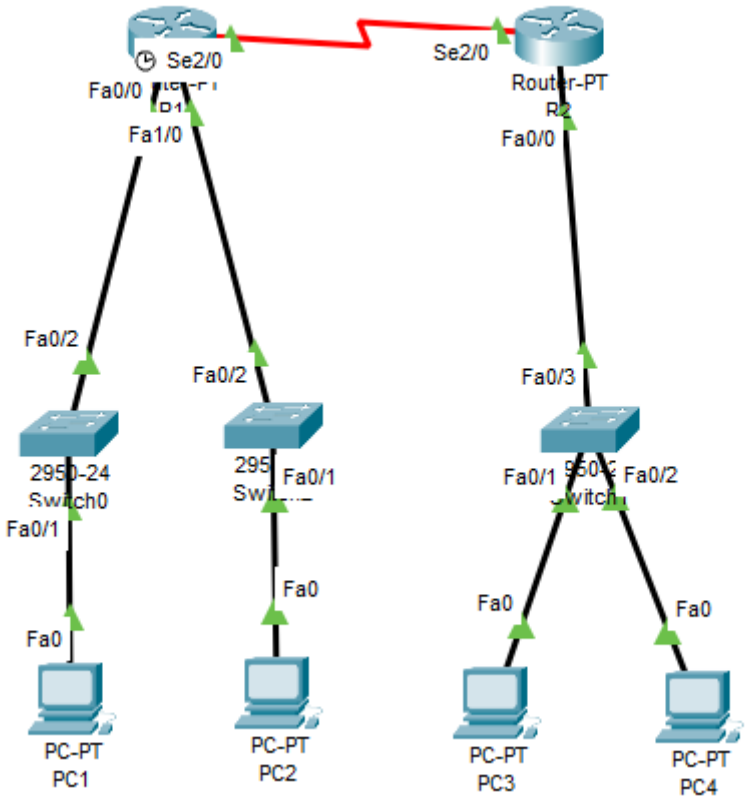
4. Kako se dobiva wildcard maska? Primjer.

Wildcard maska se dobiva invertiranjem mrežne maske. Na primjer, ako je mrežna maska 255.255.255.0, njena wildcard maska će biti 0.0.0.255.

5. Koje elemente sadrži proširena ACL?

Proširena lista pristupa (extended ACL) obično sadrži dodatne kriterije za filtriranje prometa u usporedbi s standardnom listom pristupa. Osim IP adresa izvora i odredišta, proširena ACL može uzeti u obzir i druge faktore kao što su tipovi protokola (TCP, UDP, ICMP), specifični portovi, te različite dijelove zaglavlja paketa kako bi omogućila detaljnije upravljanje prometom.

IZVOĐENJE VJEŽBE



3. Konfiguriraj RIPv1 protokol na usmjernicima.

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

Kada ovaj (ili neki drugi) ruting protokol ne bi bio konfiguriran paketi se ne bi mogli slati iz jedne mreže u drugu.

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 fa1/0
```

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?

U instrukciji pod a) dio 0.0.0.255 predstavlja mrežnu masku.

Koja je oznaka porta koji je najbliži mreži 192.168.20.0?

Oznaka porta koji je najbliži mreži 192.168.20.0 je fa1/0.

Kojim je rednim brojevima numeriraju standardne ACL?

Rednim brojem kojim je numeriran standard ACL je 10.

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

Da li ACL odrađuje funkciju na način kako si očekivao?

Odrađuje funkciju na način kako sam očekivao.

Ako se javio problem, opiši kako se on očituje.

Nije se javio problem.

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(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?

Konfigurirana lista pristupa radi na očekivani način.

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

Može, potrebno je specificirati izlazni port u CLI-u.

Koji je način bolji i zašto?

Zavisi o slučaju. ACL filtrira promet i to može spriječiti neželjeni pristup i smanjiti promet u mreži, dok Rip protokol samo omogućuje pristup mreži od strane određenih mreža.