Niko Marinović, Luka Protrka, 3.G

# LV09: Liste pristupa (ACL) na usmjerniku

**PRIPREMA ZA VJEŽBU**:

**1. Koji slojevi OSI modela omogućavaju filtriranje prometa?**

mrežni sloj: Filtrira promet prema IP adresama.

transportni sloj: Omogućava filtriranje prema portovima i protokolima (TCP/UDP).

aplikacijski sloj: Dublja inspekcija podataka prema aplikacijskim protokolima (poput HTTP-a).

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

IP adrese izvora i odredišta.

Brojevi portova (npr. port 80 za HTTP).

Protokoli (TCP, UDP, ICMP).

Specifični sadržaj paketa (Layer 7 inspekcija).

Vrijeme pristupa ili određeni uvjeti (kod naprednih sustava).

**3. Kako funkcionira standardna lista pristupa?**

Standardna ACL omogućava filtriranje prometa temeljem izvorne IP adrese. Primjenjuje se blizu odredišta, a sintaksa je obično jednostavna (npr. access-list 10 permit 192.168.1.0 0.0.0.255).

**4. Kako se dobiva wildcard maska? Primjer.**

Wildcard maska koristi se za precizno definiranje IP adresa u ACL-ovima. Dobiva se invertiranjem subnet maske (bit za bitom).

Npr. za subnet masku 255.255.255.0, wildcard maska je 0.0.0.255. Ako želite dopustiti promet za mrežu 192.168.1.0/24, koristite: access-list 10 permit 192.168.1.0 0.0.0.255

**5. Koje elemente sadrži proširena ACL?**

Izvorne i odredišne IP adrese.

Protokole (TCP, UDP, ICMP...).

Portove (određene ili raspon).

Dodatne uvjete (vrsta ICMP poruke, TCP flagovi itd.).

**IZVOĐENJE VJEŽBE:**

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

Ako RIPv1 protokol (ili neki drugi ruting protokol) ne bi bio konfiguriran, usmjernici ne bi znali kako međusobno razmjenjivati informacije o mrežnim putanjama. To bi dovelo do nemogućnosti usmjeravanja prometa između mreža, što bi rezultiralo prekidom komunikacije između uređaja u različitim mrežama.

**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=1ms TTL=126
Reply from 192.168.30.128: bytes=32 time=1ms 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 = 1ms, Average = 1ms
```

**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**

```
R1(config)#access-list 10 deny 192.168.0.0 0.0.0.255
R1(config)#
```

**b) Istom listom omogući promet na mrežu 192.168.20.0 sa bilo koje druge mreže:**

**R1(config)#access-list 10 permit any**

```
R1(config)#access-list 10 permit any
R1(config)#
```

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

**R1(config)#interface fa 0/1**

```
R1(config)#interface fa 0/0
R1(config-if)#
```

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

**R1(config-if)#ip access-group 10 out**

```
R1(config-if)#ip access-group 10 out
R1(config-if)#
```

**- Što u instrukciji pod a) predstavlja dio 0.0.0.255?**

0.0.0.255 predstavlja "wildcard masku".

**- Koja je oznaka porta koji je najbliži mreži 192.168.20.0?**

Fast Ethernet 0/0

**- Kojim je rednim brojevima numeriraju standardne ACL?**

Standardne ACL (Access Control Lists) u Cisco uređajima numeriraju se brojevima u opsegu od 1 do 99**.** Također, postoji i prošireni opseg brojeva za proširene ACL, koji ide od 100 do 199**.**

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

**- Da li ACL odrađuje funkciju na način kako si očekivao?**

```
C:\>ping 192.168.30.128

Pinging 192.168.30.128 with 32 bytes of data:

Reply from 192.168.30.128: bytes=32 time=12ms TTL=126
Reply from 192.168.30.128: bytes=32 time=1ms TTL=126
Reply from 192.168.30.128: bytes=32 time=2ms TTL=126
Reply from 192.168.30.128: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.30.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 4ms
```

Radi

**- Ako se javio problem, opiši kako se on očituje.**

Repy from Host Unreachable.

**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**

```
R2(config)#access-list 20 deny 192.168.30.128
R2(config)#
```

**b) Istom listom pristupa omogući da ostala računala u toj mreži mogu slobodno prometovati izvan LAN-a:**

**R2(config)#access-list 20 permit any**

```
R2(config)#access-list 20 permit any
R2(config)#
```

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

**R2(config)#interface fa 0/0**

```
R2(config)#interface fa 0/0
R2(config-if)#
```

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

**R2(config-if)#ip access-group 20 in**

```
R2(config-if)#ip access-group 20 in
R2(config-if)#
```

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

**- Radi li konfigurirana lista pristupa na očekivani način?**

Da, ACL bi trebao blokirati ili proći ICMP pakete ovisno o pravilima (npr. "permit" ili "deny").

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

Da, ACL može biti primijenjen na izlaznom portu pomoću odgovarajuće konfiguracije na routeru ili firewallu.

**- Koji je način bolji i zašto?**

Filtriranje na ulaznom portu je obično bolje jer smanjuje nepotrebni promet prije nego što dođe do mrežnog uređaja, dok filtriranje na izlaznom portu omogućava većem broju uređaja da šalju promet, ali uz dodatno opterećenje.