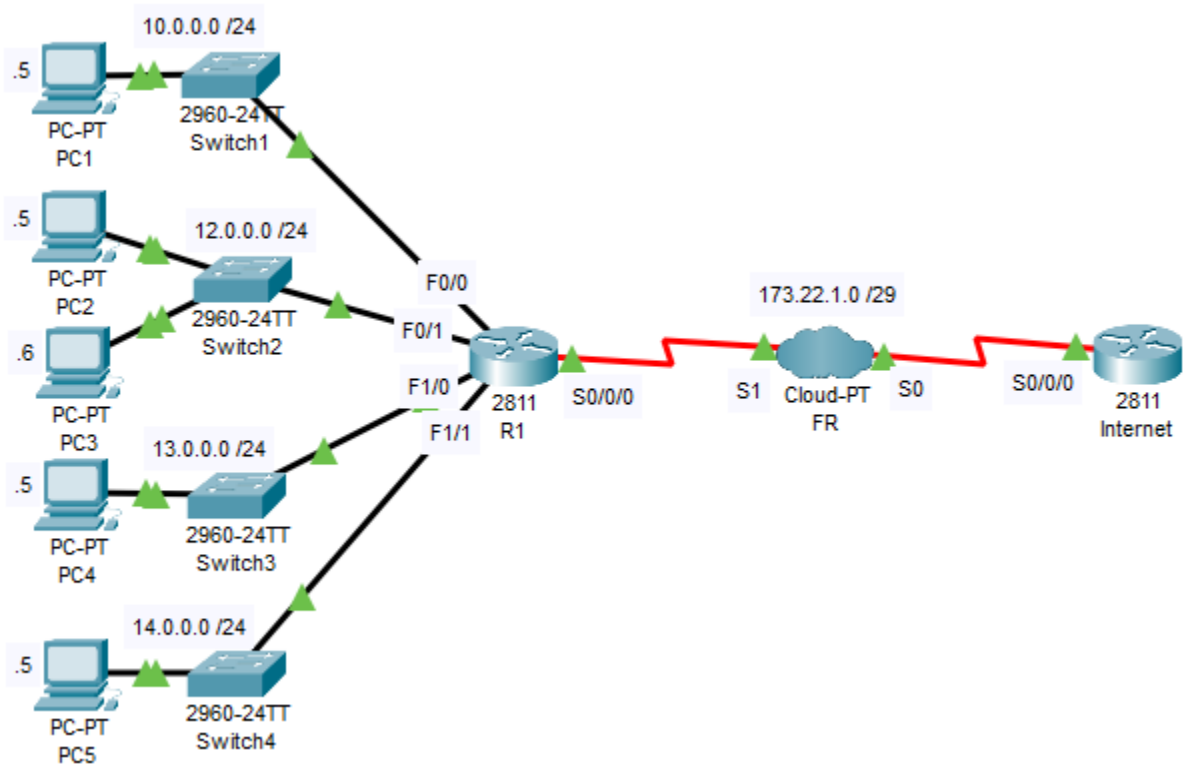
Goal. Use the provided PKT file and configure it with following access lists:

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

```
Int(config)#ip access-list standard 1
Int(config-std-nacl)#deny host 10.0.0.5
Int(config-std-nacl)#permit any
Int(config-std-nacl)#exit

Int(config)#interface Serial 0/0/0.101 point-to-point
Int(config-subif)#ip access-group 1 in
```

If there are no other networks between Router 1 and Router Internet that PC1 should access, this ACL could also be created on Router 1 and applied to Router 1’s Serial 0/0/0.101 interface, in the outgoing direction.

ACL 2

Blocking 12.0.0.0 hosts from sending packets to 14.0.0.0:

```
R1(config)#ip access-list standard 2a
R1(config-std-nacl)#deny 12.0.0.0 0.0.0.255
R1(config-std-nacl)#permit any

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

```
R1(config-if)#ip access-group 2a out
```

Blocking 14.0.0.0 hosts from sending packets to 12.0.0.0:

```
R1(config)#ip access-list standard 2b
R1(config-std-nacl)#deny 14.0.0.0 0.0.0.255
R1(config-std-nacl)#permit any

R1(config)#interface FastEthernet 0/1
R1(config-if)#ip access-group 2b out
```

ACL 3

```
R1(config)#ip access-list standard 3
R1(config-std-nacl)#deny host 12.0.0.5
R1(config-std-nacl)#permit any

R1(config)#line vty 0 15
R1(config-line)#access-class 3 in
```