Computer Communication Networks: CT-376

Design and Implementation of a Secure and Scalable Airport Network Infrastructure

Group Members:

Ayesha Yousuf (CR-22004)
Sheheryar Amir (CR-22008)
Maryam Khan (CR-22021)
Abdullah Khalid (CR-22027)

1. Overview

This report presents the design of a comprehensive and secure network infrastructure for a modern airport environment. The network leverages advanced technologies such as VLANs, Telnet, ACLs, Eth-Trunk, Static Routing, RIP, STP, DHCP, and FTP. These configurations ensure smooth communication, efficient resource utilization, scalability, and security within and across departments operating within the airport.

2. Scenario: Airport Network Design

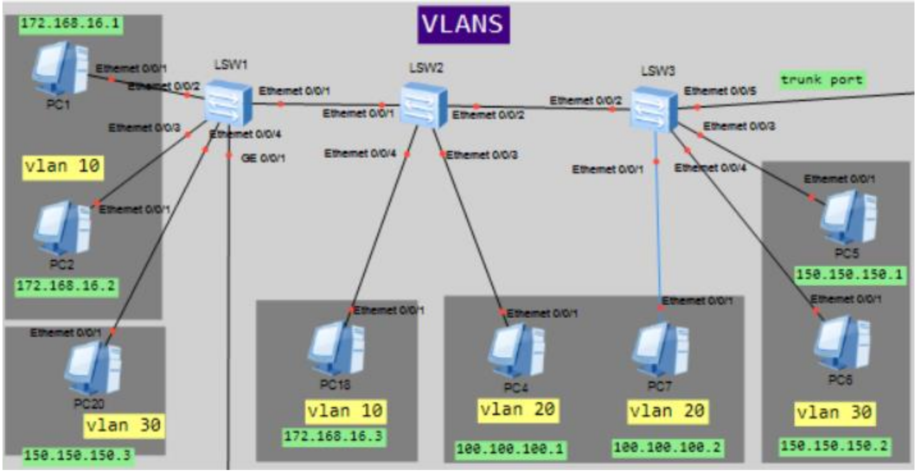
In this project, we designed a network for an international airport. Each networking feature is aligned with a specific department to meet their unique operational requirements. The goal is to build a robust network that supports airline operations, passenger services, administrative functions, and technical infrastructure.

Departments and Assigned Networking Features:

Airport Department	***Network Technology Used***
Airport Operations (Control Room)	*VLANs*
Financial Services	*Router-on-a-Stick*
IT Support (Infrastructure & Security)	*Static Routing & Telnet*
Data Center (Servers and Storage)	*Link Aggregation (Eth-Trunk)*
Customer Services	*Spanning Tree Protocol (STP)*
Human Resource Department	*Subnetting (VLSM)*
Research and Development (Airport R&D)	*RIP*
Airport-wide Public Wi-Fi Access	*DHCP*
Inter-Departmental Communication	*Inter-VLAN Routing with Layer 3*

3. Network Features & Justifications

VLANs – Airport Operations (Control Room)



Description:
Virtual Local Area Networks (VLANs) are a method of logically segmenting a physical network into multiple broadcast domains, even if the devices are physically connected to the same switch. In the airport's **Operations Department***, which includes critical teams such as:*

- ***Ground Services*** *(baggage handling, vehicle coordination)*
- ***Air Traffic Communication*** *(coordination with control towers)*
- ***Gate Management*** *(boarding processes, flight updates)*

Each of these sub-departments is assigned its own VLAN (e.g., VLAN 10 for Ground Services, VLAN 20 for Air Traffic, VLAN 30 for Gate Management).

This logical separation ensures that network traffic from one operational area does not interfere with others, and broadcast traffic is limited to each VLAN. Devices in VLAN 10 can't directly communicate with those in VLAN 20 or VLAN 30 unless explicitly allowed via routing (Layer 3).

Justification:
The Operations Department is the ***backbone of real-time airport activities****, and any delays or interference could cause* ***safety risks or operational disruptions****. Using VLANs in this department offers the following key benefits:*

- ***Security Isolation****:*
  Each team handles sensitive data (e.g., flight control commands or passenger gate information). VLANs isolate this data from unauthorized users and departments, reducing the risk of data leaks or internal misuse.
- ***Minimized Network Congestion****:*
  By containing broadcast traffic within a VLAN, there's less congestion on the overall

network, ensuring fast and reliable data transmission – which is crucial for time-sensitive operations like runway clearance or boarding announcements.

- ***Policy Enforcement and Access Control**:*
  Network administrators can apply policies at the VLAN level, such as allowing only certain services or protocols, which adds a layer of control over how different teams operate and what they can access.
- ***Scalability and Flexibility**:*
  As the airport grows or new services are introduced (e.g., a new boarding gate system), additional VLANs can be created without altering the physical infrastructure. This makes the network more adaptable to future needs.
- ***Failure Isolation**:*
  If a misconfiguration or attack affects one VLAN (e.g., a DoS attack on baggage systems), it doesn't impact other VLANs like air traffic communications, preserving overall system integrity.

Configuration:

*Three Layer 2 switches (LSW1, LSW2, and LSW3) were configured with **VLANs 10, 20, and 30**. Each switch is connected to multiple PCs, and each PC is assigned to a specific VLAN based on its department or role. The steps taken are:*

✓ ***PC-to-Switch Connections**:*

- *Multiple PCs were connected to each switch using Ethernet ports.*
- *PCs were assigned IP addresses from separate subnets according to their VLANs.*

✓ ***VLAN Creation**:*

VLANs 10, 20, and 30 were created on each switch using:

▪ *system-view*
▪ *vlan batch 10 20 30*

✓ ***Access Port Configuration**:*

Interfaces connected to PCs were configured as access ports and assigned to the appropriate VLAN:

▪ *interface Ethernet0/0/x*
▪ *port link-type access*
▪ *port default vlan <VLAN-ID>*

✓ ***Trunk Port Configuration**:*

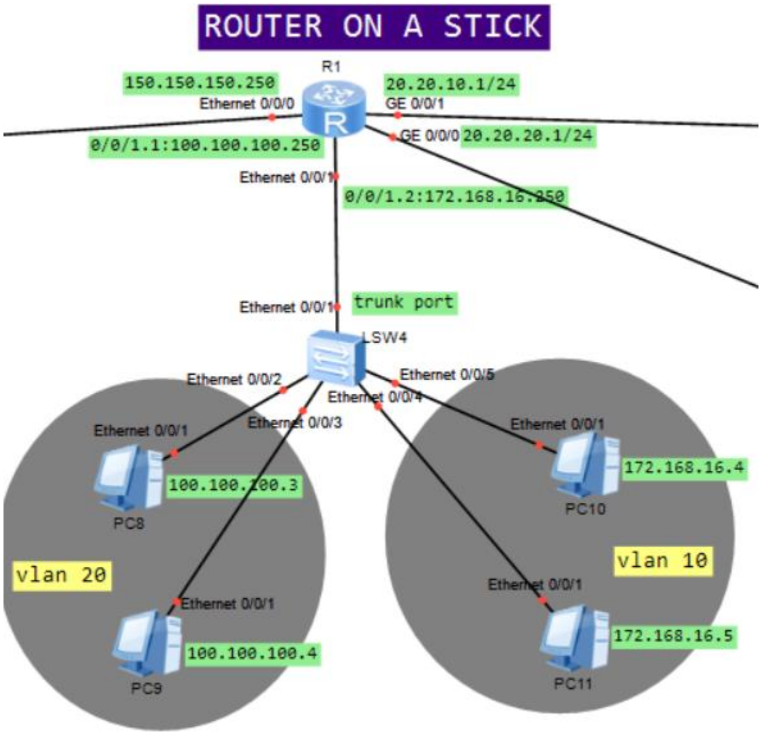
Interfaces connecting switches to each other were configured as trunk ports to allow VLAN traffic to pass between them:

▪ *interface Ethernet0/0/x*

        - *port link-type trunk*
        - *port trunk allow-pass vlan 10 20 30*
- ✓ ***Connectivity Testing**:*

    - *PCs within the **same VLAN** across different switches were able to communicate (ping success).*
    - *PCs in **different VLANs** could **not communicate**, as inter-VLAN routing was not yet configured.*

Router-on-a-Stick – Financial Services



Description:

Each of these teams is placed into its own VLAN (e.g., VLAN 10 for Payroll, VLAN 20 for Billing) to isolate their traffic for security and efficiency. However, these teams still require intercommunication to share financial records, access centralized systems, and generate consolidated reports.

*To allow communication between these VLANs without using multiple physical routers, the **Router-on-a-Stick** technique is employed. This involves configuring a **single physical interface** on a router with **multiple subinterfaces**, each corresponding to a VLAN. Each subinterface is configured with a unique IP address that acts as the default gateway for devices in that VLAN.*

*This setup enables **Layer 3 routing** between VLANs on the same router, facilitating secure and controlled communication across financial teams.*

Justification:

- ***Cost-Effective Solution****:*
  Eliminates the need to deploy multiple routers, reducing both capital and operational costs.
- ***Secure Inter-VLAN Routing****:*
  Subinterfaces can be tightly controlled through access control lists (ACLs), ensuring that only authorized communication occurs between teams.
- ***Efficient Use of Router Hardware****:*
  One physical interface can support multiple VLANs, maximizing hardware utilization.
- ***Centralized Routing****:*
  Easier to manage and troubleshoot inter-VLAN routing when all logic is handled through one router interface.
- ***Scalability****:*
  Additional VLANs can be added later by simply defining more subinterfaces—ideal for dynamic airport environments where financial operations may expand.

Configuration:

- *system-view*
- *sysname R1*

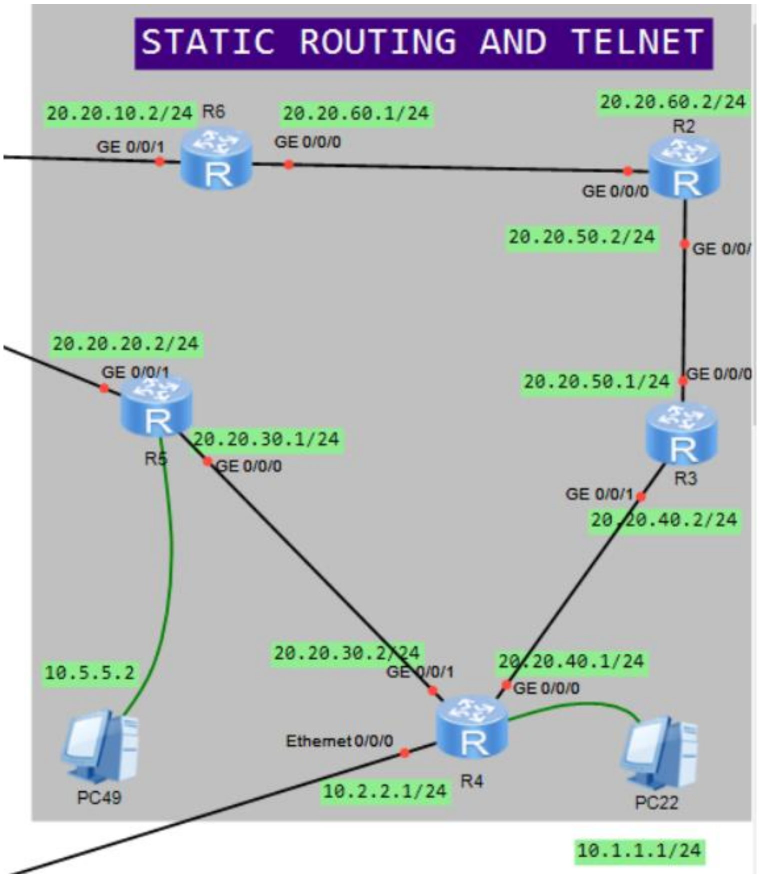
✓ ***Sub-interface for VLAN 10***

- *interface Ethernet 0/0/1.1*
- *vlan-type dot1q 10*
- *ip address 100.100.100.150 255.255.255.0*
- *quit*

✓ ***Sub-interface for VLAN 20***

- *interface Ethernet 0/0/1.2*
- *vlan-type dot1q 20*
- *ip address 100.100.100.250 255.255.255.0*

Static Routing & Telnet – IT Support Department



Description:

*The **IT Support Department** oversees the internal infrastructure of the airport's digital systems. These include ticketing servers, technical support workstations, monitoring equipment, and database services. The department is segmented into **multiple zones** (e.g., ticketing zone, backend server zone, support operations zone), each residing in different subnets.*

*To ensure **direct and controlled traffic flow** between these zones, **static routing** is implemented. Each router is manually configured with specific routes, allowing traffic to take only predefined paths, reducing overhead and improving predictability.*

*Additionally, to facilitate **remote device management**, **Telnet** is enabled across networking devices. IT administrators can remotely connect to switches and routers, perform configurations, and monitor operations from a central management system.*

Justification:

- ***Path Predictability**:*
  Static routes allow full control over the data path, reducing the risk of unexpected routing changes and ensuring reliable connectivity in critical IT systems.

- ***Improved Security and Simplicity**:*
  Since routes are manually defined, there's less risk of accidental exposure through dynamic protocol misconfiguration.
- ***Ideal for Small, Stable Networks**:*
  The IT zones in the airport have relatively fixed topology, making static routing an optimal solution.
- ***Remote Management via Telnet**:*
  Telnet provides command-line remote access, enabling IT staff to troubleshoot and configure devices from any part of the airport network.
- ***No Need for Dynamic Routing Protocol Overhead**:*
  Reduces router CPU and memory usage, which is essential in segments not expected to frequently change.

Configuration:

- ✓ *Establish connections between all six routers as shown in the topology to ensure direct links are active.*
- ✓ *Assign IP addresses to each router interface so that neighboring routers on the same network segment can successfully communicate.*
- ✓ *On **Router R1**, configure the following static routes to enable connectivity to remote networks:*

  - *Route to 20.20.60.0/24 via next hop 20.20.10.2*
  - *Route to 20.20.30.0/24 via next hop 20.20.20.2*
  - *Route to 20.20.50.0/24 via next hop 20.20.60.2*
  - *Route to 20.20.40.0/24 via next hop 20.20.30.2*

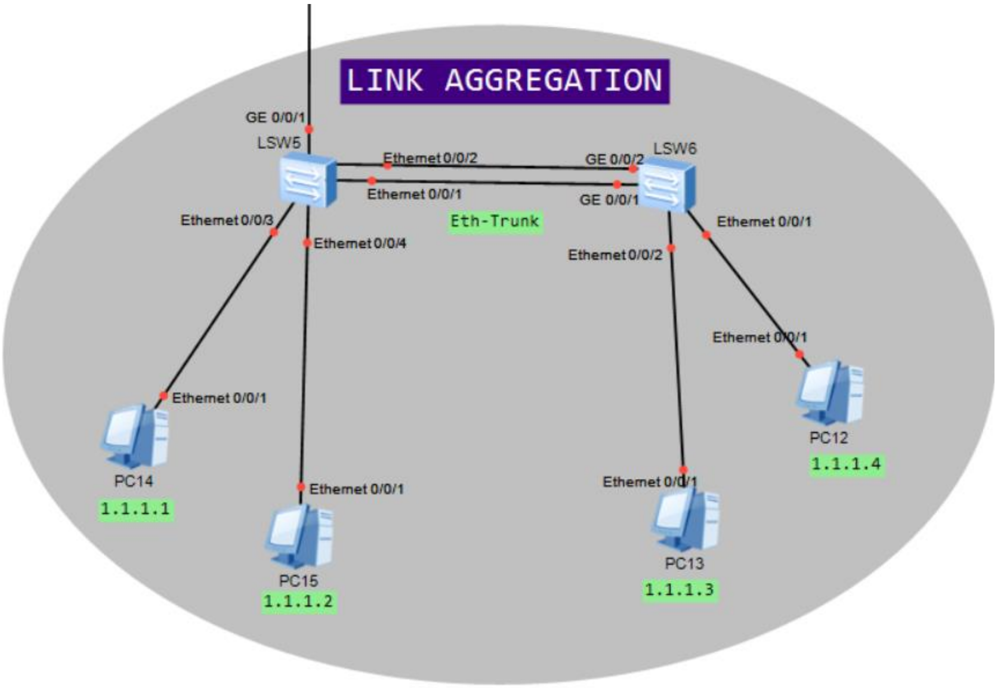
- ✓ *Use the ping command on the routers to test reachability between various networks and verify that routing is functioning properly.*
- ✓ *For **Telnet setup**, connect PCs (PC22 and PC49) to their respective routers using a console cable.*
- ✓ *On each router connected to a PC, enter the following commands to enable Telnet access:*

  - *Enable Telnet service: telnet server enable*
  - *Access VTY lines: user-interface vty 0 4*
  - *Set login method: authentication-mode password*
  - *Define a password with encryption: set authentication password cipher <your_password>*
  - *Assign administrative privileges: user privilege level 15*
  - *Exit configuration mode with quit*

- ✓ *Finally, switch to the **Console tab** on the PC connected to the router, and use the Telnet client to test connectivity by entering:*

  - *telnet <router_ip_address>*

Eth-Trunk – Data Center



Description:

In the ***Data Center****, high-performance operations depend on robust, uninterrupted connections between core switches and servers.* ***Eth-Trunk*** *technology (Link Aggregation) combines multiple physical links into one logical connection, allowing traffic to balance across multiple interfaces.*

Justification:

- ***Increased Bandwidth****: Combines throughput of all trunked links.*
- ***Fault Tolerance****: If one link fails, traffic continues through remaining ones.*
- ***Load Balancing****: Traffic is intelligently distributed to prevent bottlenecks.*
- ***Simplified Management****: Treated as a single interface by the system.*

Configuration Summary:

✓ *By assigning IP addresses to all PCs that are connected to the respective switches.*

✓ *Proceed to configure* ***link aggregation*** *on both switches. Start by entering system view mode and creating an* ***Eth-Trunk*** *interface using the following commands:*

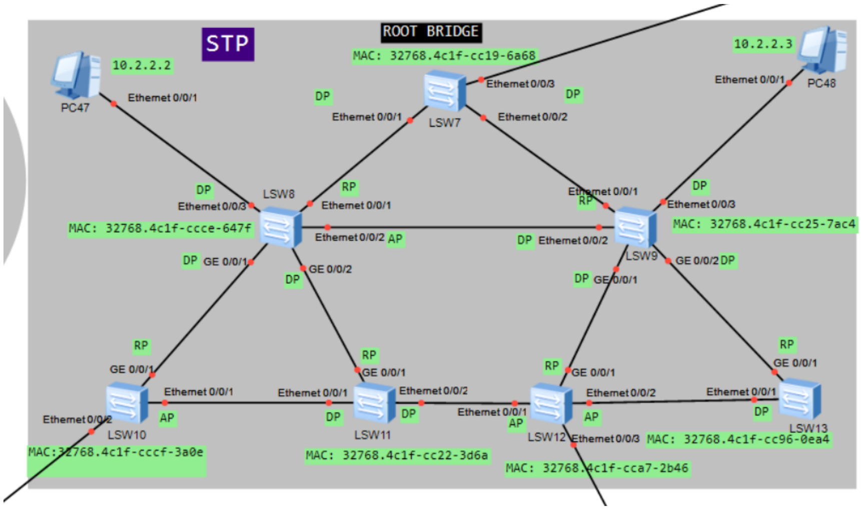
- *system-view*
- *interface Eth-Trunk 1*

✓ *After creating the trunk, configure all physical interfaces that connect the two switches to be part of this trunk by entering:*

- *Eth-Trunk 1 under each of those interface settings.*

✓ *Once configuration is complete, test the scenario by checking connectivity between devices. If successful, the **link aggregation** between LSW5 and LSW6 is working properly.*

STP – Customer Services



Description:
*The **Customer Services Department** relies on multiple redundant switch links for availability. **Spanning Tree Protocol (STP)** prevents Layer 2 loops that could crash the netwo*

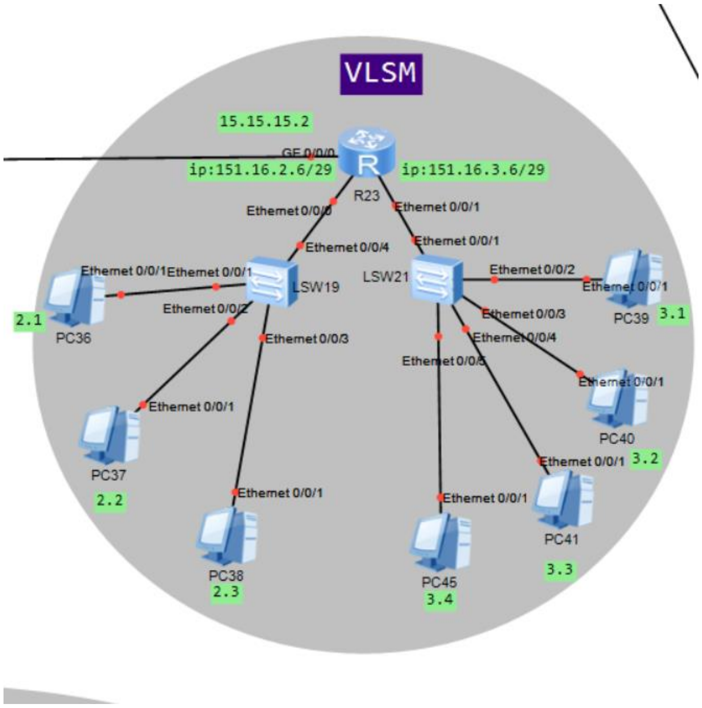
Justification:

- ***Loop Prevention**: Automatically disables redundant paths to avoid broadcast storms.*
- ***High Availability**: Re-enables backup paths when the primary fails.*
- ***Zero Downtime**: Essential for real-time customer communication.*

Configuration Summary:

Component	***Description***
Root Bridge	*The central switch in the STP topology, elected based on the lowest Bridge ID (a combination of priority value and MAC address).*
Root Port	*The interface on a non-root switch that offers the most efficient (lowest-cost) path to reach the root bridge. Only one root port per switch.*
Designated Port	*These ports forward traffic toward the root bridge. One designated port exists per network segment, offering the best path to the root.*
Alternate Port	*Backup ports that remain in a blocking state and only become active if a designated or root port fails, ensuring path redundancy in the network.*

Subnetting (VLSM) – HR Department



Description:
The ***HR Department*** *handles diverse functions such as payroll, recruitment, and employee databases.* ***Variable Length Subnet Masking (VLSM)*** *divides a single IP block into efficient subnets tailored to specific needs.*

Justification:

- ***Efficient IP Allocation****: Prevents IP waste.*
- ***Logical Segmentation****: Each HR module is logically separated for security and management.*
- ***Scalability****: Easier to expand subnets independently.*

Configuration Summary:

Devices Involved: *Router R23, Switches LSW19 and LSW21*

We're working with two separate IP networks: ***151.16.2.0/29*** *and* ***151.16.3.0/29****, each designated for a small group of hosts (3 and 4 respectively).*

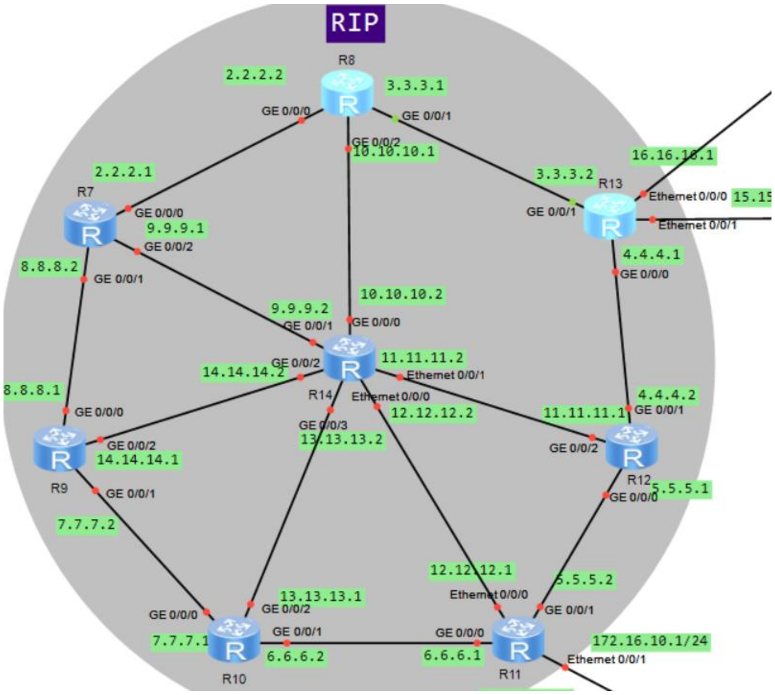
Subnet Details:

- ***First Network – 151.16.2.0/29***
  Designed for a setup requiring 3 host IPs. A subnet with 8 total addresses (6 usable) meets this need.
  - ***Subnet Mask:*** *255.255.255.248*
  - ***IP Range:*** *151.16.2.0 to 151.16.2.7*
- ***Second Network – 151.16.3.0/29***
  Configured for 4 hosts. Just like the first, a /29 subnet provides enough usable addresses.
  - ***Subnet Mask:*** *255.255.255.248*
  - ***IP Range:*** *151.16.3.0 to 151.16.3.7*

Steps to Set Up:

1. ***PC to Switch Connectivity:***
   Connect a group of PCs to LSW19 and LSW21. Assign each switch a different subnet — one for each calculated IP range.
2. ***PC Configuration:***
   Manually assign each PC an appropriate IP address, subnet mask, and default gateway that corresponds to its respective subnet.
3. ***Switch to Router Integration:***
   Link the switches to router R23. Each subnet's gateway should be configured on the router interface linked to the relevant switch.
   - *Example:*
     - *Interface Ethernet0/0/0 → IP address: 151.16.2.6 with Subnet Mask: 255.255.255.248 (used as the gateway for the 151.16.2.0/29 subnet)*

RIP – Airport R&D



Description:

*The **Research & Development (R&D)** department operates in a dynamic, isolated network environment where frequent changes in topology occur due to testing, prototyping, and experimental setups. The use of **Routing Information Protocol (RIP)** provides a simple and effective way to ensure connectivity between different routers within this testbed.*

*RIP is a **distance-vector dynamic routing protocol** that allows routers to automatically share and update their routing tables. It uses **hop count as a routing metric**, meaning it chooses paths with the least number of intermediate routers.*

In this R&D context, RIP ensures that new routers or topology changes are quickly propagated throughout the test network without the need for manual route configuration.

Justification:

- ***Automation in Route Management**:*
  R&D networks often undergo constant structural changes. RIP dynamically advertises routing updates every 30 seconds, reducing manual intervention.
- ***Simplicity and Lightweight Operation**:*
  RIP is easy to configure and maintain, making it ideal for experimental or temporary setups where simplicity and speed matter more than scalability.
- ***Loop Prevention with Split Horizon and Hold-down Timers**:*
  *RIP employs basic techniques like **split horizon** and **route poisoning** to avoid routing loops, which are crucial in environments with frequent reconfiguration.*

- ***Isolation Compatibility**:*
  Since R&D networks are usually not connected to the production environment, RIP's limitations (such as a maximum of 15 hops) are not a concern, making it suitable and secure for internal experiments.
- ***Low Resource Usage**:*
  RIP's simple operations don't demand high processing power or memory, which is ideal for lightweight lab routers or virtual test devices used in R&D.

RIP Configuration (on R7 to R14):

1. Assign IP Addresses

*Manually assign appropriate IP addresses and subnet masks to all router interfaces **before** proceeding.*

2. Enter Configuration Mode and Enable RIP

*On **each router (R7 to R14)**, run the following:*

- *system-view*
- *rip 1*

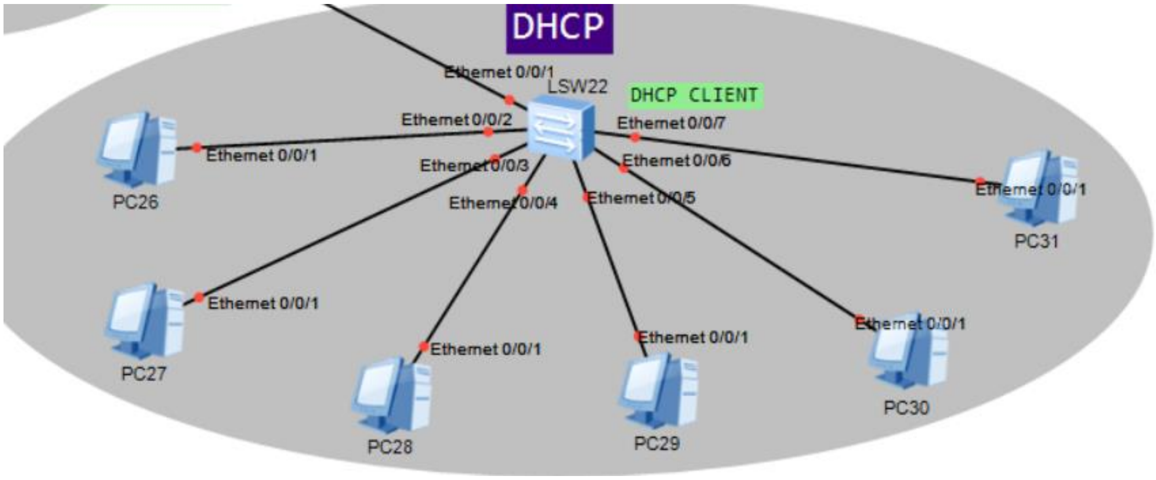
3. Advertise Connected Networks

*Use the network command for **each subnet directly connected to that router**. Below is an **example for R7**:*

- *network 2.0.0.0*
- *network 8.0.0.0*
- *network 9.0.0.0*

*Repeat these commands on **each router** with the correct network values based on its interfaces.*

DHCP – Airport-wide Wi-Fi



Description:

Dynamic Host Configuration Protocol (DHCP) *is a network management protocol used to automatically assign IP addresses and other network configuration parameters to devices on a network. In the airport's public Wi-Fi scenario, DHCP plays a crucial role in enabling seamless connectivity for thousands of transient users like passengers, visitors, and staff using mobile devices and laptops.*

Instead of requiring manual configuration on each device, DHCP allows client devices to ***automatically obtain an IP address, subnet mask, default gateway, and DNS information*** *from a DHCP server as soon as they connect to the Wi-Fi network. This not only reduces configuration time but also ensures that IP address allocation is efficient and conflict-free*

Justification

- ***Scalability for High User Volume****:*
  Airports have a high density of users connecting and disconnecting frequently. DHCP supports ***automatic, real-time IP assignment****, making it highly scalable for fluctuating demand.*
- ***Ease of Use for Public Users****:*
  Most users of public Wi-Fi are non-technical. DHCP enables ***plug-and-play connectivity****, requiring no user-side configuration.*
- ***Efficient IP Address Management****:*
  Through IP lease times, DHCP ensures that unused IP addresses are returned to the pool for reuse, avoiding exhaustion in large networks.
- ***Reduced Administrative Overhead****:*
  Network administrators don't need to assign static IPs manually to every device, which is impractical in large or dynamic environments like public Wi-Fi.

- ***Centralized Control and Policy Enforcement****:*
  DHCP servers can be configured to apply policies such as assigning IPs from different pools, enforcing time-based access limits, or segregating guest and staff users.

Configuration Summary:

```
dhcp enable
ip pool airport_wifi
network 192.168.50.0 mask 255.255.255.0
```

Step 1: Configure PCs (Connected to LSW22)

Step 2: Configure DHCP on R11 (Router acting as DHCP Server)

- *system-view*
- *dhcp enable*
- *ip pool airport_wifi*
- *network 192.168.50.0 mask 255.255.255.0*

Step 3: Assign IP Address to Router Interface (Gateway for Clients)

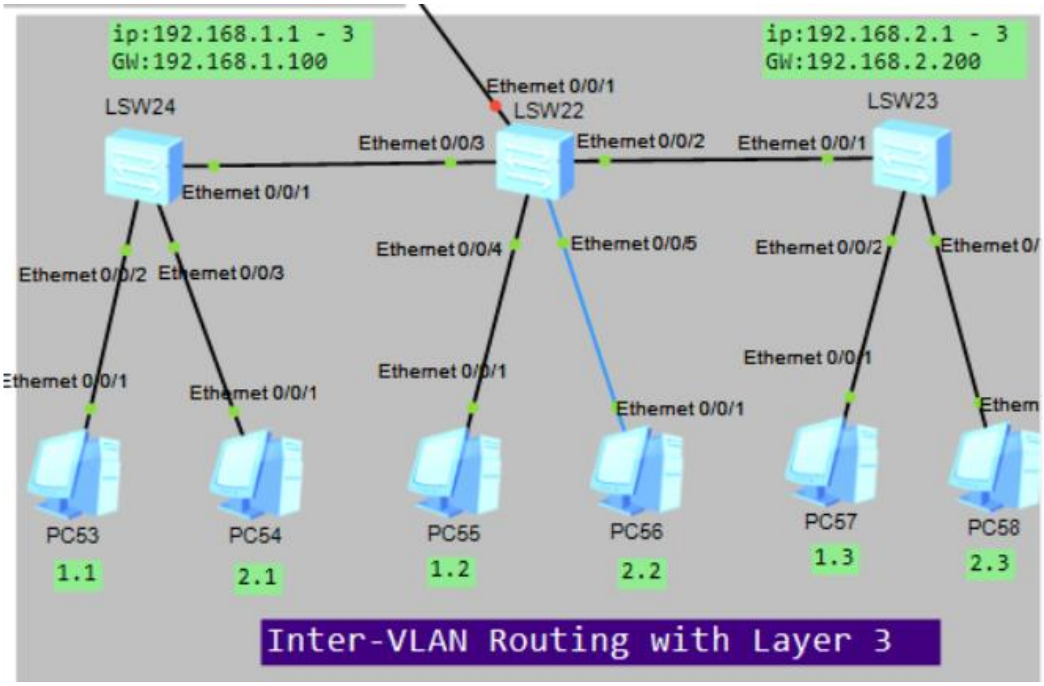
Step 4: Verify IP Assignment on PCs

On each PC connected to LSW22, open the command prompt and run:

- *ipconfig*

You should see the ***assigned IP address, subnet mask, and gateway*** *obtained from the DHCP server.*

Inter-VLAN Routing with Layer 3- Inter-Departmental Communication



Description:

In a complex and high-traffic airport network, various departments (e.g., IT Support, HR, Customer Service, Financial Services) operate on separate VLANs for security, segmentation, and performance. However, inter-departmental communication is crucial — for example, HR systems need access to the financial servers, or IT support tools must reach devices in different zones.

To enable communication between these VLANs, a Layer 3 Switch is deployed with VLANIF interfaces, acting as a virtual router inside the switch.

This method is known as Inter-VLAN Routing using Layer 3 Switches, where each VLAN is assigned a VLANIF (Layer 3 Interface) to route traffic between VLANs without needing an external router.

This setup ensures high-speed, hardware-based routing, minimizing latency and improving scalability — essential in time-sensitive environments like airports.

Justification:

- ***High-Speed Routing:***
  Layer 3 switches provide wire-speed routing between VLANs, ideal for airport operations requiring minimal delay.

- ***Reduced Device Load:***
  Unlike Router-on-a-Stick (used for Finance), the routing happens directly in the switch's ASICs, reducing CPU load and bottlenecks.
- ***Simplified Network Design:***
  Removes the need for separate routers for VLAN routing, centralizing Layer 3 logic at the distribution layer.
- ***Security and Control:***
  ACLs (Access Control Lists) and QoS policies can be applied per VLANIF to control and prioritize inter-departmental traffic.
- ***Scalability:***
  More VLANs and departments can be added without redesigning the topology or reconfiguring core routing devices.
- ***Redundancy & STP Compatibility:***
  Easily integrates with redundant Layer 2 uplinks and STP configurations used across the campus network.

Configuration Summary

Assume:

- *VLAN 10 → HR Dept → 192.168.1.0/24 → Gateway: 192.168.1.100*
- *VLAN 20 → IT Dept → 192.168.2.0/24 → Gateway: 192.168.2.200*

LSW22

- *Configured as the central routing device.*
- *Uses VLANIF interfaces to route between VLAN 10 (192.168.1.0/24) and VLAN 20 (192.168.2.0/24).*
- *Acts as the **default gateway** for all VLANs*
- *Two VLANIF interfaces (VLAN 10 and VLAN 20) are created with gateway IPs `192.168.1.100` and `192.168.2.200`.*
- *Ports connecting to access switches and PCs are set to **trunk** or **access** as needed.*

```
# Enter system view
system-view

# VLAN 10 Interface (HR Dept)
interface Vlanif 10
ip address 192.168.1.100 255.255.255.0
quit

# VLAN 20 Interface (IT Dept)
interface Vlanif 20
ip address 192.168.2.200 255.255.255.0
quit

# Configure Layer 2 Access Ports on LSW22
interface Ethernet 0/0/3
```

```
port link-type access
port default vlan 10
quit

interface Ethernet 0/0/4
port link-type access
port default vlan 20
quit
```

LSW24

- *Connects end devices in the* ***192.168.1.x*** *subnet.*
- *All access ports are assigned to VLAN 10.*
- *Uplink port to L3 switch is configured as a* ***trunk****.*

Key Configuration*:*

- *Ports to PCs: Access, VLAN 10*
- *Port to L3 Switch: Trunk, allows VLAN 10*

```
interface Ethernet 0/0/2
port link-type access
port default vlan 10
quit

interface Ethernet 0/0/3
port link-type access
port default vlan 10
quit

interface Ethernet 0/0/1
port link-type trunk
port trunk allow-pass vlan 10
quit
```

LSW23

- *Connects end devices in the* ***192.168.2.x*** *subnet.*
- *All access ports are assigned to VLAN 20.*
- *Uplink port to L3 switch is configured as a* ***trunk****.*

Key Configuration*:*

- *Ports to PCs: Access, VLAN 20*
- *Port to L3 Switch: Trunk, allows VLAN 20*

```
interface Ethernet 0/0/1
port link-type access
port default vlan 20
quit
```

```
interface Ethernet 0/0/2
port link-type access
port default vlan 20
quit

interface Ethernet 0/0/3
port link-type access
port default vlan 20
quit

interface Ethernet 0/0/0
port link-type trunk
port trunk allow-pass vlan 20
quit
```