Network Infrastructure Project Documentation

IT and HR Office Network Design and Implementation

Prepared for:

Intercity Networks

Prepared by:

Joseph Posas

Cybersecurity / Networking Program

Date:

August 17, 2025

Table of Contents

1.1 Project Overview

This project involves designing and implementing a network infrastructure for a medium-sized organization with two separate office locations: the IT Office and the HR Office. The network is built using Cisco Packet Tracer and includes routers, switches, wireless LAN controllers, access points, and end devices such as PCs and laptops. The goal is to create a reliable, scalable, and secure network that supports both wired and wireless connectivity, enabling seamless communication between offices and providing access to necessary resources.

1.2 Objectives

The main objectives of this project are:

- To design a functional network that connects the IT and HR offices effectively.
- To configure network devices including routers, switches, WLCs, and APs with proper IP addressing and VLAN segmentation.
- To ensure wired and wireless devices can communicate securely and efficiently within their respective networks.
- To document the network infrastructure clearly for future maintenance and troubleshooting.

1.3 Scope

The scope of this project includes:

- Configuration of network devices within Cisco Packet Tracer, including physical and logical setup.
- Assignment of IP addresses and subnetting for both offices.
- VLAN implementation for network segmentation and security.
- Documentation of device configurations, port statuses, and network topology.
- Verification of connectivity and network functionality for end devices.

2.1 Physical Network Layout

The physical network layout illustrates the actual placement of devices within the organization's IT and HR offices. This layout is crucial because it ensures proper connectivity between devices, minimizes cable lengths, and allows for efficient troubleshooting and maintenance. The network includes routers, switches, wireless LAN controllers, access points, and end devices, all organized in designated wiring closets and office locations. Physical diagrams will provide a clear representation of device placement and cabling.

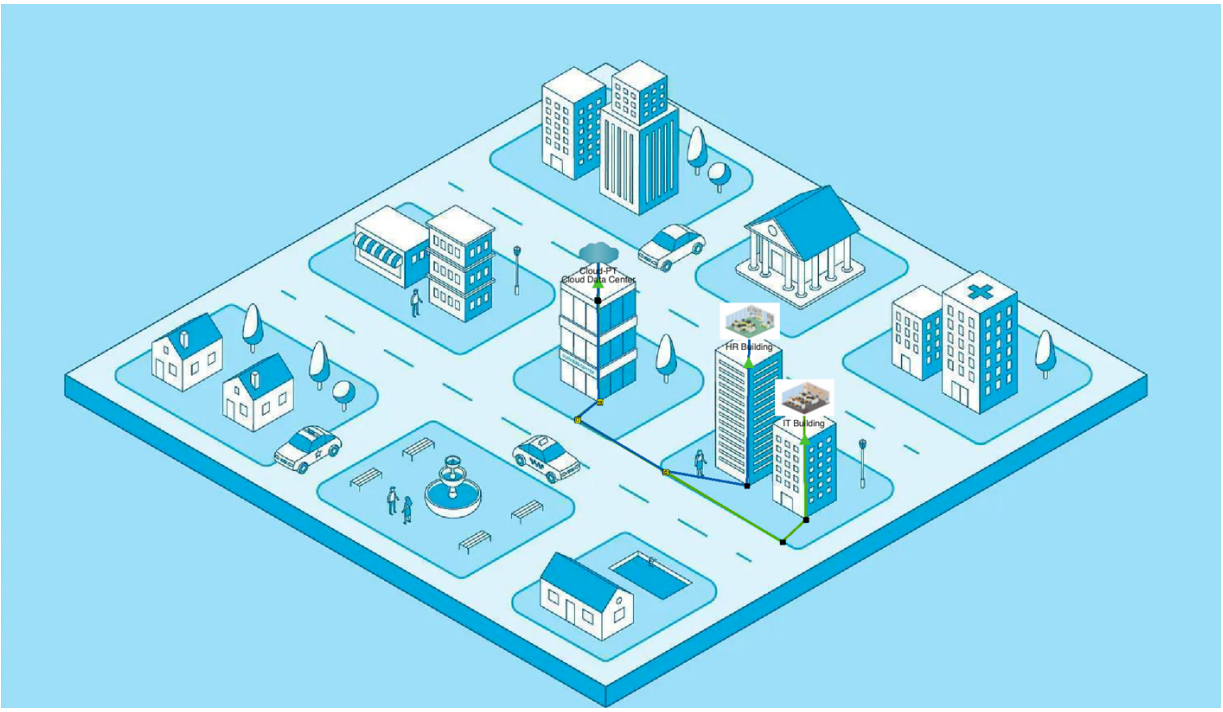

Figure 1 City-level network diagram showing the connection between IT and HR offices, including the Cloud Data Center.

Information Technology office:

Figure 2 IT office network layout showing the placement of PCs in the office.

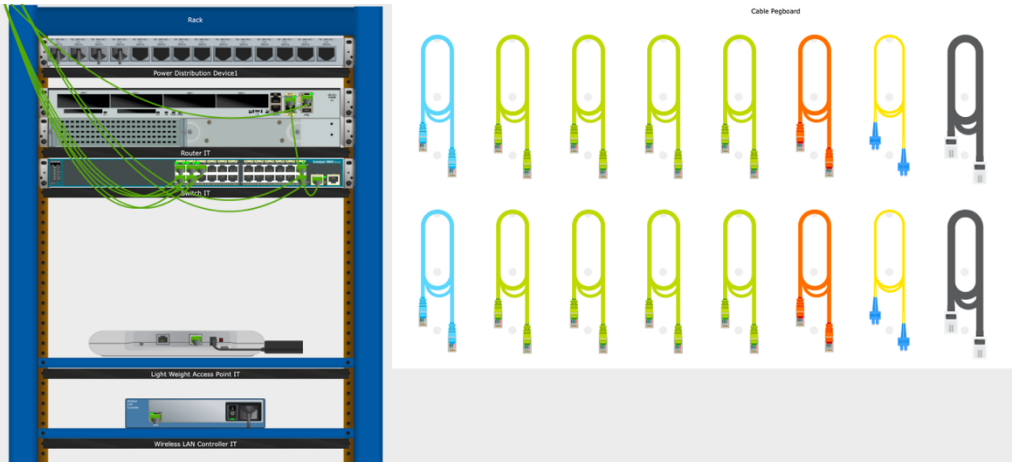

Figure 3 IT wiring closet diagram highlighting routers, switches, and APs.

Human Resources office:

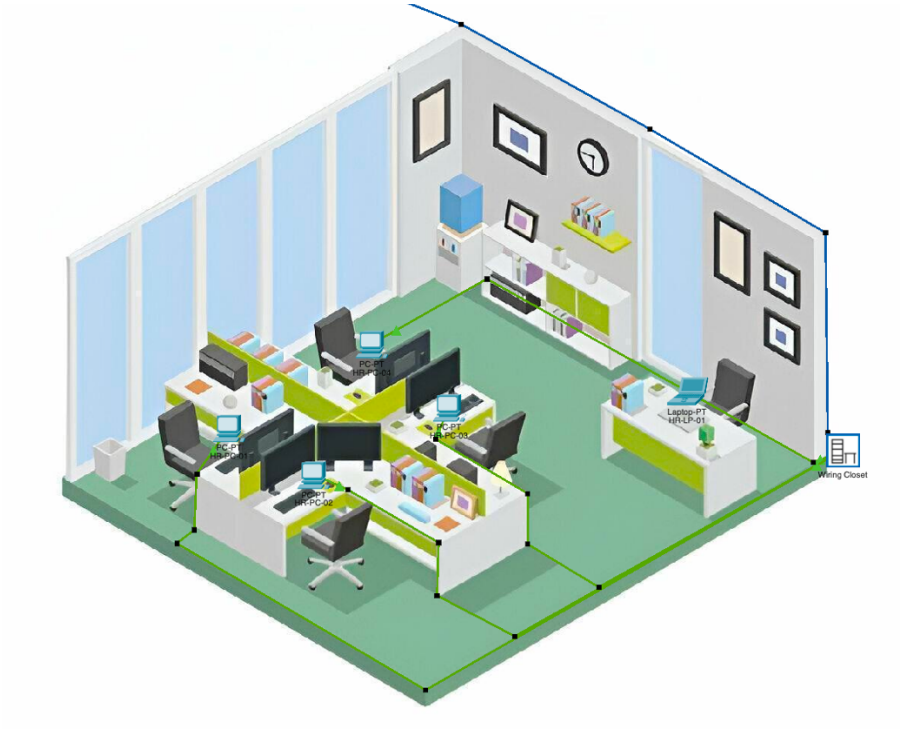

Figure 4 HR office network layout showing the placement of PCs in the office.

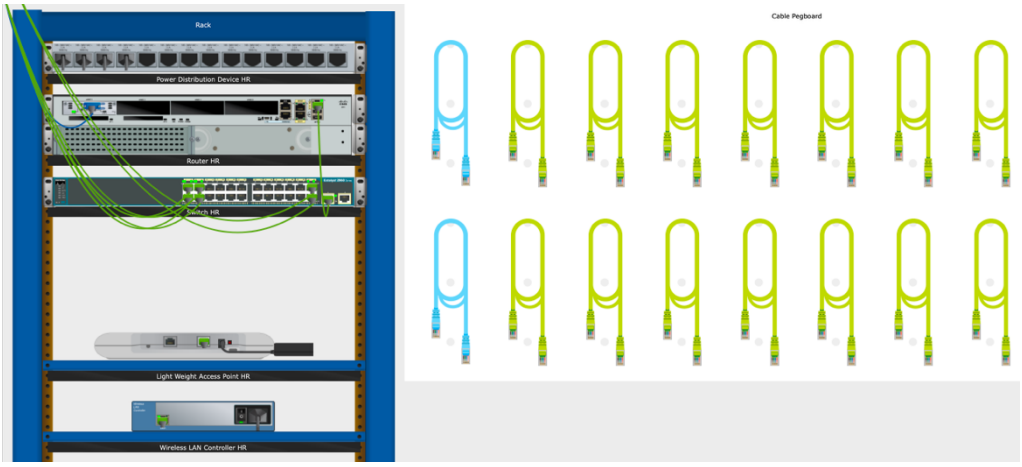

Figure 5 HR wiring closet diagram highlighting routers, switches, and APs.

2.2 Logical Network Diagram

The logical network diagram represents how data flows across the network, independent of physical placement. It highlights the interconnections between routers, switches, access points, and end devices, as well as IP addressing and VLAN segmentation. Logical diagrams are essential for understanding network functionality, planning expansions, and troubleshooting connectivity issues.

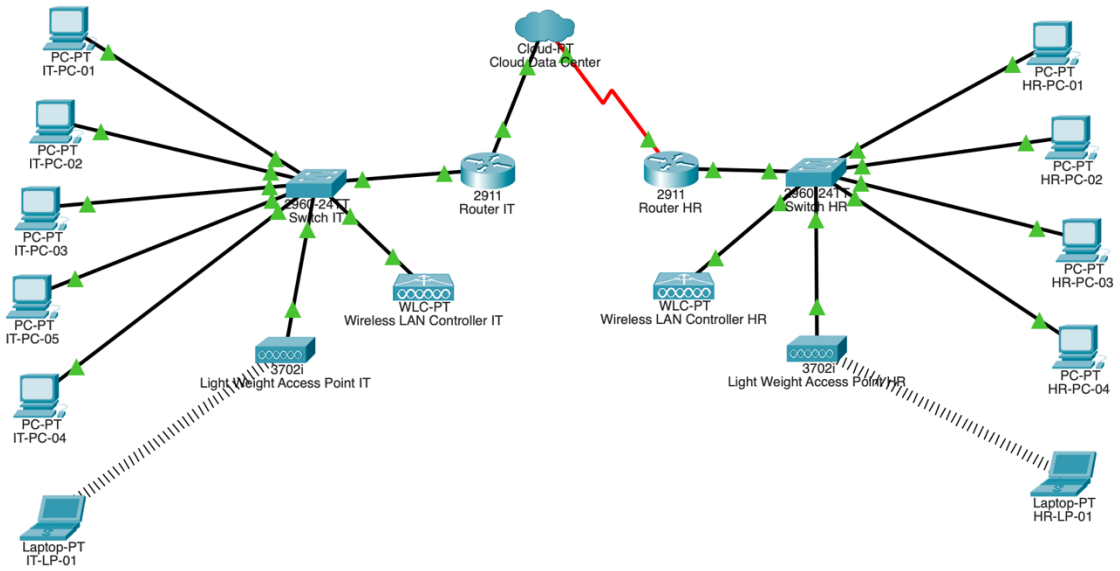

Figure 6 Logical network diagram showing device interconnections, IP addressing, and VLAN segmentation across IT and HR offices.

2.3 IP Addressing Scheme

The IP addressing scheme ensures proper communication between devices and network segments. Static and dynamic IP ranges are assigned based on device type to maintain organization and simplify management.

Device Type	IP Address Range	Example / Notes
Router	192.168.1.1	Default gateway for the network
Switch (if Layer 3)	192.168.1.2	Management IP for administrative access
WLC	192.168.1.3	Wireless LAN controller
Servers	192.168.1.10 - 192.168.1.29	File servers, DNS servers, etc.
PCs	192.168.1.50 - 192.168.1.100	Static IPs for workstations
DHCP Range	192.168.1.101 - 192.168.1.199	Dynamic IP allocation for PCs
Wireless Devices	192.168.1.200 - 192.168.1.254	Phones, laptops, and other wireless devices

2.4 VLAN Configuration

VLANs are used to logically segment the network for security and efficiency. VLAN 1 is the default VLAN for general network communication, while VLAN 2 is used for HR office switch ports to isolate HR traffic from IT traffic. VLAN implementation helps control broadcast domains, improves performance, and increases network security.

3. Cloud Data Center Infrastructure

The Cloud Data Center serves as the central hub connecting the IT and HR office networks. It provides WAN connectivity, routing, and core network services, ensuring reliable communication and data flow between offices and external networks.

3.1 Cloud Device Details

The Cloud Data Center is represented by a **Cloud-PT** device in Cisco Packet Tracer. It acts as the intercity connection point for both offices and supports multiple serial, Ethernet, and modem interfaces.

Device Name	Device Model	Physical Location

3.2 Port and Link Status

The following table summarizes the status of the Cloud Data Center's interfaces:

Port	Link Status
Serial0	Down
Serial1	Down
Serial2	Down
Serial3	Up
Modem4	Down
Modem5	Down
Ethernet6	Up
Coaxial7	Down

4. IT Office Infrastructure

The IT Office functions as the central technical hub of the organization. It houses core networking devices, including routers, switches, wireless controllers, and lightweight access points, as well as end-user PCs. The IT office is responsible for maintaining connectivity across the enterprise and managing wireless infrastructure.

4.1 IT Device Details

The IT Office contains both end-user devices and infrastructure equipment that support network management and connectivity.

Device Name	Device Type	IP Address	Role
IT-Router	Cisco 2911 Router	192.168.1.1	Default Gateway
IT-Switch	Catalyst 2960 Switch	192.168.1.2	L2/L3 Switching
IT-WLC	Wireless LAN Controller	192.168.1.3	Wireless Management
IT-AP	Lightweight Access Point	DHCP-assigned	Wireless Coverage
IT-PCs	End Devices	192.168.1.50 – 192.168.1.100	End-User Workstations

4.2 Port and Link Status

The IT Office wiring closet includes the router, switch, and WLC, with structured cabling to PCs and wireless APs. Below is a summary of major port connections:

Source Device	Source Port	Destination Device	Destination Port	Status
IT-Router	Serial0/3/0	Cloud Data Center	Serial3	Up
IT-Router	G0/0	IT-Switch	F0/1	Up
IT-Switch	F0/23	IT-WLC	G0	Up
IT-Switch	F0/24	IT-AP	G0	Up
IT-Switch	F0/2–F0/22	IT-PCs	NIC	Up

5. HR Office Infrastructure

The HR Office provides essential connectivity for Human Resources staff while remaining logically separated from the IT Office through VLAN segmentation. The HR network supports end-user PCs, printers, and wireless connectivity, with its own dedicated switch and access point, while still connecting back to the IT core.

5.1 HR Device Details

Device Name	Device Type	IP Address	Role
HR-Switch	Catalyst 2960 Switch	192.168.1.20	Local Switching
HR-AP	Lightweight Access Point	DHCP-assigned	Wireless Coverage
HR-PCs	End Devices	192.168.1.60 – 192.168.1.80	End-User Workstations
HR-Printer	Network Printer	192.168.1.81	Shared Printing Resource

5.2 Port and Link Status

The HR Office wiring closet connects the local switch to end devices and the AP, while linking back to the IT Office router for gateway and network services.

Source Device	Source Port	Destination Device	Destination Port	Status
HR-Switch	F0/1	IT-Router	G0/1	Up
HR-Switch	F0/23	HR-AP	G0	Up
HR-Switch	F0/2–F0/22	HR-PCs	NIC	Up
HR-Switch	F0/24	HR-Printer	NIC	Up

6. Network Services

The network services layer provides essential functions that support end-user connectivity, resource sharing, and centralized management. These services ensure efficient IP allocation, name resolution, and access to shared resources across both IT and HR offices.

6.1 DHCP (Dynamic Host Configuration Protocol)

A centralized DHCP service is configured on the IT router, which dynamically assigns IP addresses to wireless devices and PCs within the defined range. This reduces manual configuration errors and streamlines device onboarding.

- DHCP Range: 192.168.1.101 – 192.168.1.199
- Excluded Addresses: 192.168.1.1 – 192.168.1.100 (reserved for static devices like routers, switches, WLC, and servers)
- Default Gateway: 192.168.1.1
- DNS Server: 192.168.1.10

6.2 DNS (Domain Name System)

A dedicated server in the IT office provides DNS services for the entire organization. This enables users to resolve hostnames (e.g., fileserver.local) to IP addresses, improving ease of access and reducing dependency on raw IP memorization.

- Primary DNS Server IP: 192.168.1.10
- Role: Internal hostname resolution for servers and shared resources

6.3 File & Print Services

The File Server (192.168.1.11) supports centralized document storage for both IT and HR departments, with access controlled through permissions. The HR Office additionally has a network printer (192.168.1.81) connected via the HR switch.

- File Server: 192.168.1.11 (shared departmental folders)
- Printer (HR): 192.168.1.81 (shared via HR switch)

6.4 Wireless LAN Controller (WLC) Services

The WLC (192.168.1.3) manages all lightweight access points in the IT and HR offices, ensuring consistent SSID configuration, authentication, and security policies across the wireless network.

- SSID (Employees): Secure WPA2-Enterprise, VLAN-tagged
- SSID (Guests): Isolated network, limited access, internet-only

7. Network Security

Security is a core component of the network design, ensuring data confidentiality, integrity, and availability across IT and HR offices. Multiple layers of security are implemented, combining VLAN segmentation, access control, firewall rules, and wireless encryption to protect organizational resources from internal and external threats.

7.1 VLAN Segmentation

VLANs are configured to isolate network traffic between IT and HR departments. This segmentation prevents unauthorized access, reduces broadcast domains, and enhances overall security.

- VLAN 1: Default/Management
- VLAN 2: HR Office Devices
- VLAN 10: Wireless Clients (Employees)
- VLAN 20: Wireless Clients (Guests – Internet only)

7.2 Access Control Lists (ACLs)

ACLs are applied at the router to filter traffic between VLANs and to the cloud data center. This ensures that sensitive HR and IT traffic remains isolated while still allowing access to shared services like DNS and File Servers.

- HR VLAN (2): Restricted to HR servers and printers
- IT VLAN (1): Full access to network infrastructure and shared servers
- Guest VLAN (20): Internet access only, no internal resources

7.3 Firewall and Perimeter Security

The IT office router acts as the first layer of defense between the internal LAN and the external cloud/data center. Basic firewall configurations block unauthorized inbound traffic while allowing only necessary services (e.g., DNS, HTTP/HTTPS). This functionality is enforced

through Access Control Lists (ACLs) configured on the router, which act as a lightweight firewall by filtering permitted traffic and blocking unauthorized access attempts.

7.4 Wireless Security

Wireless access points managed by the WLC use WPA2-Enterprise with centralized authentication. Guest users are placed on a separate VLAN, ensuring no access to internal resources.

- Employee SSID: WPA2-Enterprise, VLAN 10
- Guest SSID: WPA2-Personal, VLAN 20, Internet-only

7.5 Device Hardening

All networking devices (routers, switches, WLC) are secured with:

- Strong console and SSH passwords
- Disabled unused ports
- Regular firmware updates
- Enforced management via SSH instead of Telnet

8. Network Monitoring & Management

Monitoring and management ensure the network remains reliable, secure, and high-performing. This chapter describes the tools and practices used to oversee the IT and HR office network infrastructure, detect issues early, and maintain long-term operational stability.

8.1 Monitoring Tools and Protocols

While the current implementation provides a functional and secure network for small business operations, future iterations of this project can be enhanced with monitoring and logging tools for better visibility and troubleshooting:

- **SNMP (Simple Network Management Protocol): For centralized monitoring of device health, bandwidth utilization, and performance metrics.**
- **Syslog: To centralize logging of important events such as authentication attempts, errors, and configuration changes.**
- **NetFlow: For detailed traffic flow analysis, helping identify bandwidth-heavy applications or anomalies.**
- **Packet Capture (Wireshark): For deep packet inspection and advanced troubleshooting.**
- **Configuration Backups: Automating backup procedures to quickly recover from misconfigurations or device failures.**

8.2 Device Management

- **Switches & Routers:** Managed via SSH for secure remote configuration.

- **Wireless LAN Controller (WLC):** Provides centralized management of access points, monitoring wireless client connections and usage.
- **Servers:** Monitored for uptime, CPU, memory, and storage utilization.

8.3 Fault Detection & Troubleshooting

- Automated alerts notify administrators of device failures, link issues, or unusual traffic patterns.
- Network topology maps and logical diagrams assist in quickly pinpointing problem areas.
- Common troubleshooting tools include:
    - **Ping & Traceroute:** Connectivity and path verification.
    - **Packet Capture (Wireshark):** Deep traffic inspection.
    - **Configuration Backups:** Ensures rapid recovery from misconfigurations.

8.4 Performance Optimization

As the network scales, additional performance optimization measures can be adopted to improve efficiency and ensure consistent service:

- **Bandwidth Utilization Reviews:** Regular monitoring to detect and address bottlenecks.
- **QoS (Quality of Service) Policies:** Prioritizing business-critical traffic (e.g., HR applications or VoIP) over less important traffic.
- **Wireless Optimization:** Fine-tuning wireless channels and access point placement to reduce interference and maximize coverage.

8.5 Maintenance Practices

- **Regular Updates:** Firmware and security patches applied to routers, switches, WLC, and servers.

- **Configuration Management:** Version control for network device configurations.
- **Capacity Planning:** Monitoring growth trends to prepare for future expansion.

9. Conclusion & Recommendations

This network infrastructure project successfully established a secure, reliable, and scalable network for the IT and HR offices, integrating both wired and wireless connectivity. The design incorporates proper IP addressing, VLAN segmentation, and centralized management through routers, switches, and wireless LAN controllers, ensuring efficient communication between devices and departments.

9.1 Key Achievements

- **Reliable Connectivity:** Both offices are fully connected to the cloud data center and to each other, with redundant pathways where necessary.
- **Logical & Physical Organization:** Devices are systematically placed in wiring closets, with clear cable management and labeling.
- **IP Addressing & VLANs:** Structured addressing and VLAN segmentation improve network performance, security, and manageability.
- **Centralized Wireless Management:** Wireless LAN controllers allow efficient monitoring and configuration of access points, ensuring strong coverage and optimized bandwidth.

9.2 Recommendations

- **Implement Network Monitoring Tools:** Deploy SNMP, Syslog, and NetFlow monitoring for proactive issue detection and performance analysis.
- **Regular Maintenance:** Schedule firmware updates, configuration backups, and security patching for all devices.
- **Scalability Planning:** Anticipate growth in users or devices by reserving additional IP addresses and VLANs.
- **Security Enhancements:** Consider implementing firewalls, access control lists (ACLs), and intrusion detection/prevention systems for increased protection.
- **Documentation Updates:** Maintain up-to-date network diagrams, inventory, and configuration records for operational efficiency and troubleshooting