

Liste pristupa (ACL) na usmjerniku

Izradili: Marko Sesar, Josip Sremić 3.C

Uvježbati postupke konfiguracije dinamičkog rutiranja. Naučiti primjenu standardne liste pristupa.

Priprema za vježbu:

Zadatak 1: Koji slojevi OSI modela omogućavaju filtriranje prometa?

Odgovor: Filtriranje prometa se odvija na mrežnom, transportnom ili aplikacijskom sloju, a samo filtriranje nam omogućava Firewall.

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

Odgovor: Kriteriji mogu biti točnost izvorišne i odredišne IP adrese, protokol ili po podacima u paketu.

Zadatak 3: Kako funkcionira standardna lista pristupa?

Odgovor: Funkcionira tako što filtrira promet na temelju izvorišne IP adrese.

Zadatak 4: Kako se dobiva wildcard maska? Primjer.

Odgovor: 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.

Zadatak 5: Koje elemente sadrži proširena ACL?

Odgovor: 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)

3. Konfiguriraj RIPv1 protokol na usmjernicima.

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

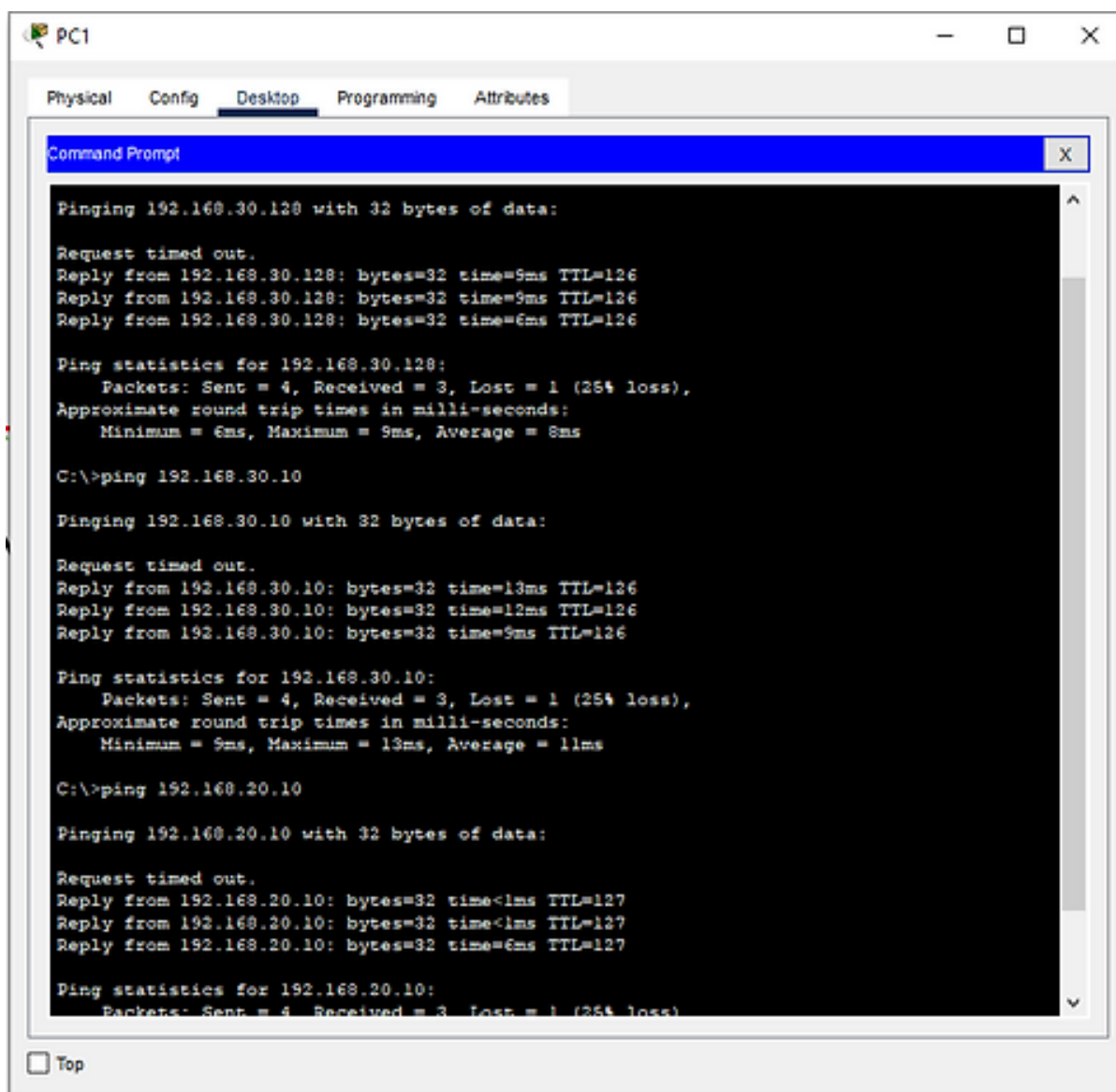
Kad nebi konfigurirali niti jedan protokol u tom slučaju računala nebi bila međusobno povezana.

```
Router(config-if)#  
Router(config-if)#exit  
Router(config)#router rip  
Router(config-router)#network 192.168.10.0  
Router(config-router)#network 192.168.20.0  
Router(config-router)#network 172.16.0.0  
Router(config-router)#
```

R1:

R2:

```
Router(config)#router rip  
Router(config-router)#network 192.168.30.0  
Router(config-router)#network 172.16.0.0  
Router(config-router)#
```



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?

```
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.10.0
Router(config-router)#network 192.168.20.0
Router(config-router)#network 172.16.0.0
Router(config-router)#exit
Router(config)#access-list 10 deny 192.168.10.0 0.0.0.255
Router(config)#access-list 10 permit any
Router(config)#interface fa 0/1
%Invalid interface type and number
Router(config)#interface fastethernet0/1
%Invalid interface type and number
Router(config)#interface fastethernet 0/1
%Invalid interface type and number
Router(config)#interface fastethernet 1/0
Router(config-if)#ip access-group 10 out
Router(config-if)#exit
```

- Dio 0.0.0.255 je wildcard maska.
- Oznaka porta koji je nablži mreži 192.168.20.0 je FastEthernet 1/0.
- Standardne ACL se numeriraju brojevima 1-99 i 1300-1999.

6. Proveri 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

Promet s mreže 192.168.10.0 na mrežu 192.168.20.0 je zabranjen:

```
C:\>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:


Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Top

Promet s mreže 192.168.30.0 na mrežu 192.168.20.0 je omogućen što znači da sve mreže osim ove prve komuniciraju s mrežom 192.168.20.0:

 PC3

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:

Reply from 192.168.20.10: bytes=32 time=1ms TTL=126
Reply from 192.168.20.10: bytes=32 time=8ms TTL=126
Reply from 192.168.20.10: bytes=32 time=1ms TTL=126
Reply from 192.168.20.10: bytes=32 time=14ms TTL=126

Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 14ms, Average = 6ms

C:\>
```

7. Konfiguracija druge liste pristupa na usmjerniku R2.

a) Listom pristupa pod rednim brojem 20 onemogućiti 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
```

- Konfigurirana lista radi očekivano
- Nije se javio problem i sva provjera je bila uspješna.

```
Router>enabl
Router#conf terminal
Enter configuration commands, one per line. End v
Router(config)#access-list 20 deny 192.168.30.128
Router(config)#access-list 20 permit any
Router(config)#interface fastethernet0/0
Router(config-if)#ip access-group 20 in
Router(config-if)#exit
Router(config)#
```

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

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

Promet s računala 192.168.30.128 je onemogućen:

```
Physical  Config  Desktop  Programming  Attributes

Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>|
```

- Konfigurirana lista radi očekivano

- Može se primijeniti tako da ACL filtrira promet na izlaznom portu, ali je bolje na ulaznom, jer mu je bitnije što ulazi nego što izlazi.