NETWORKING PROJECT SUBMISSION

SECTION 1 – Student Information

Name: Alex Ayoola

Module: Introduction to Networking

Assignment Title: Small Office Network Configuration with ACL and HTTP Access Control

Date Submitted: 30/11/2025

SECTION 2 – Objective / Executive Summary

The goal of this project is to design and configure a routed small office network for DataBridge Innovations, featuring three departments — Admin, Sales, and HR. The network demonstrates how to implement core services such as DHCP, DNS, and HTTP, and how to apply Access Control Lists (ACLs) to control interdepartmental access. Only Admin and Sales departments should access the Admin Web Server, while the HR department should be denied. This setup illustrates secure traffic management and proper network segmentation.

SECTION 3 – Network Design

The topology consists of:

- Router (R1) connecting three departmental LANs
- Three switches (Admin, Sales, HR)
- Two servers:
  • Admin Server (DHCP/DNS) – 192.168.10.2
  • Admin Web Server (HTTP) – 192.168.10.5
- Six PCs (two per department)

Department	Subnet	Gateway	Role
Admin	192.168.10.0/24	192.168.10.1	DHCP/DNS/Web access
Sales	192.168.20.0/24	192.168.20.1	Limited access
HR	192.168.30.0/24	192.168.30.1	Internet only

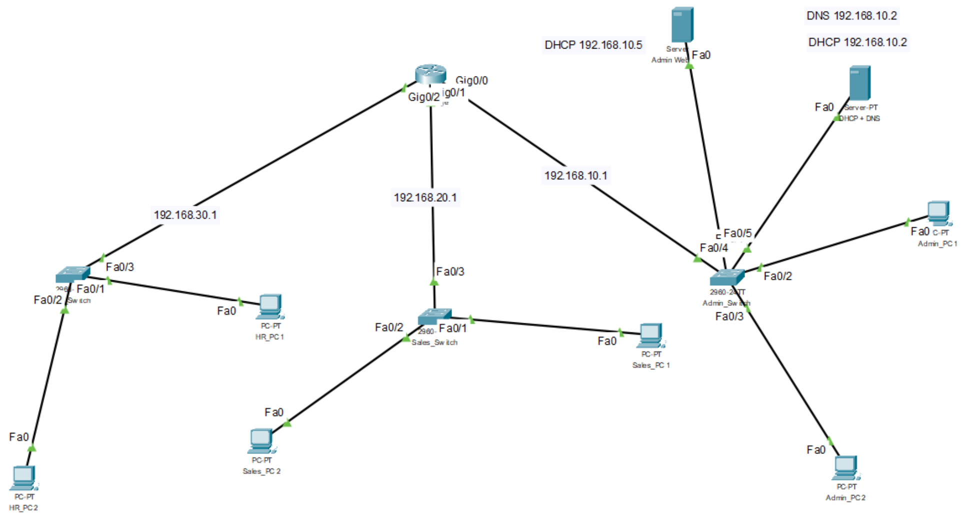


Figure 01: Screenshot of Packet Tracer topology (showing all IPs and connections).

SECTION 4 – Configuration Steps

Router Configuration (R1):

```
enable
configure terminal
interface Gig0/0
 ip address 192.168.10.1 255.255.255.0
 no shutdown
exit
interface Gig0/1
 ip address 192.168.20.1 255.255.255.0
 ip helper-address 192.168.10.4
 no shutdown
exit
interface Gig0/2
 ip address 192.168.30.1 255.255.255.0
 ip helper-address 192.168.10.4
 no shutdown
exit
ip access-list extended HR_ACL
 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
 permit ip 192.168.30.0 0.0.0.255 any
exit
interface gigabitEthernet0/2
 ip access-group HR_ACL in
exit
```

```
ip access-list extended SALES_ACL
 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
 permit ip 192.168.20.0 0.0.0.255 any
exit
interface gigabitEthernet0/1
 ip access-group SALES_ACL in
exit
end
write memory
```

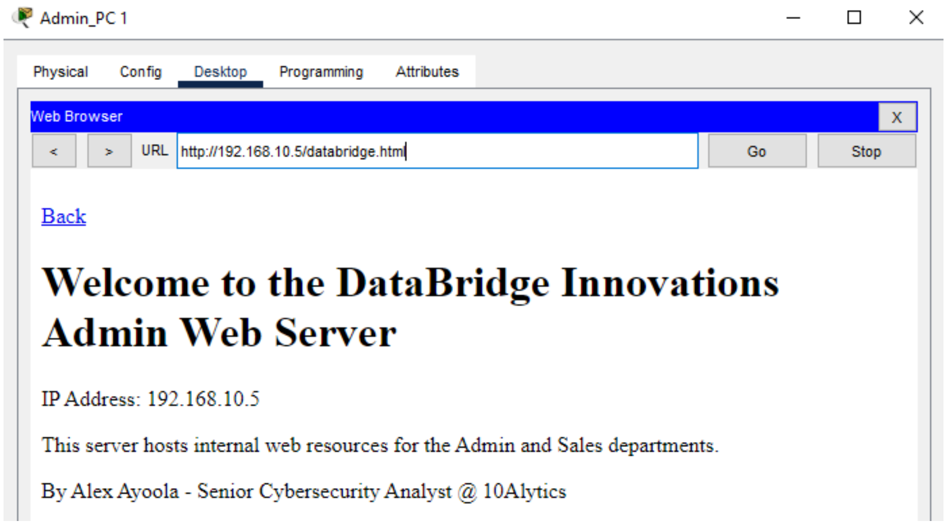
Admin Web Server (192.168.10.5):

IP Address: 192.168.10.5
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.10.1
DNS Server: 192.168.10.5
HTTP Service: Enabled

SECTION 5 – Screenshots

Screenshots showing:

1. Successful HTTP access from Admin and Sales



URL: http://192.168.10.5/databridge.html

Back

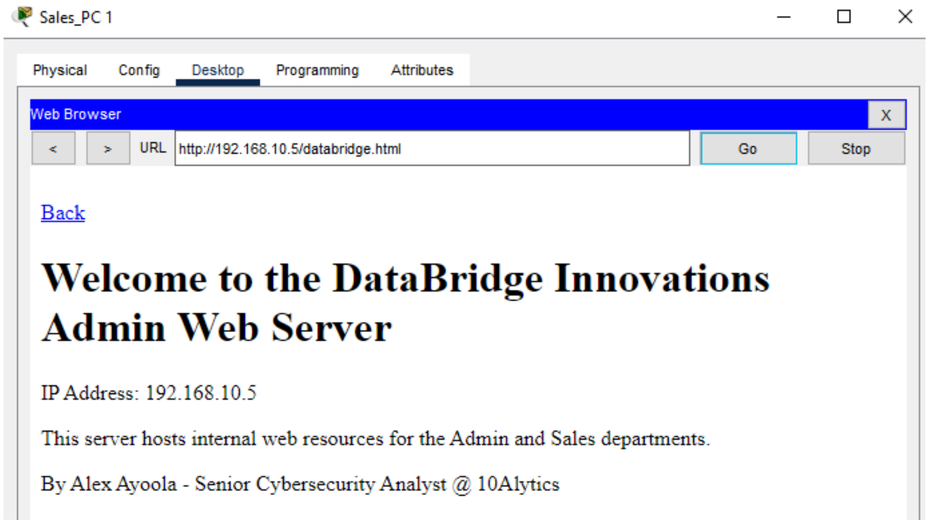
Welcome to the DataBridge Innovations Admin Web Server

IP Address: 192.168.10.5

This server hosts internal web resources for the Admin and Sales departments.

By Alex Ayoola - Senior Cybersecurity Analyst @ 10Alytics

Figure 02: Successful HTTP access from Admin_PC1



Welcome to the DataBridge Innovations Admin Web Server

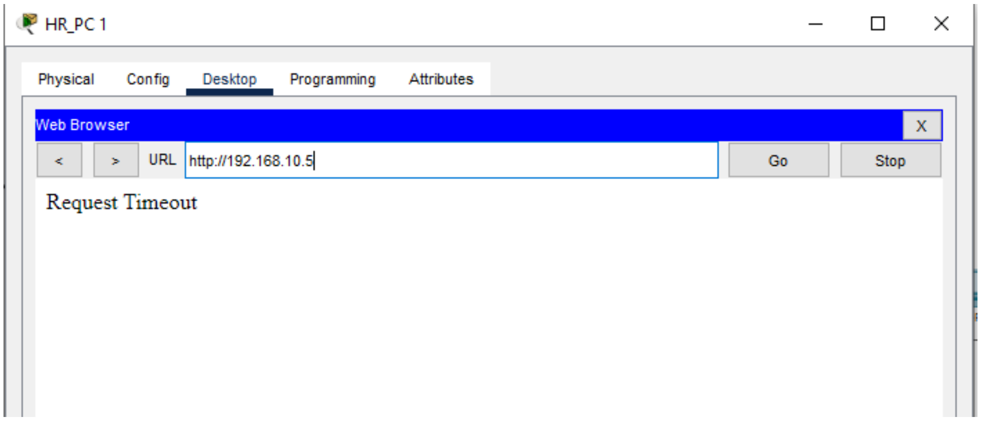
IP Address: 192.168.10.5

This server hosts internal web resources for the Admin and Sales departments.

By Alex Ayoola - Senior Cybersecurity Analyst @ 10Alytics

Figure 03: Successful HTTP access from Sales_PC1

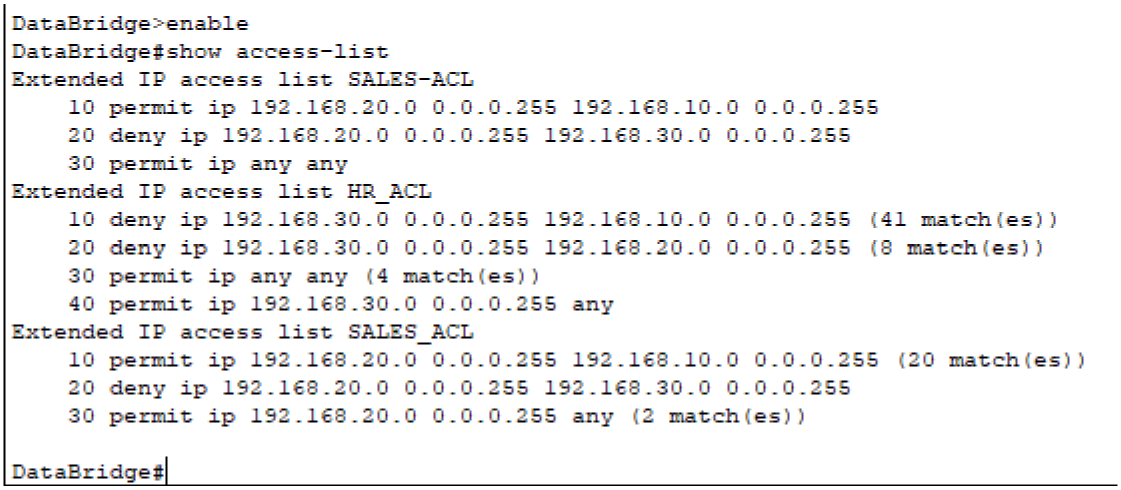
2. Denied access from HR



Request Timeout

Figure 04: Denied HTTP access from HR_PC1

3. Router ACL verification using 'show access-lists'



```
DataBridge>enable
DataBridge#show access-list
Extended IP access list SALES-ACL
    10 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
    20 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
    30 permit ip any any
Extended IP access list HR_ACL
    10 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255 (41 match(es))
    20 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255 (8 match(es))
    30 permit ip any any (4 match(es))
    40 permit ip 192.168.30.0 0.0.0.255 any
Extended IP access list SALES_ACL
    10 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255 (20 match(es))
    20 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
    30 permit ip 192.168.20.0 0.0.0.255 any (2 match(es))

DataBridge#
```

Figure 05: Router ACL verification (Output: **show access-lists** command)

SECTION 6 – Explanation

Access Control Lists (ACLs) were used to secure internal resources by filtering network traffic based on IP and protocol. The Admin Web Server was configured to accept HTTP traffic only from the Admin and Sales subnets, while the HR subnet was completely denied. This ensures that unauthorized users cannot reach sensitive internal systems, demonstrating how ACLs enhance network security and enforce departmental boundaries.

SECTION 7 – Conclusion

The project successfully demonstrated a multi-department office network using Cisco Packet Tracer. Through proper IP addressing, DHCP/DNS configuration, and ACL enforcement, the network achieved secure and efficient communication. The application of ACLs improved traffic control and protected internal assets, highlighting their importance in real-world network management and security.