**Contents**

[1. Network Overview 1](#_Toc177251750)

[2. Network Topology 1](#_Toc177251751)

[3. IP Addressing Scheme 1](#_Toc177251752)

[4. Routing and Switching Technologies: 2](#_Toc177251753)

[5. Layer 2 Technologies 2](#_Toc177251754)

[7. IP Services: 3](#_Toc177251755)

[8. Voice and Video Technologies 3](#_Toc177251756)

[9. IoT Integration 3](#_Toc177251757)

[10. High Availability and Redundancy 4](#_Toc177251758)

[11. Conclusion 4](#_Toc177251759)

[Figure 1 Headquarter's DHCP server 5](#_Toc177253979)

[Figure 2 Branch's DHCP server 5](#_Toc177253980)

# 1. Network Overview

This document provides a comprehensive view of the network infrastructure for a large-scale enterprise designed using Cisco Packet Tracer. The network follows a three-tier architecture comprising the Core, Distribution, and Access layers to ensure a modular and scalable infrastructure. The network is designed to support various services such as VoIP, IoT, and data communication using technologies like OSPF, EIGRP, RIP, Static Routing, EtherChannel, ACLs, NAT, and more.

# 2. Network Topology

The topology of the network consists of multiple sites connected via a redundant core and distribution layers. These sites represent various enterprise branches or departments. The network includes:

* Core Layer: Fast switching and routing to ensure efficient data transmission between the distribution layers.
* Distribution Layer: Traffic filtering, VLAN segmentation, inter-VLAN routing, and policy enforcement.
* Access Layer: Connection to end devices like desktops, laptops, VoIP phones, and IoT devices.

The network is divided into different zones for functional departments and services, each assigned its own VLANs and security policies.

# 3. IP Addressing Scheme

An organized IP addressing scheme has been employed using both public and private IPs for efficient network management. The IP ranges are broken down as follows:

* Core Layer:
  + - 192.168.0.0/16
    - 23.23.23.0/30
    - 24.24.24.0/30
    - 27.27.27.0/30
    - 28.28.28.0/30
    - 29.29.29.0/30
    - 30.30.30.0/30
* Distribution Layer:
  + - 192.168.0.0/16
    - 33.33.33.0/30
    - 34.34.34.0/30
    - 35.35.35.0/30
    - 36.36.36.0/30
    - 37.37.37.0/30
    - 38.38.38.0/30
    - 39.39.39.0/30
    - 40.40.40.0/30
    - 41.41.41.0/30
    - 42.42.42.0/30
* Access Layer (end-user devices):
  + - 172.16.0.0/16
    - 192.168.0.0/16

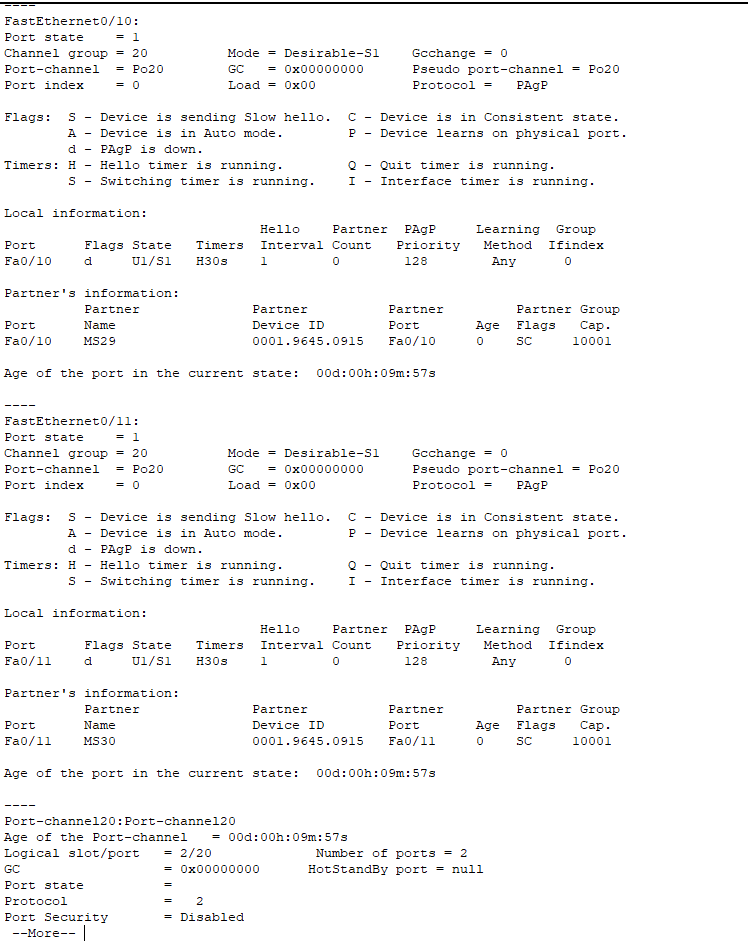
Each VLAN has its own subnet, facilitating traffic segregation and ease of IP management through DHCP.

# 4. Routing and Switching Technologies:

* OSPF: OSPF (Open Shortest Path First) is deployed in the Core Layer and inter-site links to provide fast convergence and efficient route updates. The core routers use Area 0 to interconnect with different branches.
* EIGRP: EIGRP (Enhanced Interior Gateway Routing Protocol) is implemented in the Distribution Layer between select branches for fast convergence and flexible metric-based routing.
* Static Routing: Static routes are used for connecting smaller subnets to the core layer, providing manual control for specific traffic flows. These are mainly implemented for internal services like DHCP and DNS servers.
* RIP: RIP (Routing Information Protocol) is used for legacy systems and older routers. This ensures backward compatibility and connects legacy devices while isolating them from modern systems.

# 5. Layer 2 Technologies

* VLAN Configuration: VLANs are deployed throughout the network for the HQ and its branch to segment traffic for various departments and services. For example:
* VLAN 10, 20, 100, 105: Sales & Marketing Departments
* VLAN 30, 40, 110, 115: HR Department
* VLAN 50, 60, 120, 125: IT Department & Security
* VLAN 70, 80, 130, 135: Servers
* VLAN 90, 5, 140, 145: Accounting & Finance Departments
* Spanning Tree Protocol (STP): STP is implemented to prevent Layer 2 loops in the network. It provides redundancy by enabling multiple links between switches while blocking loops to avoid broadcast storms.
* EtherChannel: EtherChannel is configured between switches to increase bandwidth and provide redundancy by aggregating multiple physical links into a single logical link.



# 6. Security Configuration

* Access Control Lists (ACLs): ACLs are applied to control access between different VLANs and zones. For example:
* Only authorized users from the IT VLAN can access the network management systems.
* Traffic between the IoT VLAN and other VLANs is restricted for security purposes.
* Network Address Translation (NAT): NAT is implemented to allow private IP addresses to access the internet. This helps in conserving public IP addresses and maintaining security by hiding internal IPs from external users.

# 7. IP Services:

* DHCP (Dynamic Host Configuration Protocol): DHCP is used to assign IP addresses dynamically to end devices in the access layer. Each VLAN is assigned its own DHCP scope to ensure proper IP address management and avoid IP conflicts.

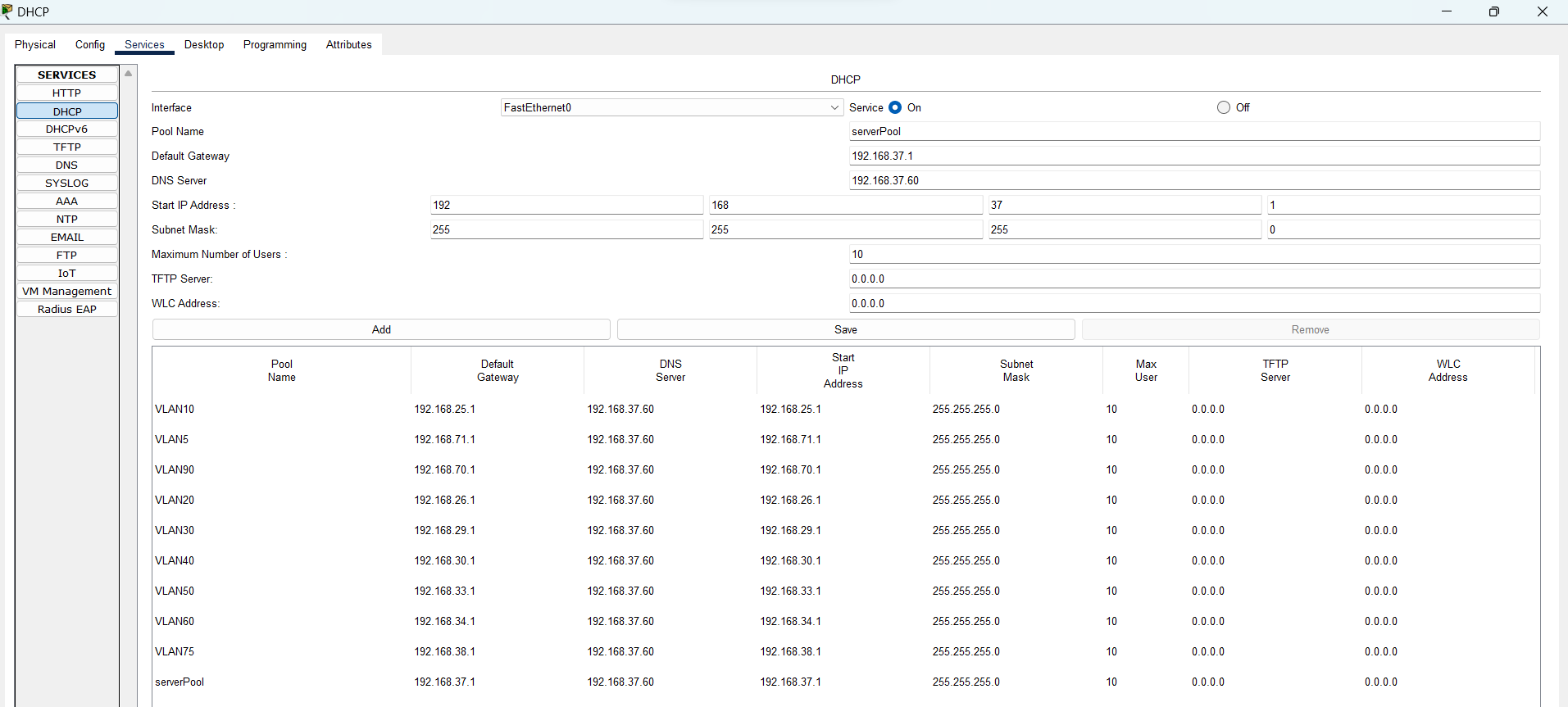


Figure Headquarter's DHCP server

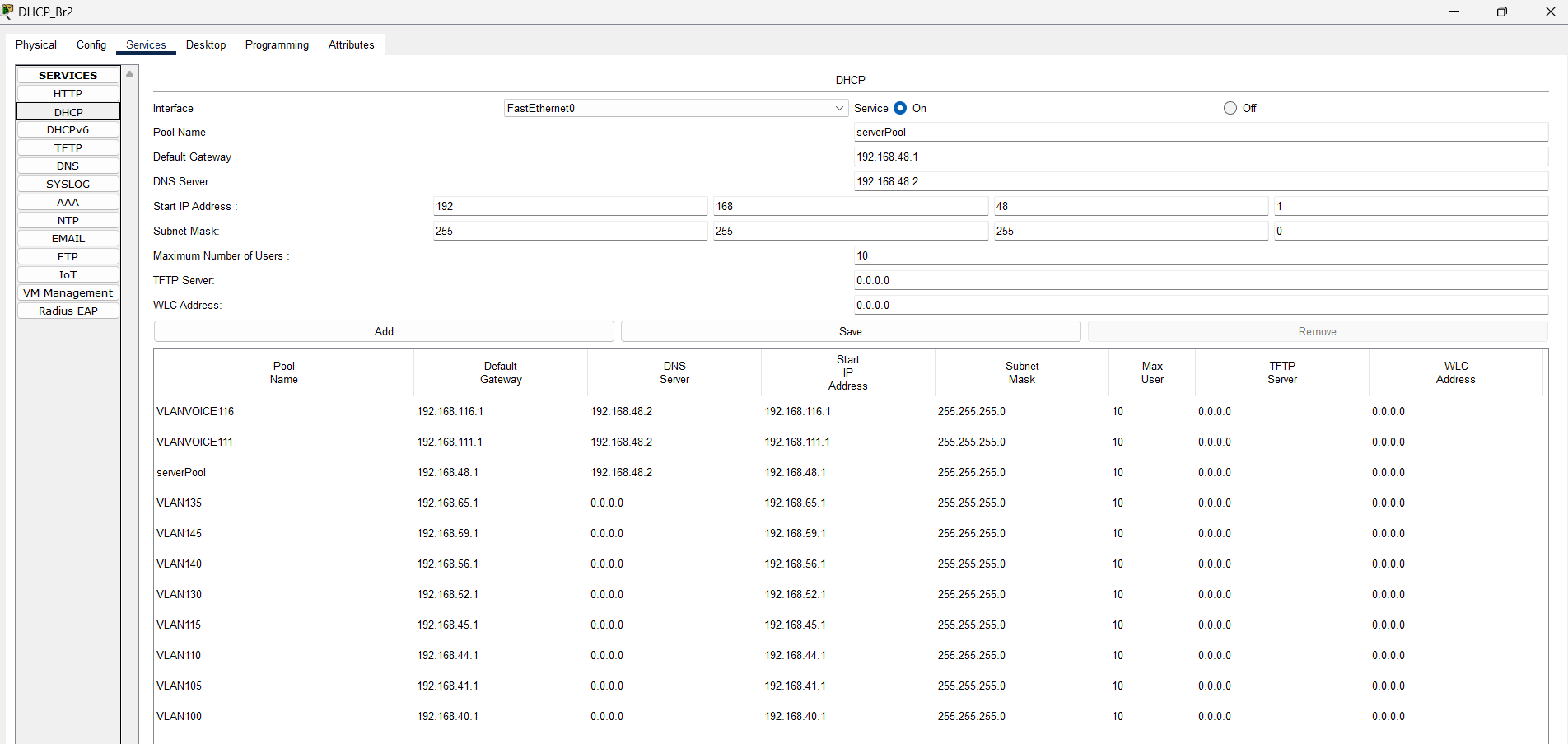


Figure Branch's DHCP server

* DNS (Domain Name System): DNS servers are configured to translate domain names to IP addresses within the network. This is essential for internal name resolution of services, such as web servers and VoIP systems

# 8. Voice and Video Technologies

* VoIP (Voice over IP): The network is configured to support VoIP services for internal communication. Quality of Service (QoS) is applied to ensure that voice traffic is prioritized over other types of traffic, ensuring high-quality voice calls.
* IP Phones: IP phones are deployed at various endpoints, connected to the network through PoE (Power over Ethernet) enabled switches. VoIP VLANs are isolated to ensure secure and reliable voice communication.

# 9. IoT Integration

* 4G Cellular Tower: A 4G cellular tower is included in the design to connect IoT devices and provide mobile connectivity. This enables real-time data transmission from remote devices such as sensors, IP cameras, and environmental monitors.
* IoT Devices: IoT devices are placed in their own VLAN to separate them from other user traffic. They communicate with the rest of the network via specific security policies to prevent unauthorized access or attacks on the main network.

# 10. High Availability and Redundancy

* To ensure maximum uptime and reliability, the following techniques are implemented:
* Redundant Core and Distribution Links: The core and distribution layers are interconnected using redundant links to prevent single points of failure.
* Multiple Routing Protocols: The use of multiple routing protocols like OSPF, EIGRP, and RIP provides redundancy and flexibility in case of link failures.
* Failover Configurations: Routers are configured with failover links to automatically reroute traffic in case of primary link failure.

# 11. Conclusion

This enterprise network topology represents a scalable, redundant, and secure solution to support modern data, voice, and IoT services. By incorporating advanced technologies such as OSPF, EIGRP, VLANs, NAT, ACLs, and VoIP, the network is designed to handle the complex requirements of a growing organization. The use of 4G technology for IoT integration extends connectivity to remote devices, ensuring the enterprise is future-proof and ready for modern challenges.