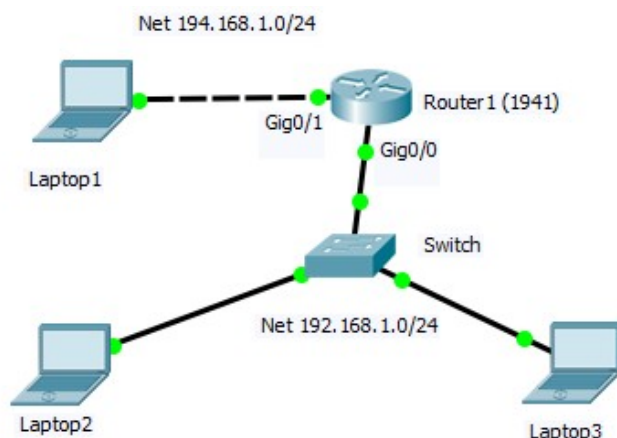


Tehtävä 5

Standard ACL (Access Control List)



Router name	Gig0/1 Address	Gig0/0 Address
Router1	194.168.1.1/24	192.168.1.1/24

Router name	Enable password	VTY password
Router1	cisco	labra

Host	FastEthernet Address	Gateway Address
Laptop1	194.168.1.2/24	194.168.1.1
Laptop2	192.168.1.2/24	192.168.1.1
Laptop3	192.168.1.3/24	192.168.1.1

Asennetaan yllä oleva verkko ja konfiguroidaan työasemille ja reitittimelle taulukon mukaiset asetukset. Tehtävällä konfiguraatiolla estetään Laptop3 työaseman liikennöinti reitittimeen sekä sallitaan Telnet yhteys Laptop1:ltä reitittimeen. Kopioidaan lopuksi asetukset muistiin ja testataan laitteiden väliset yhteydet.

Access-listaa käytetään reitittimissä rajoittamaan pakettien pääsyä muihin verkkoihin. Access-listat numeroidaan ja niitä on kahdenlaisia. Standardit ACL:t on numeroitu välille 1-99 ja extended ACL:t välille 100-199. Standardi lista käy kun suodatus tehdään lähdeosoitteen perusteella kun taas extended listalla voidaan määrittää tarkemmin suodatus kriteerit (esim porttinumeroiden perusteella). Listassa määritelty kohde tai lähde voi olla yksittäinen IP osoite, kaikki IP osoitteet tai verkko. Verkko osoite merkitään käänteisen, wildcard-maskin avulla. Alla esimerkissä estetään (deny) yksittäisen osoitteen läpi pääsy ja sallitaan (permit) kaikkien muiden läpi pääsy

```
Router1(config)#access-list 1 deny host 192.168.1.3
Router1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

Syntaksi: access-list *nro* deny/permit *lähde*

Reitittimen konfigurointi

```
Router>enable
Router#configure terminal
Router(config)#hostname Router1
Router1(config)#interface GigabitEthernet0/0
Router1(config-if)#ip address 192.168.1.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit

Router1(config)#interface GigabitEthernet0/1
Router1(config-if)#ip address 194.168.1.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit

Router1#configure terminal
Router1(config)#access-list 1 remark Example1
Router1(config)#access-list 1 deny host 192.168.1.3
Router1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router1(config)#interface gigabitEthernet 0/0
Router1(config-if)#ip access-group 1 in
Router1(config-if)#exit

Router1(config)#access-list 10 remark Example2
Router1(config)#access-list 10 permit 194.168.1.2
Router1(config)#line vty 0 4
Router1(config-line)#login
Router1(config-line)#password labra
Router1(config-line)#access-class 10 in
Router1(config-line)#exit
Router1(config)#enable secret cisco
Router1(config)#exit

Router1#write
Building configuration...
[OK]
Router1#
```

Testataan konfiguraatio

Yhteys koneiden Laptop3 (192.168.1.3) --- > Laptop1 (194.168.1.2) ei onnistu kuten kuuluukin

```
PC>ping 194.168.1.2

Pinging 194.168.1.2 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 194.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>|
```

Yhteys koneiden Laptop2 (192.168.1.2) ja Laptop1 (194.168.1.2) välillä onnistuu kuten kuuluukin

```
PC>ping 194.168.1.2

Pinging 194.168.1.2 with 32 bytes of data:

Reply from 194.168.1.2: bytes=32 time=1ms TTL=127
Reply from 194.168.1.2: bytes=32 time=1ms TTL=127
Reply from 194.168.1.2: bytes=32 time=17ms TTL=127
Reply from 194.168.1.2: bytes=32 time=0ms TTL=127

Ping statistics for 194.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 17ms, Average = 4ms

PC>|
```

Telnet yhteys **Laptop1:ltä** reitittimeen onnistuu, **muista koneista ei**

```
PC>telnet 194.168.1.1
Trying 194.168.1.1 ...Open

User Access Verification

Password:
Router1>enable
Password:
Router1#
```