

# Secure Company Network Design

(Cisco Packet Tracer)



GitHub Repository : [Click Here](#)

## Table of Contents

INTRODUCTION .....	3
TECHNICAL REQUIREMENTS .....	3
NETWORK TOPOLOGY .....	4
IP ADDRESSING SCHEME .....	5
DEVICE CONFIGURATION .....	6
ROUTING PROTOCOLS .....	6
SECURITY IMPLEMENTATIONS .....	7
TESTING AND VERIFICATION .....	9
WIRELESS LAN .....	9
WLAN - CONNECTIVITY TEST (STAFF MOBILE) .....	10
PING AND TRACERT TESTING .....	11
DHCP .....	11
OSPF .....	12

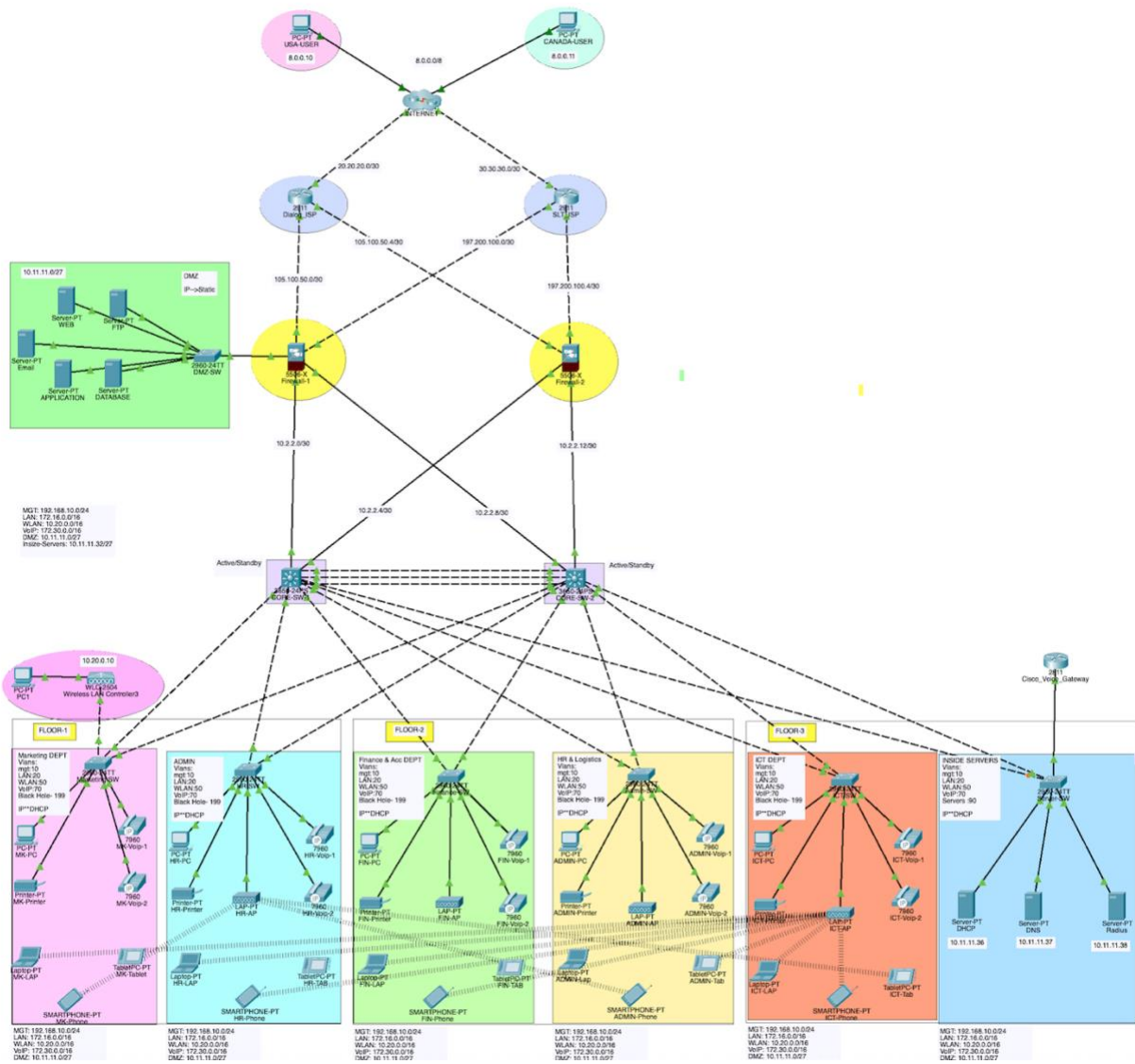
# Introduction

This document describes the design and implementation of a Secure Company Network using Cisco Packet Tracer, following a hierarchical network design with redundant, scalable, and secure infrastructure. The project meets the technical requirements outlined for supporting multiple departments, VLAN segmentation, inter-VLAN routing, wireless connectivity, and security controls.

## Technical Requirements

- Hierarchical Design – Core Layer , Distribution Layer and Access Layer
- ISP Connection – Dual ISP links
- WLC – Wireless Lan Controller used to manage and distribute WLANS
- VLAN & inter VLAN Routing- For Each Building
- EtherChannel – Between 2 L3 Switches
- VoIP – Connectivity between departments
- STP & BPDU Guard – Spanning tree Features
- Subnetting – Necessary IP address implementation
- Basic Settings – Security Implementations(Passwords) , Port Security and ACL
- IP Assignment and Sec - DHCP & DHCP Snooping
- Routing - OSPF

# Network Topology



# IP Addressing Scheme

## For Vlans

Vlan Name	Network & Subnet	Broadcast	Default Gateway	Host range
Management	192.168.10.0/24	192.168.10.255	192.168.10.1	192.168.10.1 192.168.10.254
Wireless-LAN	10.20.0.0/16	10.20.255.254	10.20.0.1	10.20.0.1 10.20.255.254
LAN	172.16.0.0/16	172.16.255.255	172.16.0.1	172.16.0.1 172.16.255.254
VoIP	172.30.0.0/16	172.30.255.255	172.30.0.1	172.30.0.1 172.30.255.254
Demilitarized Zone	10.11.11.0/27	10.11.11.31	10.11.11.1	10.11.11.1 10.11.11.30
LAN Servers	10.11.11.32/27	10.11.11.63	10.11.11.33	10.11.11.11.33 10.11.11.62

## For Routers,Firewalls,Multilayer Switch

Interfaces	Network Address & Subnet
Cloud	8.0.0.0/8
ISP1 - Internet	20.20.20.0/30
ISP2 - Internet	30.30.30.0/30
ISP1 - FWL1	105.100.50.0/30

# Device Configuration

All Config Files are available in my GitHub page -:

## Routing Protocols

- Configured OSPF for internal dynamic routing
- Summarized routes where applicable
- Neighbor relationships confirmed

```
CS-1#show ip os
CS-1#show ip ospf ne
CS-1#show ip ospf neighbor
```

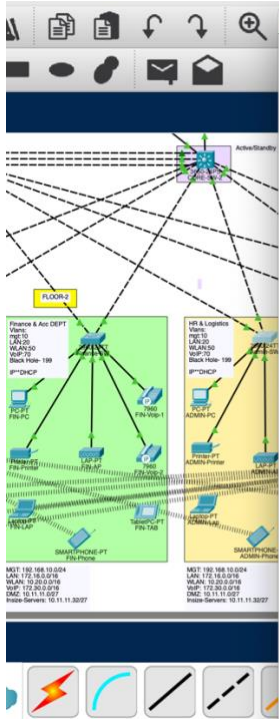
Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.2.2	1	FULL/DR	00:00:39	192.168.10.2	Vlan10
1.1.2.2	1	FULL/DR	00:00:39	172.16.0.2	Vlan20
1.1.2.2	1	FULL/DR	00:00:39	10.20.0.3	Vlan50
1.1.2.2	1	FULL/DR	00:00:39	10.11.11.35	Vlan90
1.1.8.8	1	FULL/DR	00:00:39	10.2.2.2	GigabitEthernet1/0/1

CS-1#

---

# Security Implementations

- Enable Secret
- Console Login
- Password-Encryption
- DHCP Snooping
- Port-Security
- BPDU Guard
- SSH Based Switch Management
- Cisco ASA Firewall Configurations
- Access Control Lists



Admin-SW

Physical Config **CLI** Attributes

IOS Command Line Interface

Password:  
Password:

**DHCP-Snooping**

```

ADMIN>en
ADMIN#show ip dhcp
ADMIN#show ip dhcp sn
ADMIN#show ip dhcp snooping
Switch DHCP snooping is disabled
DHCP snooping is configured on following VLANs:
none
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled

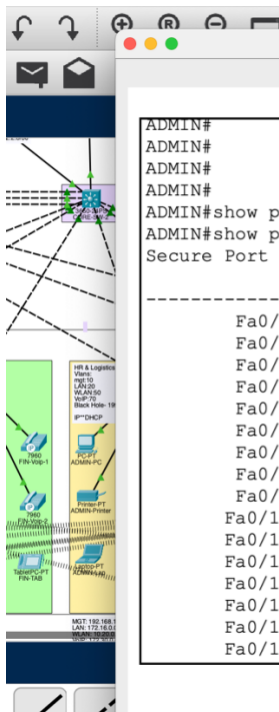
```

Interface	Trusted	Rate limit (pps)
FastEthernet0/1	yes	unlimited
FastEthernet0/2	yes	unlimited
FastEthernet0/3	yes	unlimited
FastEthernet0/4	yes	unlimited
FastEthernet0/5	yes	unlimited
FastEthernet0/6	no	4
FastEthernet0/7	no	4

ADMIN#

Copy Paste

Top



Admin-SW

Physical Config **CLI** Attributes

IOS Command Line Interface

ADMIN#

ADMIN#

ADMIN#

**Port-Security**

```

ADMIN#show po
ADMIN#show port-security

```

Secure	Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
	Fa0/1	1	0	0	Shutdown
	Fa0/2	1	0	0	Shutdown
	Fa0/3	1	0	0	Shutdown
	Fa0/4	1	0	0	Shutdown
	Fa0/5	1	1	0	Shutdown
	Fa0/6	1	0	0	Shutdown
	Fa0/7	1	0	0	Shutdown
	Fa0/8	1	0	0	Shutdown
	Fa0/9	1	0	0	Shutdown
	Fa0/10	1	0	0	Shutdown
	Fa0/11	1	0	0	Shutdown
	Fa0/12	1	0	0	Shutdown
	Fa0/13	1	0	0	Shutdown
	Fa0/14	1	0	0	Shutdown
	Fa0/15	1	0	0	Shutdown
	Fa0/16	1	0	0	Shutdown

C



# Testing and Verification

## Wireless LAN

Web Browser

URL: <https://10.20.0.10/frameWireless.html> Go Stop

**CISCO** MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home

**Wireless**

- Access Points
  - All APs
  - Radios
    - 802.11a/n/ac
    - 802.11b/g/n
    - Dual-Band Radios
    - Global Configuration
- Advanced
  - Mesh
- ATF
  - RF Profiles
  - FlexConnect Groups
  - FlexConnect ACLs
  - FlexConnect VLAN
  - Templates

**All APs** Entries 1 - 4 of 4

Current Filter [Change Filter] [Clear Filter]

Number of APs 4

AP Name	IP Address(Ipv4/Ipv6)	AP Model
<a href="#">HR-AP</a>	10.20.0.11	PT-AIR-CAP1000I-A-K9
<a href="#">FIN-AP</a>	10.20.0.14	PT-AIR-CAP1000I-A-K9
<a href="#">ADMIN-AP</a>	10.20.0.12	PT-AIR-CAP1000I-A-K9
<a href="#">ICT-AP</a>	10.20.0.13	PT-AIR-CAP1000I-A-K9

Web Browser

URL: <https://10.20.0.10/frameMonitor.html>

**CISCO** MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

**Monitor**

- Summary
- Access Points
- Cisco CleanAir
- Statistics
- CDP
- Rogues
- Clients
  - Sleeping Clients
  - Multicast
- Applications
- Local Profiling

**Access Point Summary**

	Total	Up	Down	
802.11a/n/ac Radios	4	4	0	<a href="#">Detail</a>
802.11b/g/n Radios	4	4	0	<a href="#">Detail</a>
Dual-Band Radios	0	0	0	<a href="#">Detail</a>
All APs	4	4	0	<a href="#">Detail</a>

**Client Summary**

Current Clients	11	<a href="#">Detail</a>
Excluded Clients	0	<a href="#">Detail</a>
Disabled Clients	0	<a href="#">Detail</a>

FIN-Phone

PhysicalConfigDesktopProgrammingAttributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

Wireless0

3G/4G Cell1

Bluetooth

Wireless0

Port StatusOn

Bandwidth300 Mbps

MAC Address00D0.BC54.D441

SSIDSTAFF

Authentication

DisabledWEPWPA802.1X

WPA2-PSKWPA2Method:

WEP Key

PSK Pass Phrasewifi2025

User ID

Password

MD5

User Name

Password

Encryption TypeAES

IP Configuration

DHCPStatic

IPv4 Address10.20.0.20

Subnet Mask255.255.0.0

IPv6 Configuration

AutomaticStatic

IPv6 Address

Link Local AddressFE80::2D0:BCFF:FE54:D441

## Ping and Tracert Testing

The screenshot displays a Cisco Packet Tracer network simulation. On the left, a network diagram shows a central core network connected to multiple edge networks. A red box highlights a specific network segment. On the right, a command prompt window titled "ADMIN-PC" shows the output of a traceroute command:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>tracert 8.0.0.10

Tracing route to 8.0.0.10 over a maximum of 30 hops:

  1  0 ms  0 ms  0 ms    172.16.0.3
  2  0 ms  *      0 ms    10.2.2.2
  3  0 ms  0 ms  0 ms    197.200.100.5
  4  0 ms  0 ms  0 ms    30.30.30.2
  5  0 ms  0 ms  0 ms    8.0.0.10

Trace complete.

C:\>
```

A red text overlay on the network diagram reads: "Successful ping from AdminPc(LAN) to WAN Network".

## DHCP

The screenshot displays the DHCP configuration interface in Cisco Packet Tracer. On the left, the "IP Configuration" window for an "ADMIN-PC" shows the DHCP settings:

- IP Configuration: DHCP (selected), Static
- IPv4 Address: 172.16.0.14
- Subnet Mask: 255.255.0.0
- Default Gateway: 172.16.0.1
- DNS Server: 10.11.11.37
- IPv6 Configuration: Automatic (selected), Static
- IPv6 Address: /
- Link Local Address: FE80::260:70FF:FE59:43E3
- Default Gateway: /
- DNS Server: /
- 802.1X: Use 802.1X Security (unchecked)
- Authentication: MD5

On the right, the "DHCP" configuration window for a "FastEthernet0" interface shows the DHCP service settings:

- Interface: FastEthernet0
- Service: On (selected), Off
- Pool Name: serverPool
- Default Gateway: 0.0.0.0
- DNS Server: 0.0.0.0
- Start IP Address: 0 0 0 0
- Subnet Mask: 0 0 0 0
- Maximum Number of Users: 0
- TFTP Server: 0.0.0.0
- WLC Address: 0.0.0.0

Below the configuration fields, a table lists the DHCP pools:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
WLAN	10.20.0.1	10.11.1...	10.20.0...	255.25...	1...	0.0.0.0	10.20.0...
LAN	172.16...	10.11.1...	172.16...	255.25...	1...	0.0.0.0	0.0.0.0
MGT	192.16...	10.11.1...	192.16...	255.25...	200	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0

# OSPF

Cisco Packet Tracer - /Users/yashanmaduwantha/Desktop/Company\_Project.pkt

**CORE-SW-1**

Physical Config **CLI** Attributes

IOS Command Line Interface

Routing Protocol is "ospf 35"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 1.1.1.1

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

- 10.2.2.0 0.0.0.3 area 0
- 10.2.2.4 0.0.0.3 area 0
- 192.168.10.0 0.0.0.255 area 0
- 172.16.0.0 0.0.255.255 area 0
- 10.20.0.0 0.0.255.255 area 0
- 10.11.11.32 0.0.0.31 area 0

Routing Information Sources:

Gateway	Distance	Last Update
1.1.1.1	110	00:11:48
1.1.2.2	110	00:11:41
1.1.3.3	110	00:11:41
1.1.4.4	110	00:11:46
1.1.5.5	110	00:11:47
1.1.8.8	110	00:11:49
1.1.9.9	110	00:11:44

Distance: (default is 110)

Copy Paste

✓ Top

**CORE-SW-2**

Physical Config **CLI** Attributes

IOS Command Line Interface

Routing Protocol is "ospf 35"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 1.1.2.2

Number of areas in this router is 1. 1 normal 0 stub 0 ns

Maximum path: 4

Routing for Networks:

- 10.2.2.8 0.0.0.3 area 0
- 10.2.2.12 0.0.0.3 area 0
- 192.168.10.0 0.0.0.255 area 0
- 172.16.0.0 0.0.255.255 area 0
- 10.20.0.0 0.0.255.255 area 0
- 10.11.11.32 0.0.0.31 area 0

Routing Information Sources:

Gateway	Distance	Last Update
1.1.1.1	110	00:12:06
1.1.2.2	110	00:11:58
1.1.3.3	110	00:11:59
1.1.4.4	110	00:12:03
1.1.5.5	110	00:12:05
1.1.8.8	110	00:12:06
1.1.9.9	110	00:12:02

Distance: (default is 110)

CS-2#

Copy Pas

Top