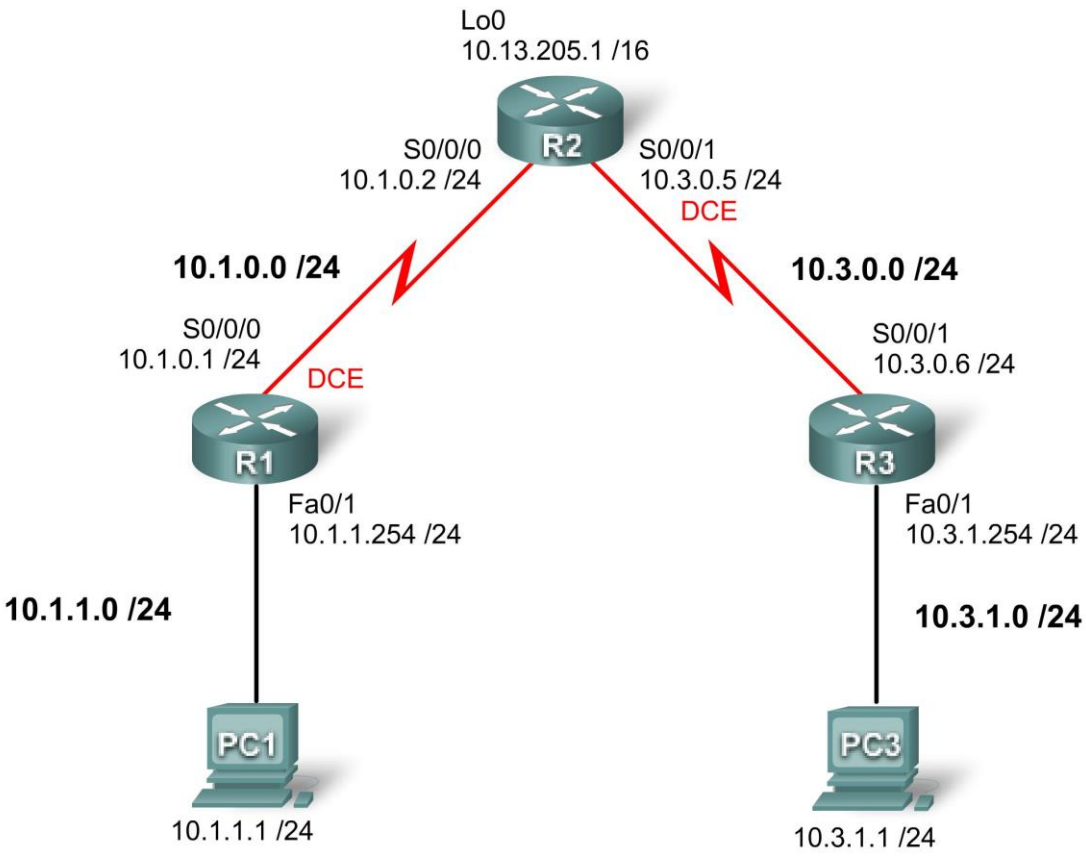
Felix Rohrer

Lab 5.5.3: Troubleshooting Access Control Lists

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**S0/0/0**	10.1.0.1	255.255.255.0	N/A
	Fa0/1	10.1.1.254	255.255.255.0	N/A
R2	**S0/0/0**	10.1.0.2	255.255.255.0	N/A
	S0/0/1	10.3.0.5	255.255.255.0	N/A
	Lo 0	10.13.205.1	255.255.0.0	N/A
R3	**S0/0/1**	10.3.0.6	255.255.255.0	N/A
	Fa0/1	10.3.1.254	255.255.255.0	N/A
PC 1	**NIC**	10.1.1.1	255.255.255.0	10.1.1.254
PC 3	**NIC**	10.3.1.1	255.255.255.0	10.3.1.254

Learning Objectives

To complete this lab:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Load routers with scripts
- Find and correct network errors
- Document the corrected network

Scenario

You work for a regional service provider that has customers who have recently experienced several security breaches. Some security policies have been implemented that haven't addressed the specific needs of the customers. Your department has been asked to examine the configuration, conduct tests and change the configuration as necessary to secure the customer routers.

Ensure that your final configurations implement the following security policies:

- R1 and R3 customers request that only local PCs are able to access VTY lines. Log any attempts by other devices to access the VTY lines.
- R1 and R3 LANs should not be allowed to send or receive traffic to each other. All other traffic should be allowed to and from R1 and R3.

A minimum of ACL statements should be used and applied inbound on the R2 serial interfaces. OSPF is used to distribute routing information. All passwords, except the enable secret password, are set to cisco. The enable secret password is set to **class**.

Task 1: Load Routers with the Supplied Scripts

Your instructor will either load the devices prior to this lab, or provide you with the configs.

done

Task 2: Find and Correct Network Errors

Find and correct all errors in the configuration. Document the steps you used to troubleshoot the network and note each error found.

R1:

- Int S0/0/0 hat eine ACL gesetzt die falsch ist -> löschen
  - `interface Serial0/0/0`
    - `no ip access-group VTY-Local out`
- Line vty hat keine ACL -> ACL setzen
  - `line vty 0 4`
    - `access-class VTY-Local in`
- ACL logging von fehlerhaften versuchen ist nicht aktiviert -> aktivieren
  - `ip access-list standard VTY-Local`
    - `deny any log (log geht in PacketTracer nicht!)`

R2:

- ACL auf S0/0/0 und S0/0/1 sind vertauscht (und out bei R1 falsch) -> beide tauschen, beide “in”:
  - `interface Serial0/0/0`
    - `no ip access-group block-R3 in`
    - `ip access-group block-R1 in`
  - `interface Serial0/0/1`
    - `no ip access-group block-R1 out`
    - `ip access-group block-R3 in`
- ACL block-R1 falsche IP -> bereinigen (Reihenfolge beachten!)
  - `ip access-list extended block-R1`
    - `no deny ip 10.1.1.0 0.0.0.255 10.3.0.0 0.0.0.255`
    - `no permit ip any any`
    - `deny ip 10.1.0.0 0.0.1.255 10.3.0.0 0.0.1.255`
    - `permit ip any any`
- ACL block R3 kein permit für die restlichen Ranges -> hinzufügen
  - `ip access-list extended block-R3`
    - `permit ip any any`

R3:

- ACL falsche IP und fehlendes deny mit log -> korrigieren
  - `ip access-list standard VTY-Local`
    - `no permit 10.3.11.0 0.0.0.255`
    - `permit 10.3.1.0 0.0.0.255`
    - `deny any log (log geht in PacketTracer nicht!)`

Task 3: Document the Corrected Network

Now that you have corrected all errors and tested connectivity throughout the network, document the final configuration for each device.

R1:

```
Current configuration : 1075 bytes
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
no ip domain-lookup
spanning-tree mode pvst
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 ip address 10.1.1.254 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.0.1 255.255.255.0
 clock rate 125000
!
interface Serial0/0/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.1.0.0 0.0.0.255 area 0
 network 10.1.1.0 0.0.0.255 area 0
!
ip classless
!
ip access-list standard VTY-Local
 permit 10.1.1.0 0.0.0.255
 deny any
!
banner motd ^CUnauthorized access strictly prohibited, violators will be prosecuted to the full extent of
the law.^C
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 access-class VTY-Local in
 password cisco
 login
!
```


R2:

```
Current configuration : 1307 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R2
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
spanning-tree mode pvst
!
interface Loopback0
 ip address 10.13.205.1 255.255.0.0
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 10.1.0.2 255.255.255.0
 ip access-group block-R1 in
!
interface Serial0/0/1
 ip address 10.3.0.5 255.255.255.0
 ip access-group block-R3 in
 clock rate 125000
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.1.0.0 0.0.0.255 area 0
 network 10.3.0.0 0.0.0.255 area 0
 network 10.13.0.0 0.0.255.255 area 0
!
ip classless
!
ip access-list extended block-R1
 deny ip 10.1.0.0 0.0.1.255 10.3.0.0 0.0.1.255
 permit ip any any
ip access-list extended block-R3
 deny ip 10.3.0.0 0.0.1.255 10.1.0.0 0.0.1.255
 permit ip any any
!
banner motd ^CUnauthorized access strictly prohibited, violators will be prosecuted to the full extent of
the law.^C
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 login
```


R3:

```
Current configuration : 1056 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R3
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
no ip domain-lookup
spanning-tree mode pvst
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 ip address 10.3.1.254 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/0/1
 ip address 10.3.0.6 255.255.255.0
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.3.0.0 0.0.0.255 area 0
 network 10.3.1.0 0.0.0.255 area 0
!
ip classless
!
ip access-list standard VTY-Local
 permit 10.3.1.0 0.0.0.255
 deny any
!
banner motd ^CUnauthorized access strictly prohibited, violators will be prosecuted to the full extent of
the law.^C
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 access-class VTY-Local in
 password cisco
 login
```

