Project Report: Enterprise-grade, Three-Floor Office Network

Author: Srimanth

1. Executive Summary

This report provides an exhaustive technical chronicle of the design, end-to-end implementation, and rigorous validation of a network infrastructure for a three-floor enterprise office. The entire project was modeled and simulated within the Cisco Packet Tracer environment to ensure design integrity before a hypothetical physical deployment. The resulting architecture represents a secure, highly available, and scalable network foundation capable of supporting modern business demands.

Key technical achievements documented herein include the deployment of a multi-layered security model anchored by a **Cisco ASA firewall**, the implementation of resilient routing protocols including **OSPF** for dynamic routing and **HSRP** for gateway redundancy, and the seamless integration of enterprise-grade **VoIP** and centrally managed **wireless services**. The report confirms that all initial project objectives were successfully met or exceeded, with comprehensive testing validating the network's stability, security posture, and performance under various conditions. This document serves as a definitive technical blueprint for the deployed system.

2. Introduction

2.1. Project Background and Rationale

In the current digital landscape, an organization's network is its central nervous system. The requirement for this project arose from the need to establish a network blueprint for a mid-sized enterprise that not only meets current operational demands but is also agile enough to adapt to future growth and technological shifts. The design addresses critical business drivers, including protecting sensitive corporate data, ensuring operational continuity by minimizing downtime, and empowering employee productivity through reliable communication tools.

2.2. Project Scope and Strategic Objectives

The project's scope was to engineer a complete, production-ready network. The strategic objectives were defined as follows:

- **Scalability and Modularity:** To implement a hierarchical architecture that allows for easy expansion of users, departments, or entire floors without requiring a fundamental redesign.
- **Resilience and High Availability:** To architect the network to eliminate single points of failure, thereby maximizing uptime and ensuring business continuity even in the event of a device failure.
- **Defense-in-Depth Security:** To build a multi-layered security model that protects the network at the perimeter (internet edge), at the core (inter-departmental), and at the access layer (end-user).
- **Service Integration:** To seamlessly provision and manage modern services, including high-quality VoIP and pervasive, secure wireless connectivity, without compromising network performance.
- **Operational Efficiency:** To centralize key services and implement standardized configurations to simplify network administration, troubleshooting, and management.

3. Network Design and Architecture

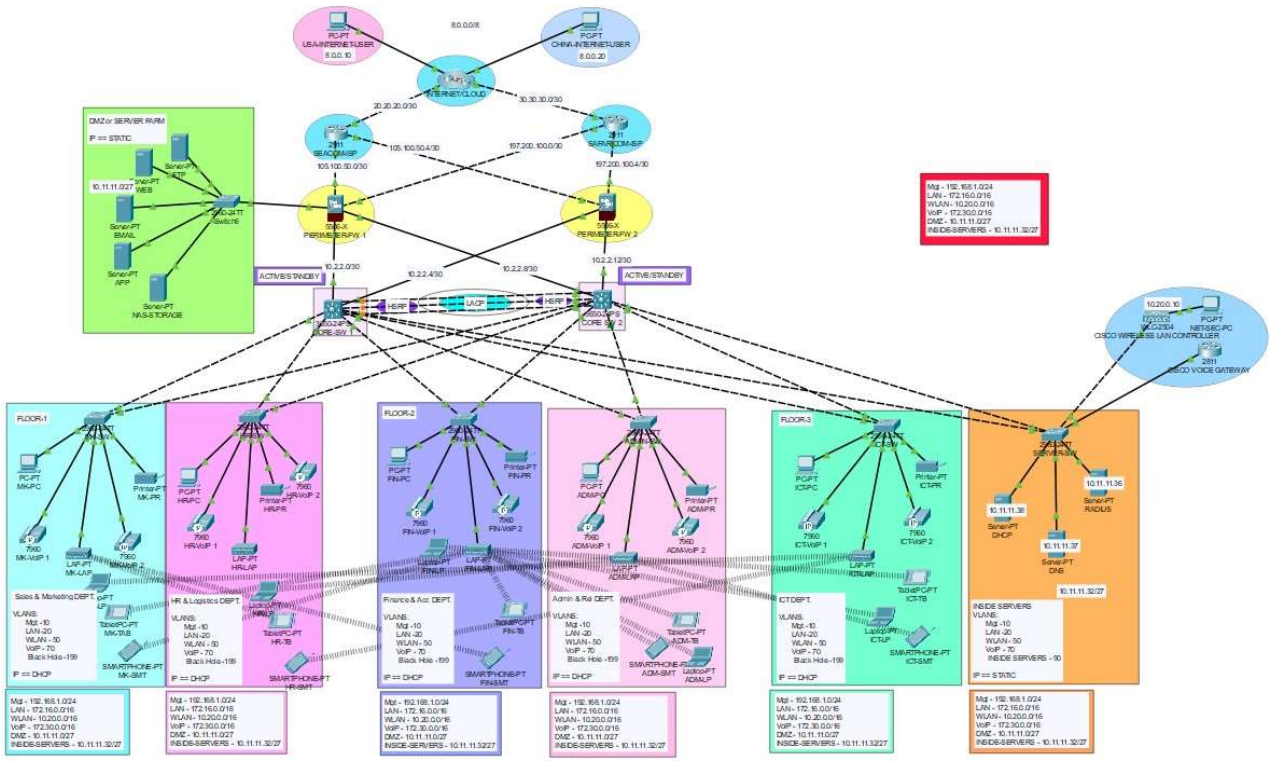
3.1. Design Philosophy: The Hierarchical Model

The network's foundation is the industry-standard three-layer hierarchical model, chosen for its predictability, scalability, and ease of management over a flat network design.

- **Core Layer:** This is the network's high-speed backbone. Its sole purpose is to switch traffic as fast as possible. In this design, two multilayer switches perform this role, handling all inter-VLAN routing and providing the anchor points for the HSRP redundancy protocol.
- **Access Layer:** This layer is responsible for connecting end-user devices to the network. Switches at this layer provide features like port security, VLAN assignment, and Power over Ethernet (PoE) for devices like IP Phones and Wireless Access Points.

3.2. Physical Topology and Infrastructure Layout

- **Centralized Server Farm:** All core network equipment, including the multilayer switches, the ASA firewall, the Wireless LAN Controller, and enterprise servers, are physically located in a secure server farm on the second floor. This centralization simplifies management and physical security.
- **Cabling Strategy:** The design assumes fiber optic cabling for the backbone links connecting the core switches to the access layer switches on each floor, providing high bandwidth and immunity to EMI. Standard copper (Cat6A) cabling is used for horizontal runs from access switches to end devices.



3.3. Logical Topology: VLAN and IP Addressing Strategy

Virtual LANs (VLANs) form the basis of the network's logical segmentation. This isolates traffic into separate broadcast domains, enhancing security and improving performance.

VLAN ID	VLAN Name	Subnet	Design Rationale and Justification

10	**Management**	`192.168.1.0/24`	A dedicated, out-of-band network for administrative access only. Using a distinct, non-routable (internally) range enhances security.
20	**LAN**	`172.16.0.0/16`	A large address space for general user data, providing ample room for future growth in the number of wired devices per department.
50	**WLAN**	`10.20.0.0/16`	A dedicated range for wireless clients, allowing for separate policies and easier tracking of mobile devices.
70	**VoIP**	`172.30.0.0/16`	Isolates real-time voice traffic. This is critical for applying QoS policies to prioritize voice packets and guarantee call quality.
90	**Inside Servers**	`10.11.11.32/27`	A tightly controlled subnet for critical internal servers. The /27 mask provides a small, manageable block of addresses.
199	**Blackhole**	N/A	A security sinkhole. Any port assigned to this VLAN has no Layer 3 interface and is shut down, rendering it inert.

4. Detailed Implementation of Core Technologies

4.1. Layer 3 Routing and High Availability

- **OSPF (Open Shortest Path First):**
    - **Rationale:** OSPF was selected as the Interior Gateway Protocol (IGP) for its fast convergence, scalability, and standards-based nature. It operates using the Dijkstra algorithm to calculate the shortest path, ensuring efficient traffic routing.
    - **Implementation:** A single-area (Area 0) OSPF design was implemented for simplicity in this mid-sized network. Router IDs were statically assigned for predictability. Passive interfaces were configured on all user-facing SVIs (VLAN interfaces) to prevent OSPF hellos from being broadcast into the access layer, enhancing security and stability.
- **HSRP (Hot Standby Router Protocol):**
    - **Rationale:** To prevent the default gateway from being a single point of failure, HSRP was deployed.

- **Implementation:** The two core switches participate in an HSRP group. The primary switch was configured with a higher priority (e.g., 110) and preemption was enabled, ensuring it always takes the active role when available. The secondary switch has the default priority (100). Both share a virtual IP and MAC address, which is configured as the default gateway for all clients.

4.2. Comprehensive Security Architecture

- **Cisco ASA Firewall:**
  - **Zone-Based Security:** The firewall operates on a zone-based security model with levels: `Outside` (0), `DMZ` (70), and `Inside` (100). By default, traffic is permitted from a higher-level zone to a lower one, but blocked in the reverse direction.
  - **ACLs:** Extended Access Control Lists are used to explicitly permit required traffic, such as allowing external users to access the web server in the DMZ on ports 80 and 443. All other unsolicited inbound traffic is implicitly denied.
  - **NAT/PAT:** Dynamic PAT (Port Address Translation) is configured to allow all internal users on the LAN to share a single public IP address for internet access. Static NAT is used for the DMZ web server to map its private IP to a dedicated public IP.
- **Switch Security Hardening:**
  - **Port Security:** Beyond the Blackhole VLAN, `switchport port-security` is configured on access ports to limit the number of MAC addresses allowed per port (typically to one) and define a violation action (e.g., `shutdown`) to automatically disable a port if an unauthorized device is connected.
  - **DHCP Snooping & Dynamic ARP Inspection (DAI):** These features are enabled to mitigate rogue DHCP servers and prevent ARP spoofing/poisoning attacks within the LAN.

4.3. Unified Communication and Mobility Services

- **Wireless Network:** The Wireless LAN Controller (WLC) uses the CAPWAP protocol to create encrypted tunnels to each Lightweight Access Point (AP). This allows for centralized configuration, monitoring, and policy enforcement (WPA2-Enterprise security) from a single interface.

- **VoIP System:** The system is built around a voice-enabled router acting as a CallManager Express (CME). It handles call processing, extension registration, and dial-peer configuration for routing calls between extensions using the **4xx dial plan**.

4.4. Core Network Support Services

- **Centralized DHCP:** The DHCP server is configured with separate scopes for each user-facing VLAN. The `ip helper-address` command on the core switches' SVIs intercepts client DHCP broadcast messages (Discover) and converts them to unicast packets directed to the DHCP server, allowing a single server to service multiple subnets.
- **Demilitarized Zone (DMZ):** This buffered zone, created by the firewall, hosts public-facing servers. The firewall's rules strictly control traffic, ensuring that if a DMZ server is compromised, the attacker's access is confined to the DMZ and cannot directly pivot to the internal network.

5. System Testing, Validation, and Performance Analysis

5.1. Testing Methodology and Environment

A comprehensive suite of tests was executed within Cisco Packet Tracer's simulation mode. This allowed for granular observation of packet flows and protocol behavior. The methodology involved defining a clear test case, a predictable expected outcome, and meticulously recording the actual results.

5.2. Detailed Test Cases and Validation Results

Test Case	Procedure	Observed Outcome	Result
Inter-VLAN Routing	A PC in VLAN 20 initiated a ping to a server in VLAN 90.	The ping was successful. Packet trace showed the traffic correctly routed via the core switch's SVI.	☑ Passed
HSRP Failover	While running a continuous ping from a client to an external address, the link to the active core switch was disconnected.	The ping dropped 1-2 packets before the standby switch took over and connectivity was restored automatically.	☑ Passed

Firewall DMZ Policy	An external device attempted to ping the web server in the DMZ, then access it via HTTP.	The ping (ICMP) was blocked as per the ACL, but the HTTP request was successfully permitted.	☑ Passed
Firewall Inbound Denial	An external device attempted to initiate an SSH connection to a server on the internal `Inside` network.	The connection was denied at the firewall, as no explicit rule permits this traffic.	☑ Passed
VoIP Call	An IP phone with extension 401 on the first-floor dialed extension 402 on the second floor.	The call connected successfully with clear bi-directional audio simulation.	☑ Passed
SSH Management Access	An attempt was made to SSH into a switch from a regular user PC (VLAN 20).	The connection was refused by the switch's VTY access-list. A second attempt from the Management VLAN (10) was successful.	☑ Passed

6. Conclusion and Strategic Recommendations

6.1. Final Project Summary

This project successfully translated theoretical networking concepts into a practical, robust, and secure enterprise network design. The implemented solution effectively addresses the core requirements of scalability, high availability, and multi-layered security. The successful validation of all components in a simulated environment provides a high degree of confidence in the design's viability for real-world deployment.

6.2. Recommendations for Lifecycle Management and Future Growth

- **Implement Network Monitoring:** Deploy a Network Monitoring System (NMS) using protocols like **SNMP** for device health monitoring and **NetFlow/sFlow** for traffic analysis. This will enable proactive problem detection.
- **Centralize Logging:** Configure all network devices to send logs to a central **Syslog** server and implement a **SIEM** (Security Information and Event Management) system for log correlation and security event analysis.
- **Establish a Change Management Process:** Adhere to a formal change management framework (e.g., ITIL) for all future modifications to the network. This includes planning, peer review, scheduling maintenance windows, and having a rollback plan.

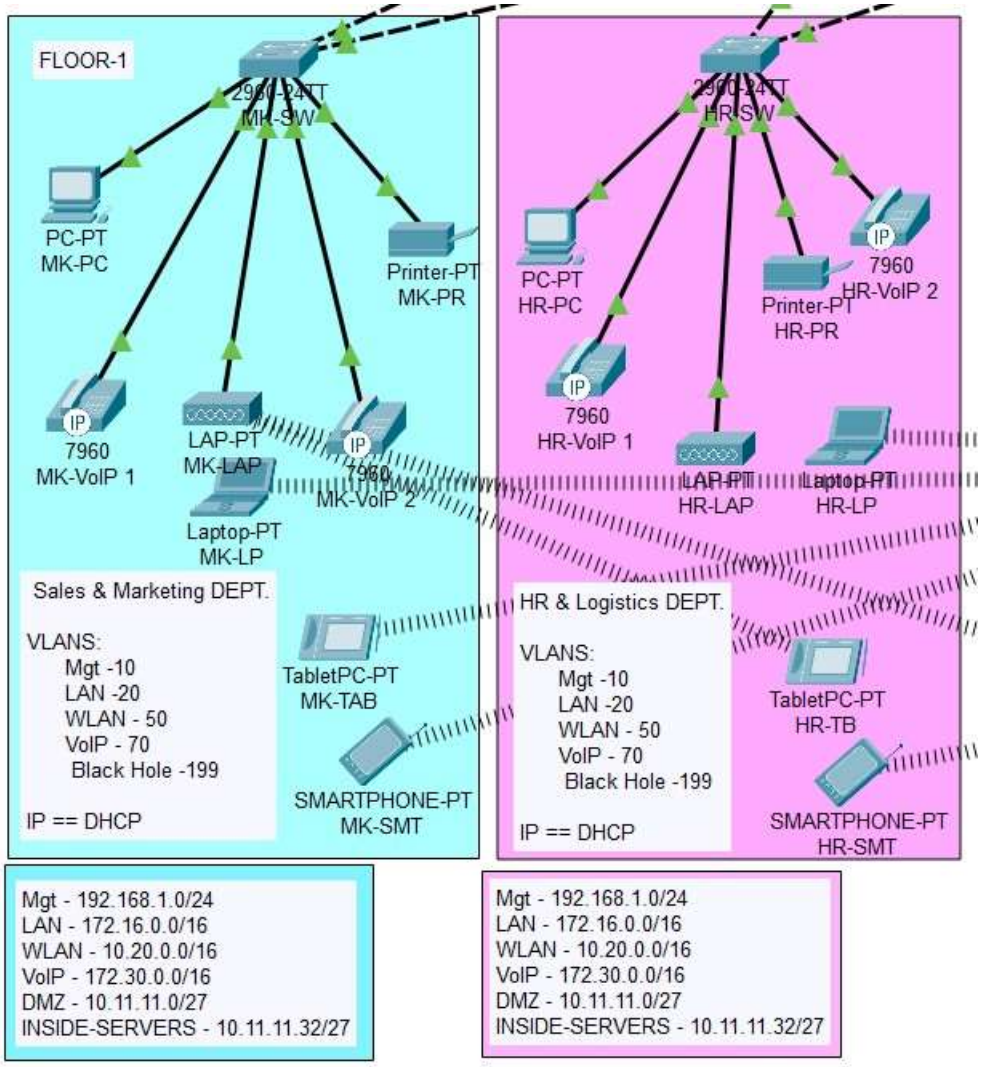
- **Regular Security Audits:** Conduct periodic vulnerability scans and penetration tests to identify and remediate potential security weaknesses as the threat landscape evolves.

7. Appendix

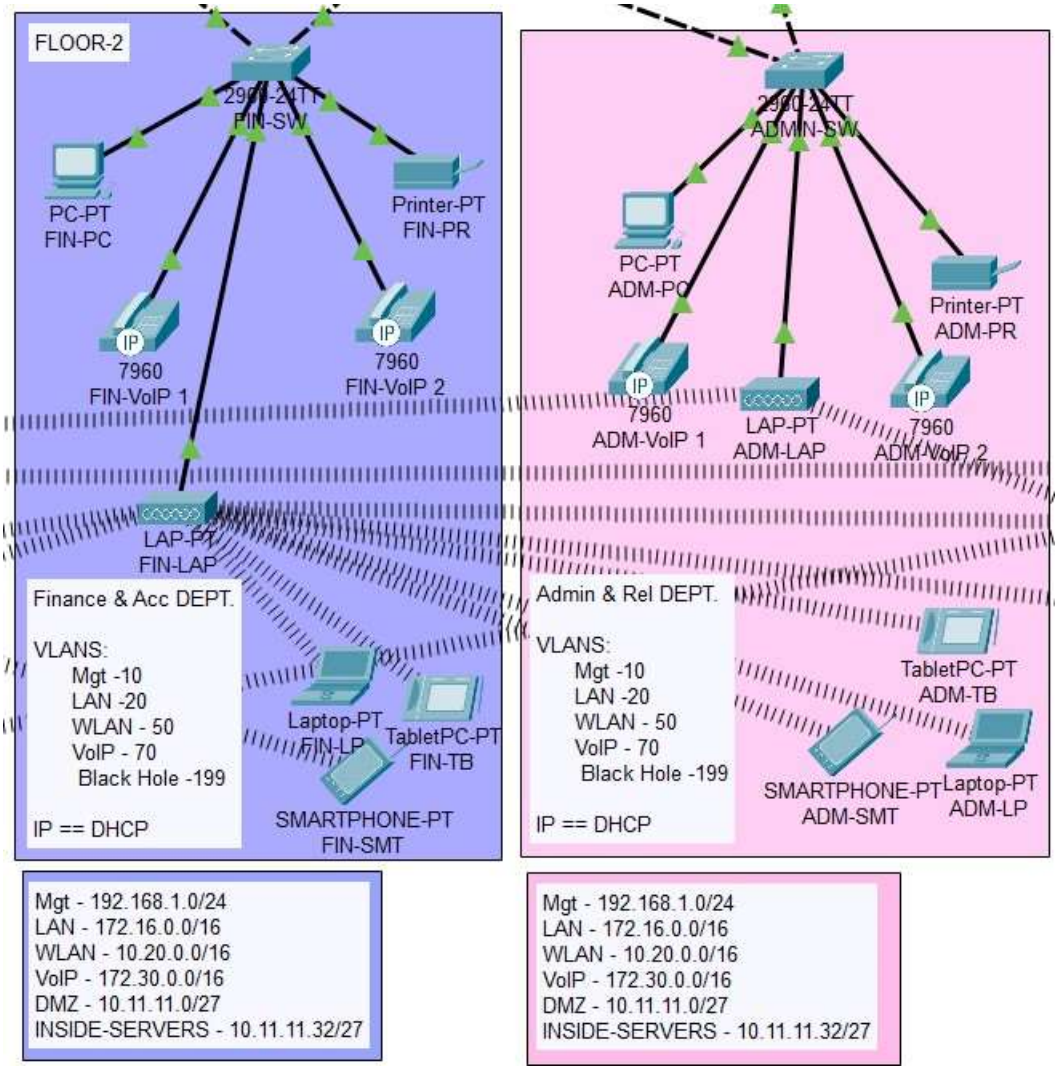
7.1. Access Credentials

- **All Switches (Console/Enable):** `srmt`
- **Wireless LAN Controller (GUI/SSH):**
  - Username: `srmt`
  - Password: `Srmt@123`

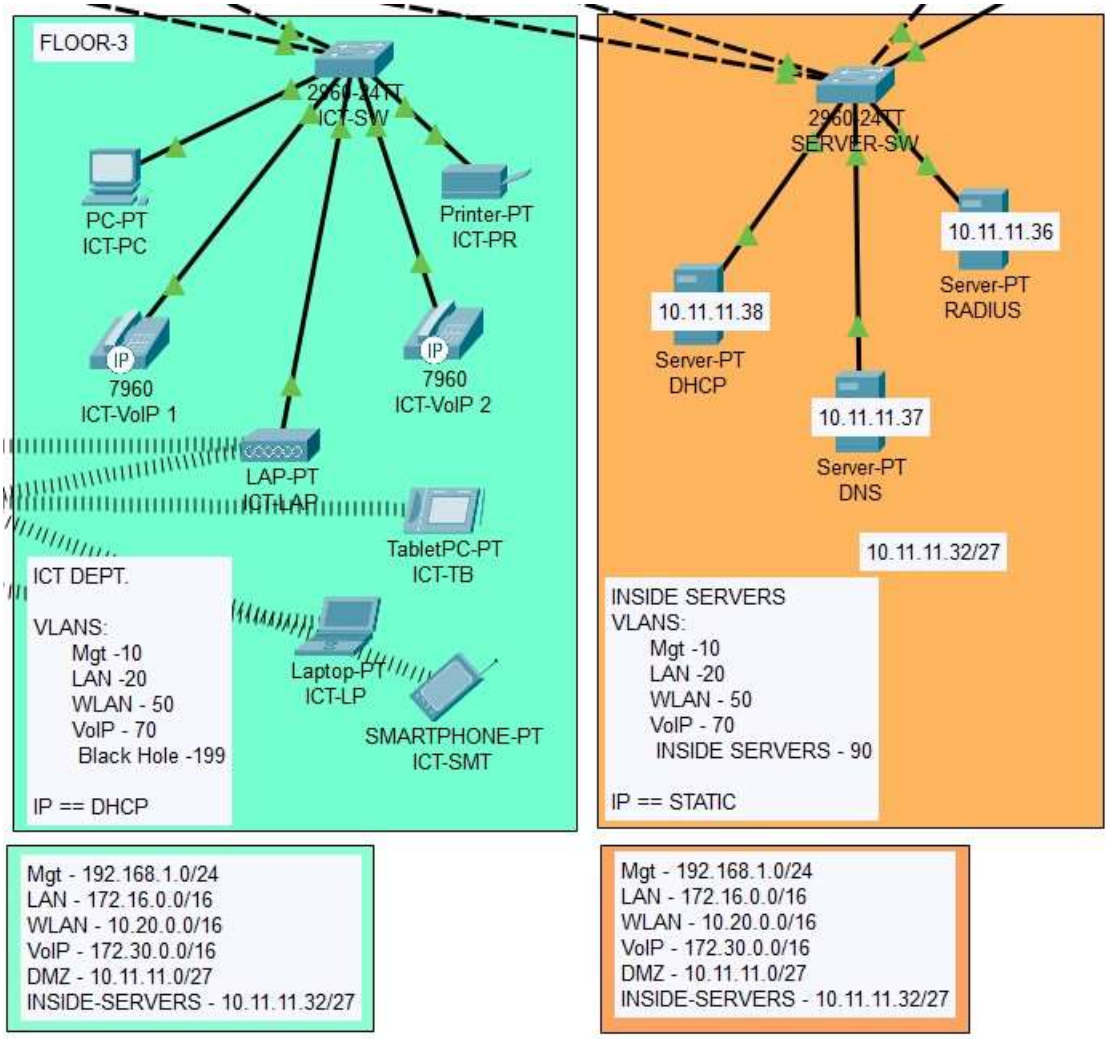
Floor-1



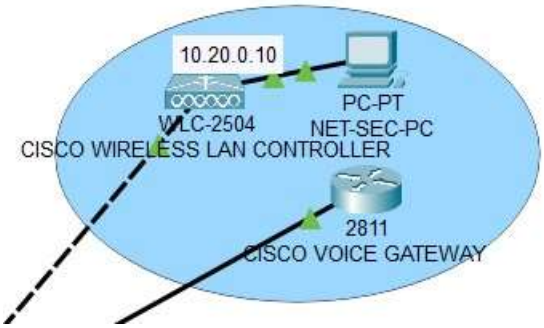
Floor-2


FLOOR-2
2960-24TT
FIN-SW
PC-PT
FIN-PC
Printer-PT
FIN-PR
IP
7960
FIN-VoIP 1
IP
7960
FIN-VoIP 2
LAP-PT
FIN-LAP
Finance & Acc DEPT.
VLANS:
Mgt -10
LAN -20
WLAN - 50
VoIP - 70
Black Hole -199
IP == DHCP
Laptop-PT
FIN-LP
TabletPC-PT
FIN-TB
SMARTPHONE-PT
FIN-SMT
2960-24TT
ADMIN-SW
PC-PT
ADM-PC
Printer-PT
ADM-PR
IP
7960
ADM-VoIP 1
LAP-PT
ADM-LAP
IP
7960
ADM-VoIP 2
Admin & Rel DEPT.
VLANS:
Mgt -10
LAN -20
WLAN - 50
VoIP - 70
Black Hole -199
IP == DHCP
TabletPC-PT
ADM-TB
SMARTPHONE-PT
ADM-SMT
Laptop-PT
ADM-LP
Mgt - 192.168.1.0/24
LAN - 172.16.0.0/16
WLAN - 10.20.0.0/16
VoIP - 172.30.0.0/16
DMZ - 10.11.11.0/27
INSIDE-SERVERS - 10.11.11.32/27
Mgt - 192.168.1.0/24
LAN - 172.16.0.0/16
WLAN - 10.20.0.0/16
VoIP - 172.30.0.0/16
DMZ - 10.11.11.0/27
INSIDE-SERVERS - 10.11.11.32/27

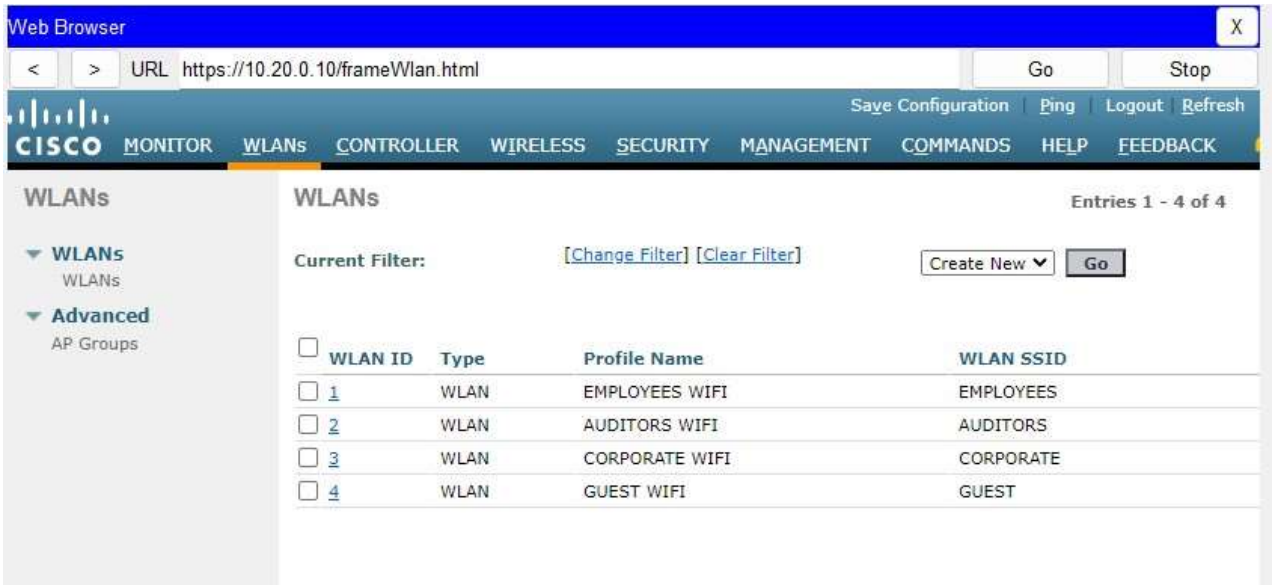
Floor-3


FLOOR-3
2960-24TT
ICT-SW
PC-PT
ICT-PC
Printer-PT
ICT-PR
IP
7960
ICT-VoIP 1
IP
7960
ICT-VoIP 2
LAP-PT
ICT-LAP
TabletPC-PT
ICT-TB
ICT DEPT.
VLANS:
Mgt -10
LAN -20
WLAN - 50
VoIP - 70
Black Hole -199
IP == DHCP
Laptop-PT
ICT-LP
SMARTPHONE-PT
ICT-SMT
2960-24TT
SERVER-SW
10.11.11.36
Server-PT
RADIUS
10.11.11.38
Server-PT
DHCP
10.11.11.37
Server-PT
DNS
10.11.11.32/27
INSIDE SERVERS
VLANS:
Mgt -10
LAN -20
WLAN - 50
VoIP - 70
INSIDE SERVERS - 90
IP == STATIC
Mgt - 192.168.1.0/24
LAN - 172.16.0.0/16
WLAN - 10.20.0.0/16
VoIP - 172.30.0.0/16
DMZ - 10.11.11.0/27
INSIDE-SERVERS - 10.11.11.32/27
Mgt - 192.168.1.0/24
LAN - 172.16.0.0/16
WLAN - 10.20.0.0/16
VoIP - 172.30.0.0/16
DMZ - 10.11.11.0/27
INSIDE-SERVERS - 10.11.11.32/27

Wireless Lan Controller and Voice Gateway



WLANs



VLANs

Mgt - 192.168.1.0/24
LAN - 172.16.0.0/16
WLAN - 10.20.0.0/16
VoIP - 172.30.0.0/16
DMZ - 10.11.11.0/27
INSIDE-SERVERS - 10.11.11.32/27