Network Design Document

Project Client	Organization: Cisco Projects of Projects
System Name	VLAN Network Design with restricted Internet Access
Date of Design Document	April 10, 2020
Version Number	Version 2
Prepared by	Chris Mara, Andy Chang, Rishi Lalbahadur, and Marcos Fermin
Team Members	Chris Mara, Andy Chang, Rishi Lalbahadur, and Marcos Fermin

1. Change History

All changes to the Design Document must be recorded in the Change History.

Date	Description of Change	Reason for Change	Version No.
3/20/2020	Initial draft	N/A	Version 1
04/10/2020	Midterm	Enhancements	Version 2

2. Table of Contents

3. Executive Summary

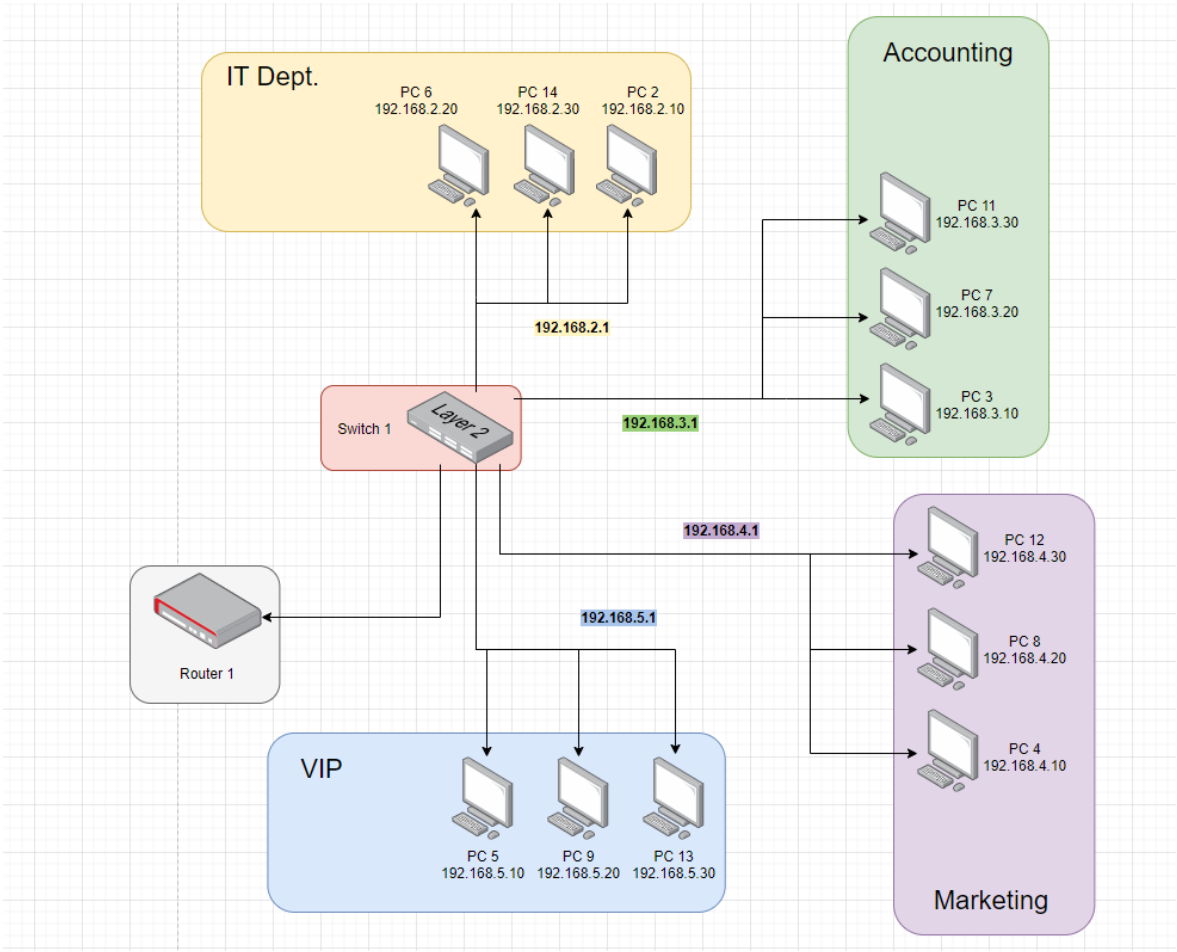
Companies have many different departments on their network, as a result VLANs have become necessary for businesses. The project is a secure network for an enterprise with four departments (accounting, IT, marketing, VIP), with potential growth to the enterprise. VPN is on a designated VLAN to channel data throughout each department.

4. Project Goals

The goal of this project is to design secure VLANs and potentially build out a growing enterprise network.

5. Logical Design

5.1. Logical Network Diagram



5.2. Addressing and Naming Structure

- Router IP: 192.168.1.10
- Computers containing “192.168.2.0” are the Information Technology Department
  - 192.168.2.10
  - 192.168.2.20
  - 192.168.2.30
- Computers containing “192.168.3.0” are the Marketing Department
  - 192.168.3.10

    - 192.168.3.20
    - 192.168.3.30
- Computers containing “192.168.4.0” are the VIP Department
    - 192.168.4.10
    - 192.168.4.20
    - 192.168.4.30
- Computers containing “192.168.5.0” are the Accounting Department
    - 192.168.5.10
    - 192.168.5.20
    - 192.168.5.30

5.3. Routing and Switching Protocols

The web traffic will be TCP packets over port 80. Port 80 is needed to have the internet operating. Each VLAN will not have internet except for the IT department. The IT department is allowed to communicate with other departments and vise versa, but other departments are not allowed to communicate with each other.

5.4. Security

- Password-based on the router and the switch
- Switch Port Security: each port corresponds to a MAC address on a certain computer. If a computer is swapped, the port will shut down and must be restarted for the network to operate again.
- The IT department has access to all other VLANs. However, each other VLAN only has access to the IT department.
- Enabled SSH(uses encryption to secure data from eavesdropping) and Disabled Telnet (use clear text username and password which can be hacked or sniffed by hackers easily).
- Disabled CISCO Discovery Protocol, CDP can be a security risk in today's networks.

5.5. Virtual LANs

- Computers containing “192.168.2.0” are the Information Technology Department
- Computers containing “192.168.3.0” are the Marketing Department
- Computers containing “192.168.4.0” are the VIP Department
- Computers containing “192.168.5.0” are the Accounting Department

6. Physical Design

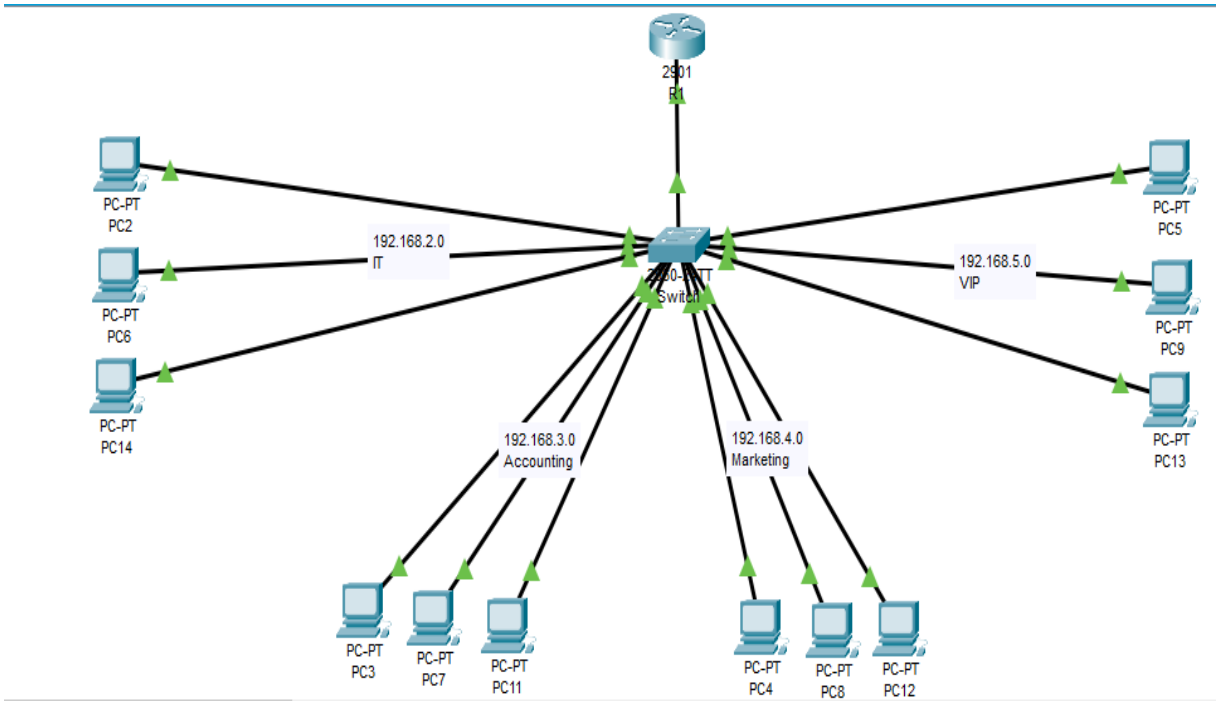
6.1. Network Topology

- Star Topology: All nodes are connected to a centralized point, in our case a switch.

6.2. LAN technologies

- Copper straight-through Cable is a type of twisted pair copper wire cable for local area network (LAN) use for which the RJ-45 connectors at each end have the same pinout. Straight through cable use one wiring standard: both ends use T568A wiring standard or both ends use T568B wiring standard.
- A Copper straight-through Cable is being used to connect the switch to the router. Straight-through cables are used to connect each computer to the switch.

6.3. Physical Network Diagram


2901
R1
PC-PT
PC2
PC-PT
PC6
PC-PT
PC14
192.168.2.0
IT
2960-24TT
Switch
192.168.5.0
VIP
PC-PT
PC5
PC-PT
PC9
PC-PT
PC13
192.168.3.0
Accounting
192.168.4.0
Marketing
PC-PT
PC3
PC-PT
PC7
PC-PT
PC11
PC-PT
PC4
PC-PT
PC8
PC-PT
PC12