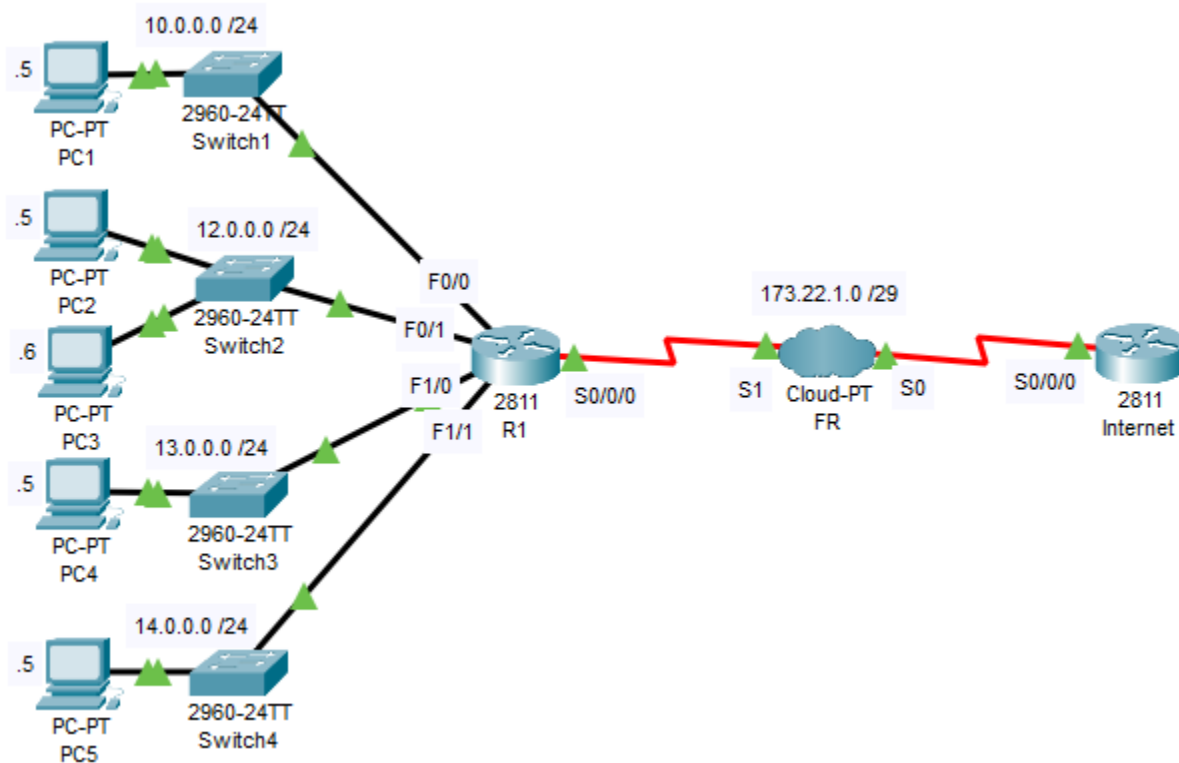


Goal. Use the provided PKT file and configure it with following access lists:

1. Ban PC1 from accessing the "Internet" router
2. Ban all communication between networks 12.0.0.0 and 14.0.0.0 (in both directions)
3. Ban PC2 from accessing Router 1 via Telnet

Enable password on Router 1 is 'quince' – it's necessary for Telnet access



ACL 1

```
R1(config)#ip access-list extended 101
R1(config-ext-nacl)#deny ip host 10.0.0.5 host 173.22.1.2
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
```

```
R1(config)#interface FastEthernet 0/0
R1(config-subif)#ip access-group 101 in
```

ACL 2

```
R1(config)#ip access-list extended 102
R1(config-ext-nacl)#deny ip 12.0.0.0 0.0.0.255 14.0.0.0 0.0.0.255
R1(config-ext-nacl)#deny ip 14.0.0.0 0.0.0.255 12.0.0.0 0.0.0.255
R1(config-ext-nacl)#permit ip any any
```

```
R1(config)#interface FastEthernet 0/1
R1(config-if)#ip access-group 102 in
```

```
R1(config)#interface FastEthernet 1/1
R1(config-if)#ip access-group 102 in
```

ACL 3

```
R1(config)#do show access-list
```

```
R1(config)#ip access-list extended 102
```

```
R1(config-ext-nacl)#25 deny tcp host 12.0.0.5 host 12.0.0.1 eq telnet
```

```
R1(config-ext-nacl)#permit ip any any
```

```
R1(config-ext-nacl)#exit
```

```
R1(config)#interface FastEthernet 0/1
```

```
R1(config-subif)#ip access-group 103 in
```

This ACL will only blocked telnet attempts from PC2 when PC2 tries to connect to 12.0.0.1. However, PC2 can use other Router 1 IP addresses, such as 10.0.0.1, 13.0.0.1, 14.0.0.1 or 173.22.1.1