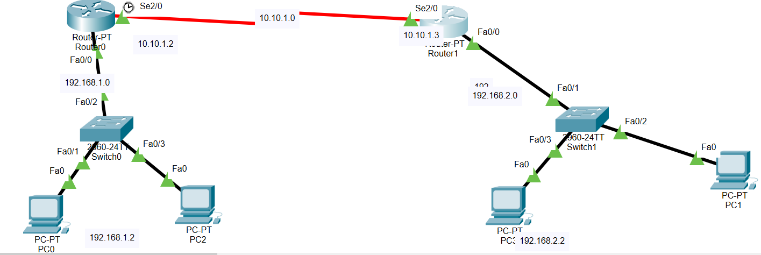
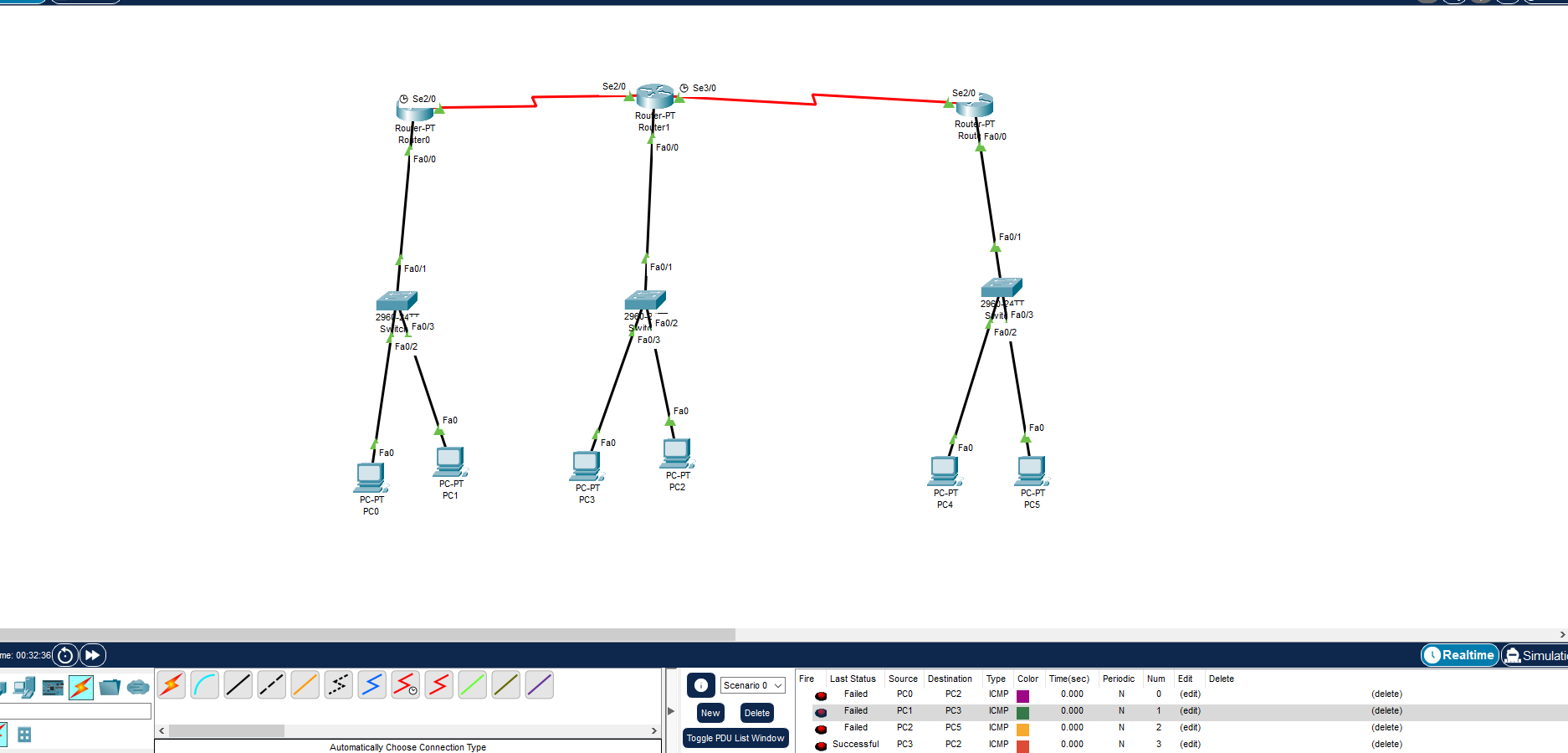
## # Exploring Router and VLAN security, setting up access lists using Cisco Packet tracer.

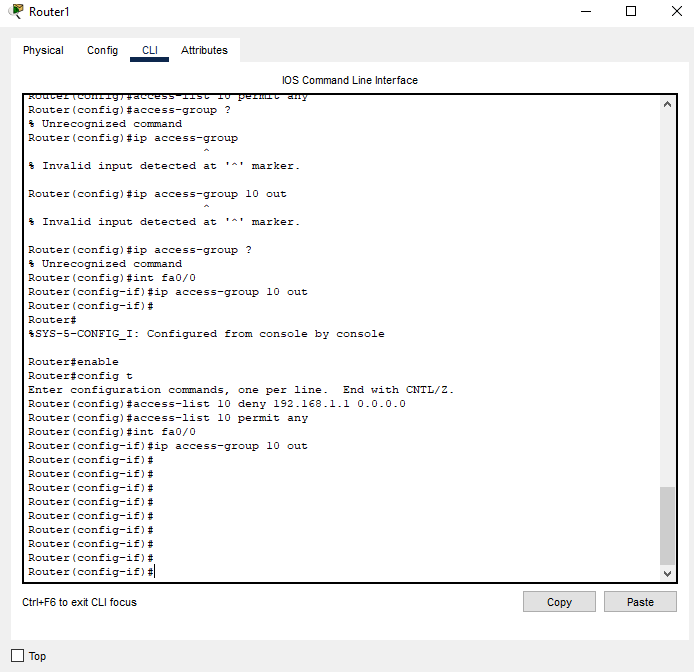
1. **Configure the router and apply ACL rules as follows:-**

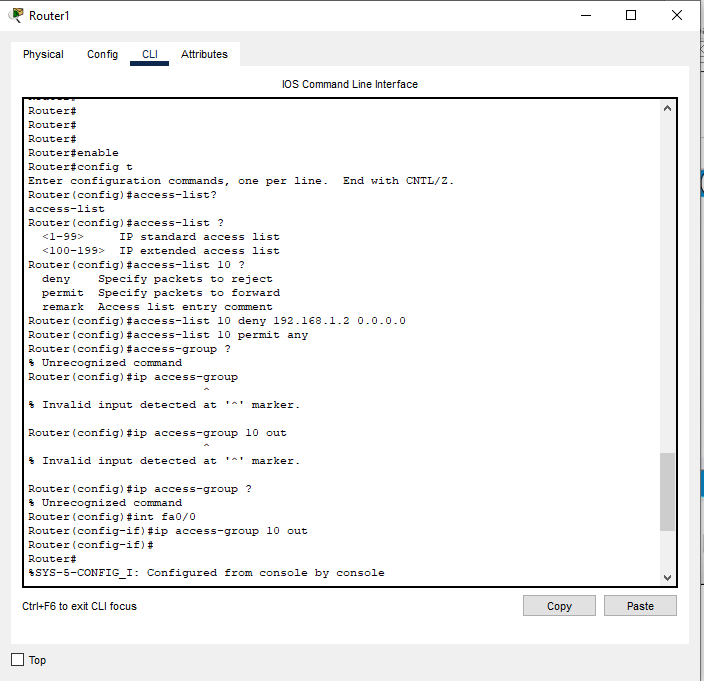
* **192.168.1.2 deny**
* **Permit any**

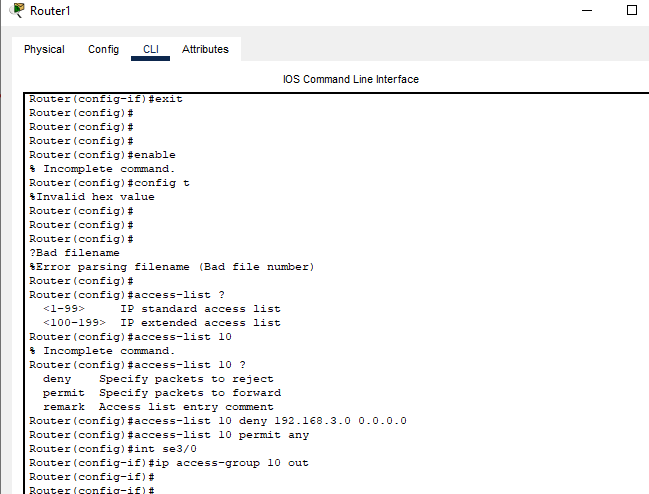
1. **Configure the router and apply ACL rules as follows:-**

* **Deny the host 192.168.1.1 with the network 192.168.2.0**
* **Deny the host 192.168.1.2 with the network 192.168.2.0**
* **Deny the host 192.168.3.0 with the network 192.168.2.0**
* **Permit all the remaining traffic**

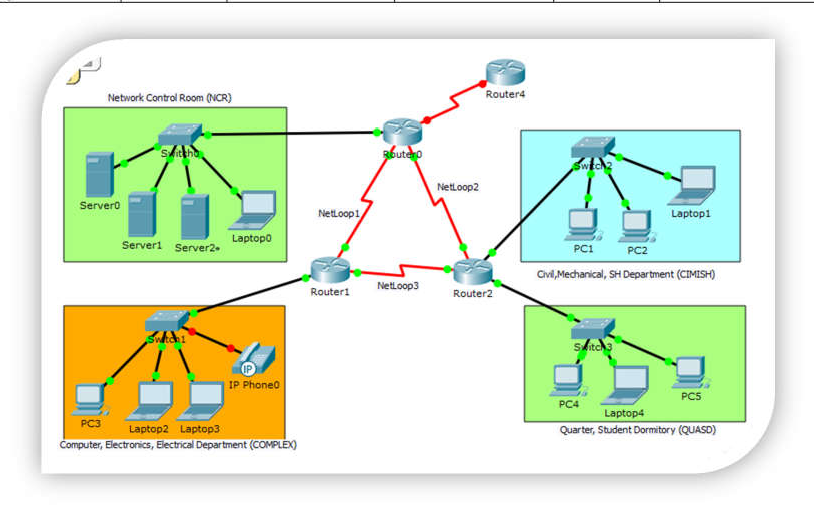








|  |  |  |
| --- | --- | --- |
| **Device Name** | **Interface Name** | **IP Address** |
| Router 0 | Serial 0/0/0 | 202.70.91.253/30 |
| Serial 0/0/1 | 202.70.91.249/30 |
| Gig 0/0 | 202.70.91.1/28 |
| Router 1 | Serial 0/0/0 | 202.70.91.254/30 |
| Serial 0/0/1 | 202.70.91.241/30 |
| Gig 0/0 | 202.70.91.17/25 |
| Router 2 | Serial 0/0/0 | 202.70.91.250/30 |
| Serial 0/0/1 | 202.70.91.242/30 |
| Gig 0/0 | 202.70.91.145/26 |
| Gig 0/1 | 202.70.91.209/28 |
| Server 0-3 | Server port | 202.70.91.2-4/28 |
| Laptop 0 | Client port | 202.70.91.5/28 |
| PC3 | Client port | 202.70.91.18/25 |
| Laptop 2-3 | Client port | 202.70.91.19-20/25 |
| PC1 | Client port | 202.70.91.146/26 |
| PC2 | Client port | 202.70.91.147/26 |
| Laptop-1 | Client port | 202.70.91.148/26 |
| PC4 | Client port | 202.70.91.210/29 |
| Laptop-4 | Client port | 202.70.91.211/29 |
| PC5 | Client port | 202.70.91.212/29 |



|  |  |
| --- | --- |
| **On Router-0, create the following ACL**  *Enable. vbbbbb vb conf ter*  *ip access-list standard 10 deny 202.70.91.16 0.0.0.127*  *deny 202.70.91.208 0.0.0.7*  *permit any ctrl+Z*  *wr* | **On Router-1, create the following ACL**  *enable conf ter*  *ip access-list standard complex deny host 202.70.91.150 permit any*  *ctrl+z wr* |
| **On Router-0, create the following ACL** | After creating those ACLs, now test the connectivity as |
| *enable* | per the requirements (the ACL has not yet been applied) |
| *conf ter* |  |
| *ip access-list standard 20* | **Ping test from pc3 to server 0** |
| *deny 202.70.91.0 0.0.0.15* | PC>ping 202.70.91.2 |
| *deny 202.70.91.16 0.0.0.127* | Pinging 202.70.91.2 with 32 bytes of data: |
| *deny 202.70.91.128 0.0.0.63* | Reply from 202.70.91.2: bytes=32 time=10ms TTL=126 |
| *permit any* | Reply from 202.70.91.2: bytes=32 time=1ms TTL=126 |
| *exit* | Reply from 202.70.91.2: bytes=32 time=1ms TTL=126 |
| *ip access-list standard cimish* | Reply from 202.70.91.2: bytes=32 time=1ms TTL=12 |
| *deny host 202.70.91.146* |  |
| *deny 202.70.91.0 0.0.0.127* |  |

|  |  |
| --- | --- |
| *permit any ctrl+z*  *wr* |  |
| **Ping test from pc1 to server0**  PC>ping 202.70.91.2  Pinging 202.70.91.2 with 32 bytes of data:  Reply from 202.70.91.2: bytes=32 time=2ms TTL=126 Reply from 202.70.91.2: bytes=32 time=1ms TTL=126 Reply from 202.70.91.2: bytes=32 time=1ms TTL=126 Reply from 202.70.91.2: bytes=32 time=1ms TTL=126 | **Ping test from pc4 to server0**  PC>ping 202.70.91.2  Pinging 202.70.91.2 with 32 bytes of data:  Reply from 202.70.91.2: bytes=32 time=2ms TTL=126 Reply from 202.70.91.2: bytes=32 time=1ms TTL=126 Reply from 202.70.91.2: bytes=32 time=1ms TTL=126 Reply from 202.70.91.2: bytes=32 time=1ms TTL=126 |
| **Ping test from pc3 to pc4**  PC>ping 202.70.91.210  Pinging 202.70.91.210 with 32 bytes of data:  Reply from 202.70.91.210: bytes=32 time=1ms TTL=126 Reply from 202.70.91.210: bytes=32 time=1ms TTL=126 Reply from 202.70.91.210: bytes=32 time=1ms TTL=126 Reply from 202.70.91.210: bytes=32 time=1ms TTL=126 | **Ping test from pc1 to pc3**  PC>ping 202.70.91.18  Pinging 202.70.91.18 with 32 bytes of data:  Reply from 202.70.91.18: bytes=32 time=2ms TTL=126 Reply from 202.70.91.18: bytes=32 time=1ms TTL=126 Reply from 202.70.91.18: bytes=32 time=2ms TTL=126 Reply from 202.70.91.18: bytes=32 time=1ms TTL=126 |

Now apply the ACL in to the corresponding interfaces with inbound and outbound settings.

**On router 0, in configuration mode, issue the following acl**

int gig 0/0

ip access-group 10 out

**On router-1, in configuration mode, issue the following acl**

int gig 0/0

ip access-group complex out

**On router-2, in configuration mode, issue the following acl**

int gig 0/0

ip access-group cimish in exit

int gig 0/1

ip access-group 20 out ctrl+z

wr