Touro University - Cybersecurity and Network Administration
Edgar Felipe Valderrama

Network Design for a Small Business
VLANs, ACLs, DHCP, and NAT

The purpose of this project is to design and secure a small-business network using Cisco Packet Tracer. The goal was to segment traffic by departments, enforce least-privilege access, management of IP addresses, and securely simulate internet connectivity. This network was designed to show real-world enterprise practices, including testing and troubleshooting.

Network Architecture: The network supports four departments.

- Management (VLAN 10)
- IT (VLAN 20)
- Sales (VLAN 30)
- Guest (VLAN 40)

VLAN segmentation was implemented to isolate traffic and reduce the attack surface. Also, configuration of Inter-VLAN routing using a router-on-a-stick with 802.1Q trunking protocol between the switch and the router.

Security Controls: To enforce security policies, ACLs were applied on VLAN subinterfaces.

- Guest VLAN was restricted to access internal networks.
- Sales VLAN was blocked from accessing IT resources.
- IT VLAN had full access for administrative purposes.

During the configuration, there were ICMP traffic failures because of stateless ACL behavior. To resolve this issue, I permitted ICMP echo-reply traffic for trusted VLANs without affecting the strict access restrictions.

Network Services:

- Configuration of DHCP on the router to dynamically assign IP addresses in each VLAN; this improved scalability and avoided manual configuration.
- NAT overload (PAT) was implemented to translate private IP addresses to a public interface and simulate secure internet access. Since Packet Tracer has a cloud limitation, the NAT functionality was validated using router translation tables.

Testing: connectivity tests confirm the following

- Good VLAN isolation
- Correct inter-VLAN routing
- Enforcement of access control policies
- DHCP address assignment
- Active NAT translations on outbound traffic

Conclusion: With this project, I applied my skills obtained during different courses that helped me with a strong foundation in network administration, cybersecurity, troubleshooting, and technical documentation that is necessary in the real world.

Touro University - Cybersecurity and Network Administration
Edgar Felipe Valderrama

Network Topology: small business network topology with VLAN segmentation and router-on-a-stick architecture (Packet Tracer workspace view). Figure1

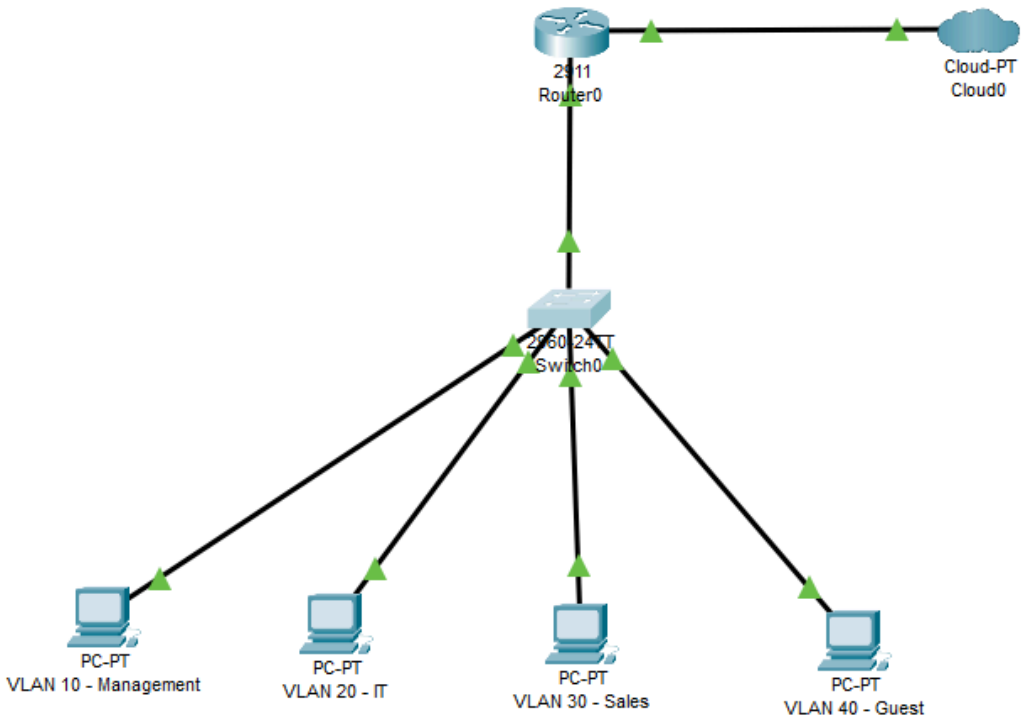

Figure 1

VLAN Configuration: VLAN configuration and access port assignments on the switch. Figure 2

```
Switch>show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Gig0/1
                                                 Gig0/2
10   Management                        active    Fa0/1
20   IT                                active    Fa0/2
30   Sales                             active    Fa0/3
40   Guest                             active    Fa0/4
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch>
```

Figure 2

Inter-VLAN Routing: Router subinterfaces configured for inter-VLAN routing. Figure 3

```
Router>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/0.10  192.168.10.1    YES manual up                    up
GigabitEthernet0/0.20  192.168.20.1    YES manual up                    up
GigabitEthernet0/0.30  192.168.30.1    YES manual up                    up
GigabitEthernet0/0.40  192.168.40.1    YES manual up                    up
GigabitEthernet0/1     209.165.200.226 YES manual up                    up
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router>
```

Figure 3

ACL Configuration: Extended ACLs enforcing least-privilege access between VLANs. Figure 4

```
Router>enable
Router#show ip access-lists
Extended IP access list 130
    10 permit icmp 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255 (4 match(es))
    20 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
    30 permit ip any any (2 match(es))
    40 permit icmp 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255 echo-reply
Extended IP access list 140
    10 permit icmp 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255 echo-reply (4 match(es))
    20 deny ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255 (4 match(es))
    30 deny ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255
    40 deny ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255
    50 permit ip any any (14 match(es))
Standard IP access list 1
    10 permit 192.168.0.0 0.0.255.255
```

Figure 4

DHCP Verification: DHCP-assigned IP address from the correct VLAN scope. Figure 5

```
Router>
Router>show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.10.2     0010.1145.3725           --                     Automatic
192.168.20.2     0001.C9C1.5524           --                     Automatic
192.168.30.2     00D0.974E.7B06           --                     Automatic
192.168.40.2     0001.64EE.2D5E           --                     Automatic
Router>
```

Figure 5

Testing

Ping from Guest to Management failed because it doesn't have access to internal networks. Figure 6

```
C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 6

Ping from the internal network, in this case from IT to Sales, is successful. Figure 7

```
C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 7