ITNET02 Case Study

Phase 2

Xcite Interactive Game Studio Network Documentation

Submitted by:

Bolima, Dave Aldwin L.

Go, Aldrich Matthew S.

Lim, Shaun Tristan Y.

Submitted to:

Mr. Fritz Kevin S. Flores

December 5, 2023

Table of Contents

1. Introduction

In the fast-paced landscape of modern business, an efficient and robust network infrastructure is paramount to the success and sustainability of any organization. This case study outlines the comprehensive network upgrade plan from the previous flat network design proposed for the new site of Xcite, a dynamic game studio specializing in mobile and online PC games. The company comprises a diverse team of developers, graphic artists, creative writers, marketers, and IT professionals. The proposed network design aims to address critical requirements and challenges faced by the company, ensuring enhanced scalability, connectivity, and security. The primary contents of this case study include a short introduction, cost of materials, physical layout, physical topology, logical topology, IP addressing Scheme, security configuration, and device running configuration.

1. Cost of Materials: This section includes the budget allocation for procuring the necessary hardware, cables, switches, routers, and other networking equipment. It is crucial to strike a balance between performance and cost-effectiveness while ensuring the chosen components meet the scalability requirements of the company. A cost of materials table which tallies the total cost of network devices and cabling can be found in this section.

2. Physical Layout: The physical layout of the network infrastructure is pivotal for efficient operations. It encompasses the arrangement of devices, cabling, and equipment within the premises. Careful consideration must be given to factors such as cable routing, device placement, cable trays, and physical resource utilization to ensure a secure and organized environment. A floor plan which details the physical layout of the network can be found in this section.

3. Physical Topology: The physical topology defines the actual layout of the network components, including switches, routers, servers, and host devices. Given the requirements of Xcite, collapsed two-tier campus or collapsed core network design can be found. A device interconnection table which provides a list of each network device’s interfaces and the corresponding devices connected can also be found in this section.

4. Logical Topology: The logical topology focuses on the flow of data within the network, irrespective of its physical placement. It encompasses the configuration of virtual LANs (VLANs) and ensures that users and devices can communicate efficiently. A well-structured logical topology forms the backbone of a high-performing network. The logical topology represents all infrastructure devices (routers and switches), servers and network printers; and includes a representative PC for each department present on a switch and indicates their host names and IP addresses.

5. IP Addressing Scheme: A well designed IP addressing scheme is paramount to facilitate smooth communication between devices. Utilizing the IPv4 address space 172.16.0.0/20, a common subnet will be assigned to the 6 departments within the organization. These departments are the Developer Department, Marketing / Finance Department, Creative Department, IT Department, Services, and Management. The subnet is sufficiently sized to accommodate the expected doubling of company size. An IP Addressing Assignment

Table that displays each device’s hostname, IP address, subnet mask, default gateway, and the VLAN these are part of can be found in this section.

6. Security Configuration: In an era of increasing cyber threats, robust security measures are non-negotiable. Initial device settings for routers and switches were configured following best practices to ensure manageability and security. Additionally, remote access to infrastructure devices were provided, safeguarding against unauthorized access and data capture. A table showing the requirement and security measures implemented as well as the enable secret, console, VTY and VTP can be found in this section.

7. Device Running Configuration: This section pertains to the specific configurations of individual networking devices. It includes the settings of the routers and switches to ensure they operate optimally within the network. A table listing the startup configurations and VLAN Brief (for switches) of network devices can be found in this section.

Scope and Assumptions:

The scope of this network redesign focuses on VLAN management for the various departments within the company, logical addressing, scalability, intranet connectivity, basic security, and manageability. This case study assumes that the existing physical infrastructure can support the upgraded network design without the need for substantial structural modifications.

Design Considerations:

- Scalability and Manageability: The design prioritizes scalability to accommodate the anticipated growth in manpower. Efficient cable routing, device selection, and installation ensure secure planning and optimal resource utilization.

- Intranet Connectivity: Full connectivity among all network groups is paramount. The design emphasizes seamless communication between users and devices.

- Basic Security Measures: An organized IP addressing scheme, VLAN implementation, and naming conventions contribute to a secure network environment. Additionally, initial device settings and the use of strong passwords follow industry best practices for enhanced security.

Expectations:

Upon implementation of this upgraded network design, Xcite Interactive can anticipate a robust, scalable, and secure infrastructure that aligns with their expansion plans. This design lays the foundation for seamless communication, efficient resource utilization, and a heightened level of security, ensuring the company's continued success in the dynamic realm of game development.

Deliverables:

This documentation will also include a packet tracer file of the proposed network to showcase its functionality as well as its adherence to company standards and requirements. The file will have all the devices pre-configured with the IP addressing scheme and the security measures included within this document. Each device is also connected according to the interconnection setup described. The simulated network aims to demonstrate that all devices can successfully communicate with each other and that all network devices follow the appropriate security measures to minimize vulnerabilities to external threats, with the design of the network being flexible, resilient, scalable, and manageable.

2. Cost of Materials

Being a limited start-up, there must be a balance between price to performance. No layer 3 switches were used in this network due to its cost and the inability to maximize its capabilities. Instead, we opted for a collapsed two-tier campus or collapsed core network design, following a modified router-on-a-stick. However, instead of using a layer 3 switch and router, we decided to use layer 2 switches and routers instead to save cost.

The layer 2 switch selected was the Cisco 2960 WS-C2960-24TT-L. This is because of its proven reliability, robust build quality and longevity. Its performance ensures network stability even in demanding environments. The switch can provide forwarding bandwidths up to 100-108 Gigabyte per second (Gbps) and switching bandwidth, which is full duplex up to 216 Gigabyte per second (Gbps). Furthermore, the switch also comes with a wide variety of software applications and features to provide easy operations, sustainability, highly secure business operations, as well as a borderless networking experience. In addition, since security is a paramount consideration, the switch incorporates a range of features to address this concern. These include access control lists (ACLs), VLAN support, and advanced security measures such as DHCP Snooping and Dynamic ARP Inspection, providing protection against various types of network attacks. The switch also supports Quality of Service (QoS) mechanisms, ensuring critical applications receive the necessary bandwidth and resources. It offers multiple management options, including a web-based interface, command-line interface (CLI), and Simple Network Management Protocol (SNMP), making it accessible to network administrators of varying skill levels. Additionally, the Cisco 2960 series is designed with energy efficiency in mind, featuring technologies like Energy Efficient Ethernet (EEE) and low-power modes during periods of inactivity to reduce power consumption. Finally, given its rich feature set, 24 fast ethernet ports, and 2 gigabit ethernet ports, the switch is cost effective starting at only 20,000 Philippine pesos.

The router to be used is Cisco 1941 router. One of the main reasons is also due to its proven reliability. Cisco routers typically have a long lifecycle, with support for software updates and security patches for an extended period. This helps ensure that the network remains secure and up to date. The router offers increased levels of services integration with data, security, wireless, and mobility services enabling greater efficiency and cost savings. Furthermore, the modular architecture is designed to support expanding user requirements, increased bandwidth, a diversity of connection options, and network resiliency. In addition, the router is future-enabled with multi-core CPUs, Gigabit Ethernet switching with enhanced POE, and new energy monitoring and control capabilities while enhancing overall system performance. All Cisco 1900 Series Integrated Services Routers also offer embedded hardware encryption acceleration, optional firewall, intrusion prevention, and application services. The router supports the industry's widest range of wired and wireless connectivity options such as T1/E1, xDSL, 3G, 4G LTE, and GE1.The router also offers secure collaborative communications with Group Encrypted Transport VPN, Dynamic Multipoint VPN, or Enhanced Easy VPN3. Finally, given its rich feature set and 2 fast gigabit ethernet ports, the router, like the switch, is cost effective starting at only 20,000 Philippine pesos. This makes the Cisco 1941 Router a valuable choice for seeking a sophisticated networking solution.

In total, this network design consists of 2 routers to facilitate interVLAN routing and acts as the DHCP server to assign IP addresses to the corresponding host devices. Two layer 2 switches are used to ensure resiliency in case one fails and are part of the core/distribution layer like the routers. In addition, since the marketing department has an expected total of 18 host devices and the creative department is expected to have a total of 20 host devices, each has their own corresponding layer 2 switch. However, since the developer department is expected to have 56 host devices, three layer 2 switches were used to accommodate all the users. Finally, since the IT department is expected to only contain 10 host devices, the services department only contains 3, and the management department only contains 2, all 3 departments are sharing one layer 2 switch and are separated to their corresponding VLANs. This is to save on the cost of purchasing additional layer 2 switches for the services and management department which only contain 3 and 2 devices respectively. In addition, after calculating the distances from the server room to each of the departments, as well as estimating the connection of each end device when going up and down the ceiling to be around 4 meters (there are 119 devices, when accounting the expansion, so length for of cable for devices would be 119*4 = 476m) , we have found that at least 643m (167+476) worth of cabling is needed for the layout. Therefore, we opted to use 7 Cat5e UTP Cable with a length of 100m.

Table 1. Cost of Materials

Equipment	Price	Quantity	Total
Cisco 1941 - 2 gigabit ethernet ports	₱20,000.00	2	₱40,000.00
Cisco 2960 WS-C2960-24TT-L - 24 fast ethernet ports	₱20,000.00	8	₱160,000.00
Cat5e UTP Cable 100m	₱2,000.00	7	₱14,000.00
Total			₱214,000.00

3. Physical Layout

The physical layout outlines the strategic placement of devices, switches and routers to optimize communication flow across departments without cluttering the physical environment. Careful consideration has been given to the positioning of cabling, cable trays, and other essential components to maintain an organized and efficient environment. Safety is a paramount concern, and to mitigate potential workplace hazards, cables have been expertly routed along walls and ceilings, minimizing obstruction and reducing the risk of accidents. After calculating the distances from the server room to each of the departments, as well as estimating the connection of each end device when going up and down the ceiling to be around 4 meters (there are 119 devices, when accounting the expansion, so length for of cable for devices would be 119*4 = 476m) , we have found that at least 643m (167+476) worth of cabling is needed for the layout.

In addition to functionality, visual clarity and ease of maintenance have been prioritized. Different colored cables serve as visual cues, symbolizing each department. Green cables denote the creative department, blue signifies the finance and marketing department, purple designates management, violet represents services, pink is allocated for the IT department, and red is reserved for the developer department.

This well-thought-out floor plan not only ensures efficient connectivity but also places a premium on safety and accessibility. The arrangement of devices and routing of cables has been optimized to create a robust and reliable network infrastructure that caters to the specific needs of each department. This meticulous planning is poised to contribute to a seamless and productive work environment, elevating operational efficiency across the organization.

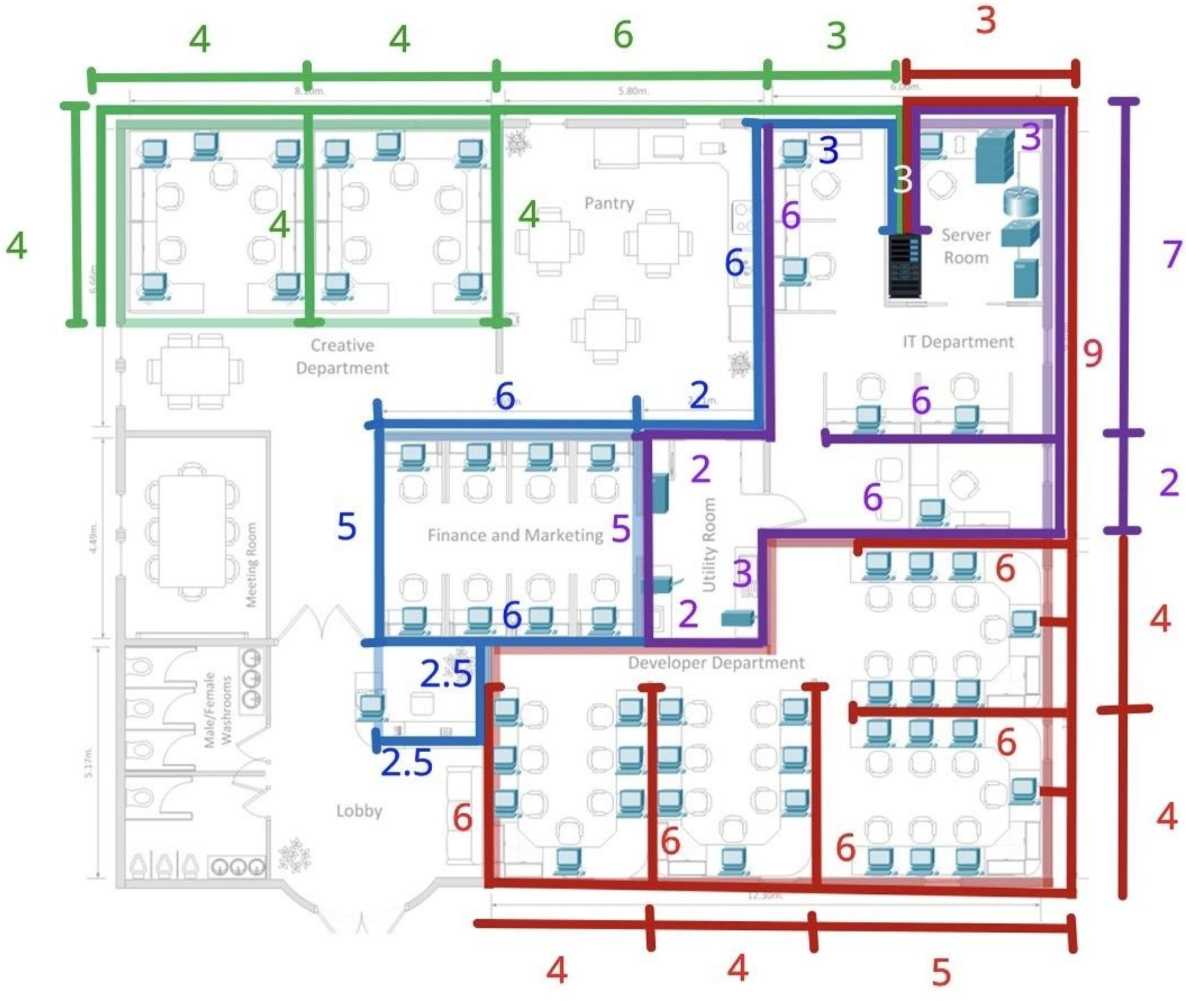


Figure 1. Physical Layout Cabling Length Estimate

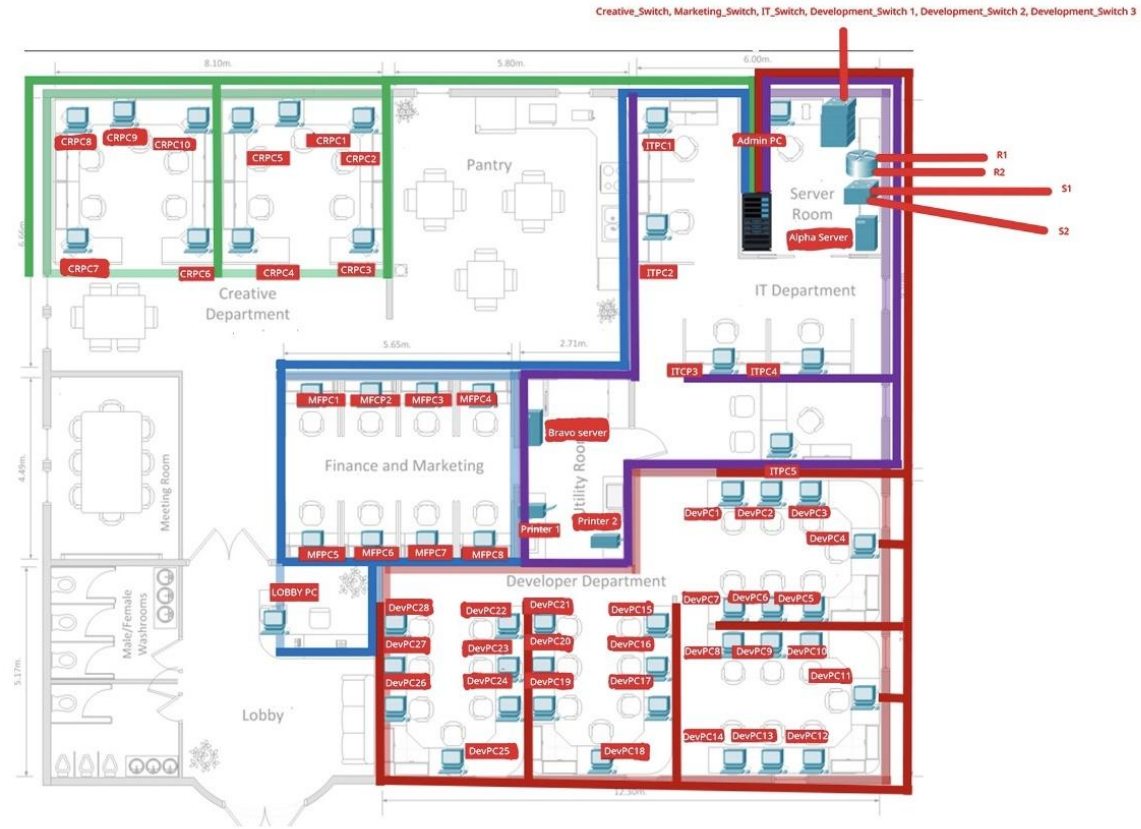


Figure 2. Physical Layout Device Names and Location

4. Physical Topology

Prior to configuring the network, it is essential to determine the specific network devices that need to be acquired, as well as their respective placements and their interconnections. This section provides a comprehensive overview of the physical topology of the recommended network design as well as device interconnections table.

The physical topology divides the device locations into their respective rooms, with the access layer devices, core/distribution devices and servers being placed in their corresponding racks and shelves. All network devices are placed in the server room to ensure security from unauthorized access. The rest of the end devices are placed in their corresponding rooms depending on which department they belong to. The device interconnection tables list the source interface of a device, the VLAN it belongs to, what device it's connected to and the interface of the connected device. All switch to switch and switch to router connections used a fast Gigabit Ethernet port if available for faster speeds during high network usage. Both routers have 1 free gigabit ethernet port for internet connectivity.

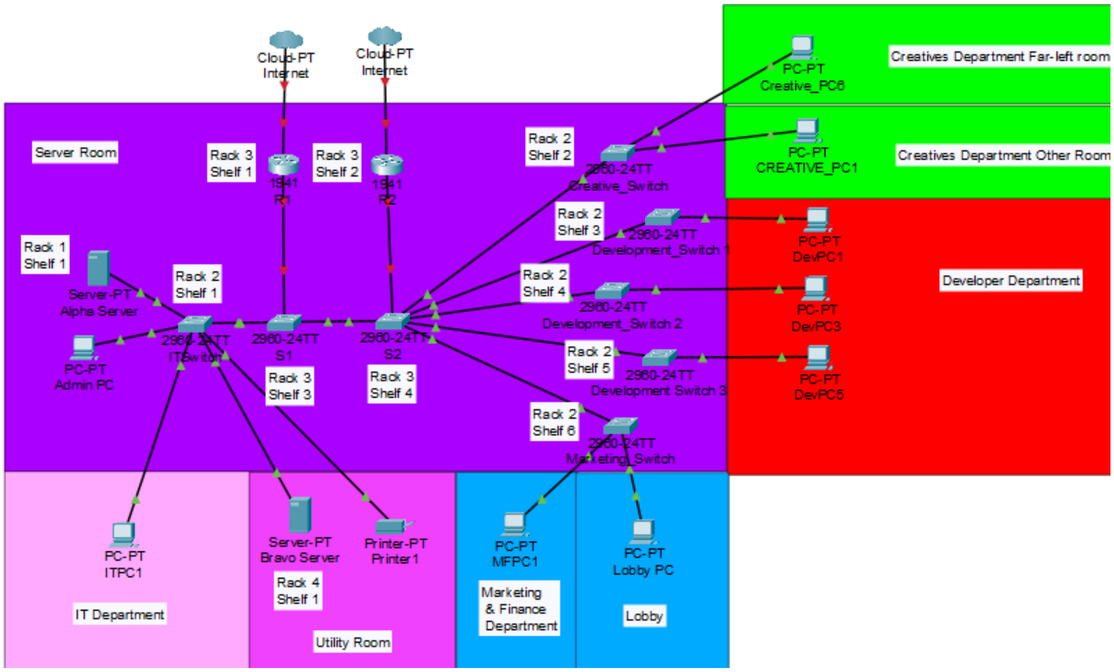


Figure 3. Physical Topology

Table 2. Device Interconnection Table for R1

R1			
Source Interface	VLAN	Connected To	Connected Interface
Gig0/1	N/A (trunk)	S1	Gig0/1

Table 3. Device Interconnection Table for R2

R2			
Source Interface	VLAN	Connected To	Connected Interface
Gig0/1	N/A (trunk)	S2	Gig0/1

Table 4. Device Interconnection Table for S1

S1			
Source Interface	VLAN	Connected To	Connected Interface
Gig0/1	N/A (trunk)	R1	Gig0/1
Gig0/2	N/A (trunk)	S2	Gig0/2
Fa0/1	N/A (trunk)	Creative_Switch	Gig0/1

Fa0/2	N/A (trunk)	Marketing_Switch	Gig0/1
Fa0/3	N/A (trunk)	IT_Switch	Gig0/1
Fa0/4	N/A(trunk)	Development_Switch1	Gig0/1
Fa0/5	N/A (trunk)	Development_Switch2	Gig0/1
Fa0/6	N/A (trunk)	Development_Switch3	Gig0/1

Table 5. Device Interconnection Table for S2

S2			
Source Interface	VLAN	Connected To	Connected Interface
Gig0/1	N/A (trunk)	R2	Gig0/1
Gig0/2	N/A (trunk)	S1	Gig0/2
Fa0/1	N/A (trunk)	Creative_Switch	Gig0/2
Fa0/2	N/A (trunk)	Marketing_Switch	Gig0/2
Fa0/3	N/A (trunk)	IT_Switch	Gig0/2

Fa0/4	N/A(trunk)	Development_Switch1	Gig0/2
Fa0/5	N/A (trunk)	Development_Switch2	Gig0/2
Fa0/6	N/A (trunk)	Development_Switch3	Gig0/2

Table 6. Device Interconnection Table for IT Switch

IT_Switch			
Source Interface	VLAN	Connected To	Connected Interface
Fa0/1	40	IT PC1	Fa0
Fa0/2	40	IT PC2	Fa0
Fa0/3	40	IT PC3	Fa0
Fa0/4	40	IT PC4	Fa0
Fa0/5	40	IT PC5	Fa0
Fa0/6	40	IT PC6	Fa0
Fa0/7	40	IT PC7	Fa0

Fa0/8	40	IT PC8	Fa0
Fa0/9	40	IT PC9	Fa0
Fa0/10	40	IT PC10	Fa0
Fa0/11	50	PRINTER1	Fa0
Fa0/12	50	PRINTER2	Fa0
Fa0/13	50	BRAVO_SERVER	Fa0
Fa0/14	99	ALPHA_SERVER	Fa0
Fa0/15	99	ADMIN_PC	Fa0
Gig0/1	N/A (trunk)	S1	Fa0/3
Gig0/2	N/A (trunk)	S2	Fa0/3

Table 7. Device Interconnection Table for Creative Switch

Creative_Switch			
Source Interface	VLAN	Connected To	Connected Interface

Fa0/1	30	CREATIVE PC1	Fa0
Fa0/2	30	CREATIVE PC2	Fa0
Fa0/3	30	CREATIVE PC3	Fa0
Fa0/4	30	CREATIVE PC4	Fa0
Fa0/5	30	CREATIVE PC5	Fa0
Fa0/6	30	CREATIVE PC6	Fa0
Fa0/7	30	CREATIVE PC7	Fa0
Fa0/8	30	CREATIVE PC8	Fa0
Fa0/9	30	CREATIVE PC9	Fa0
Fa0/10	30	CREATIVE PC10	Fa0
Fa0/11	30	CREATIVE PC11	Fa0
Fa0/12	30	CREATIVE PC12	Fa0
Fa0/13	30	CREATIVE PC13	Fa0

Fa0/14	30	CREATIVE PC14	Fa0
Fa0/15	30	CREATIVE PC15	Fa0
Fa0/16	30	CREATIVE PC16	Fa0
Fa0/17	30	CREATIVE PC17	Fa0
Fa0/18	30	CREATIVE PC18	Fa0
Fa0/19	30	CREATIVE PC19	Fa0
Fa0/20	30	CREATIVE PC20	Fa0
Gig0/1	N/A (trunk)	S1	Fa0/1
Gig0/2	N/A (trunk)	S2	Fa0/1

Table 8. Device Interconnection Table for Marketing and Finance Switch

Marketing_Switch			
Source Interface	VLAN	Connected To	Connected Interface
Fa0/1	20	FINANCE PC1	Fa0

Fa0/2	20	FINANCE PC2	Fa0
Fa0/3	20	FINANCE PC3	Fa0
Fa0/4	20	FINANCE PC4	Fa0
Fa0/5	20	FINANCE PC5	Fa0
Fa0/6	20	FINANCE PC6	Fa0
Fa0/7	20	FINANCE PC7	Fa0
Fa0/8	20	FINANCE PC8	Fa0
Fa0/9	20	FINANCE PC9	Fa0
Fa0/10	20	FINANCE PC10	Fa0
Fa0/11	20	FINANCE PC11	Fa0
Fa0/12	20	FINANCE PC12	Fa0
Fa0/13	20	FINANCE PC13	Fa0
Fa0/14	20	FINANCE PC14	Fa0

Fa0/15	20	FINANCE PC15	Fa0
Fa0/16	20	FINANCE PC16	Fa0
Fa0/17	20	LOBBY PC1	Fa0
Fa0/18	20	LOBBY PC2	Fa0
Gig0/1	N/A (trunk)	S1	Fa0/2
Gig0/2	N/A (trunk)	S2	Fa0/2

Table 9. Device Interconnection Table for First Development Switch

Development_Switch1			
Source Interface	VLAN	Connected To	Connected Interface
Fa0/1	10	DEVELOPMENT PC1	Fa0
Fa0/2	10	DEVELOPMENT PC2	Fa0
Fa0/3	10	DEVELOPMENT PC3	Fa0
Fa0/4	10	DEVELOPMENT PC4	Fa0

Fa0/5	10	DEVELOPMENT PC5	Fa0
Fa0/6	10	DEVELOPMENT PC6	Fa0
Fa0/7	10	DEVELOPMENT PC7	Fa0
Fa0/8	10	DEVELOPMENT PC8	Fa0
Fa0/9	10	DEVELOPMENT PC9	Fa0
Fa0/10	10	DEVELOPMENT PC10	Fa0
Fa0/11	10	DEVELOPMENT PC11	Fa0
Fa0/12	10	DEVELOPMENT PC12	Fa0
Fa0/13	10	DEVELOPMENT PC13	Fa0
Fa0/14	10	DEVELOPMENT PC14	Fa0
Fa0/15	10	DEVELOPMENT PC15	Fa0
Fa0/16	10	DEVELOPMENT PC16	Fa0
Fa0/17	10	DEVELOPMENT PC17	Fa0

Fa0/18	10	DEVELOPMENT PC18	Fa0
Fa0/19	10	DEVELOPMENT PC19	Fa0
Fa0/23	N/A (trunk)	Development_Switch3	Fa0/23
Fa0/24	N/A (trunk)	Development_Switch2	Fa0/24
Gig0/1	N/A (trunk)	S1	Fa0/4
Gig0/2	N/A (trunk)	S2	Fa0/4

Table 10. Device Interconnection Table for Second Development Switch

Development_Switch2			
Source Interface	VLAN	Connected To	Connected Interface
Fa0/1	10	DEVELOPMENT PC20	Fa0
Fa0/2	10	DEVELOPMENT PC21	Fa0
Fa0/3	10	DEVELOPMENT PC22	Fa0
Fa0/4	10	DEVELOPMENT PC23	Fa0

Fa0/5	10	DEVELOPMENT PC24	Fa0
Fa0/6	10	DEVELOPMENT PC25	Fa0
Fa0/7	10	DEVELOPMENT PC26	Fa0
Fa0/8	10	DEVELOPMENT PC27	Fa0
Fa0/9	10	DEVELOPMENT PC28	Fa0
Fa0/10	10	DEVELOPMENT PC29	Fa0
Fa0/11	10	DEVELOPMENT PC30	Fa0
Fa0/12	10	DEVELOPMENT PC31	Fa0
Fa0/13	10	DEVELOPMENT PC32	Fa0
Fa0/14	10	DEVELOPMENT PC33	Fa0
Fa0/15	10	DEVELOPMENT PC34	Fa0
Fa0/16	10	DEVELOPMENT PC35	Fa0
Fa0/17	10	DEVELOPMENT PC36	Fa0

Fa0/18	10	DEVELOPMENT PC37	Fa0
Fa0/23	N/A (trunk)	Development_Switch3	Fa0/24
Fa0/24	N/A (trunk)	Development_Switch1	Fa0/24
Gig0/1	N/A (trunk)	S1	Fa0/5
Gig0/2	N/A (trunk)	S2	Fa0/5

Table 11. Device Interconnection Table for Third Development Switch

Development_Switch3			
Source Interface	VLAN	Connected To	Connected Interface
Fa0/1	10	DEVELOPMENT PC38	Fa0
Fa0/2	10	DEVELOPMENT PC39	Fa0
Fa0/3	10	DEVELOPMENT PC40	Fa0
Fa0/4	10	DEVELOPMENT PC41	Fa0
Fa0/5	10	DEVELOPMENT PC42	Fa0

Fa0/6	10	DEVELOPMENT PC43	Fa0
Fa0/7	10	DEVELOPMENT PC44	Fa0
Fa0/8	10	DEVELOPMENT PC45	Fa0
Fa0/9	10	DEVELOPMENT PC46	Fa0
Fa0/10	10	DEVELOPMENT PC47	Fa0
Fa0/11	10	DEVELOPMENT PC48	Fa0
Fa0/12	10	DEVELOPMENT PC49	Fa0
Fa0/13	10	DEVELOPMENT PC50	Fa0
Fa0/14	10	DEVELOPMENT PC51	Fa0
Fa0/15	10	DEVELOPMENT PC52	Fa0
Fa0/16	10	DEVELOPMENT PC53	Fa0
Fa0/17	10	DEVELOPMENT PC54	Fa0
Fa0/18	10	DEVELOPMENT PC55	Fa0

Fa0/19	10	DEVELOPMENT PC56	Fa0
Fa0/23	N/A (trunk)	Development_Switch1	Fa0/23
Fa0/24	N/A (trunk)	Development_Switch2	Fa0/23
Gig0/1	N/A (trunk)	S1	Fa0/6
Gig0/2	N/A (trunk)	S2	Fa0/6

5. Logical Topology

The logical topology diagram of the network illustrates a well-structured and resilient architecture designed for efficiency and scalability. The network is organized according to VLAN assignments, facilitating efficient communication and management across the different departments. The inclusion of two representative PCs per department allows for comprehensive testing of intra-VLAN connectivity, ensuring robust communication within each segment. This approach reflects a thorough consideration for network reliability. Redundancy is another cornerstone of this design, with two routers and two switches in the core/distribution layer. This setup guarantees continuous available connectivity even in the event of a cable or device failure. This redundancy strategy aligns with best practices for network resilience. The architecture adheres to the collapsed two-tier campus or collapsed core network design, allowing the visualization of the role of switches depending on where they are in the hierarchy and ensures consistent configuration across switches per layer. In addition, this topology follows a replicable pattern where if the department contains enough users, it can have its own corresponding layer 2 switch. This allows for seamless network expansion and integrated services without heavy impact on network performance. Lastly, this logical topology provides a hierarchical visualization to easily distinguish the core/distribution layer from the access layer.

The network is divided into six distinct subnets, each corresponding to a specific department or function. These include the Developer Department (VLAN 10), Marketing & Finance Department (VLAN 20), Creative Department (VLAN 30), IT Department (VLAN 40), Services (VLAN 50), and Management (VLAN 99). There is also a blackhole VLAN (VLAN 100) reserved for unused ports. This segmentation enhances security, manageability, and performance optimization. The marketing and creative department each contain one layer 2 access layer switch. The developer department is equipped with three layer 2 switches, accommodating its higher user density. The IT department, services, and management departments share a single layer 2 switch, demonstrating an efficient allocation of resources.

In the diagram, each port is meticulously labeled, and devices are clearly designated, providing a visual reference for easy identification. Devices belonging to the same VLAN are grouped together, with VLAN names, network addresses, subnet masks, and default gateways clearly indicated. Each VLAN is also color coded. This enhances the diagram's clarity and aids in understanding the assignment of devices to specific VLANs. Overall, this network design exemplifies a balanced approach to resilience, modularity, and manageability. Its scalability and redundancy measures position it as a robust foundation for future growth and integrated services, while its logical organization and comprehensive labeling make it a valuable tool for administrators and technicians alike.

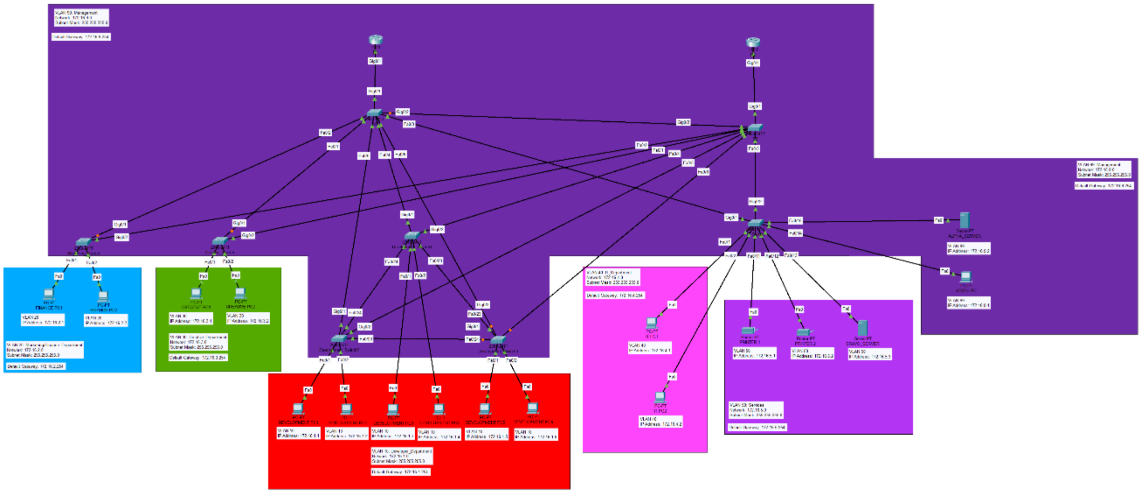


Figure 4. Logical Topology - Resilient Design (Overall view)

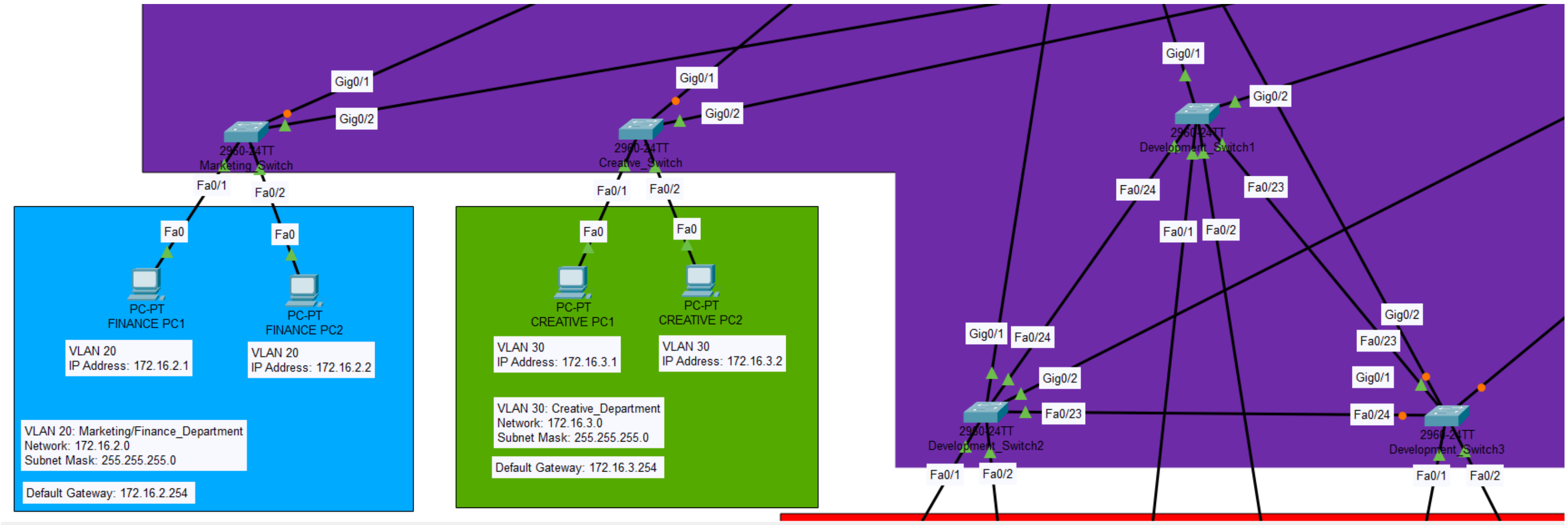


Figure 5. Zoomed in Logical Topology of VLAN 20 and 30

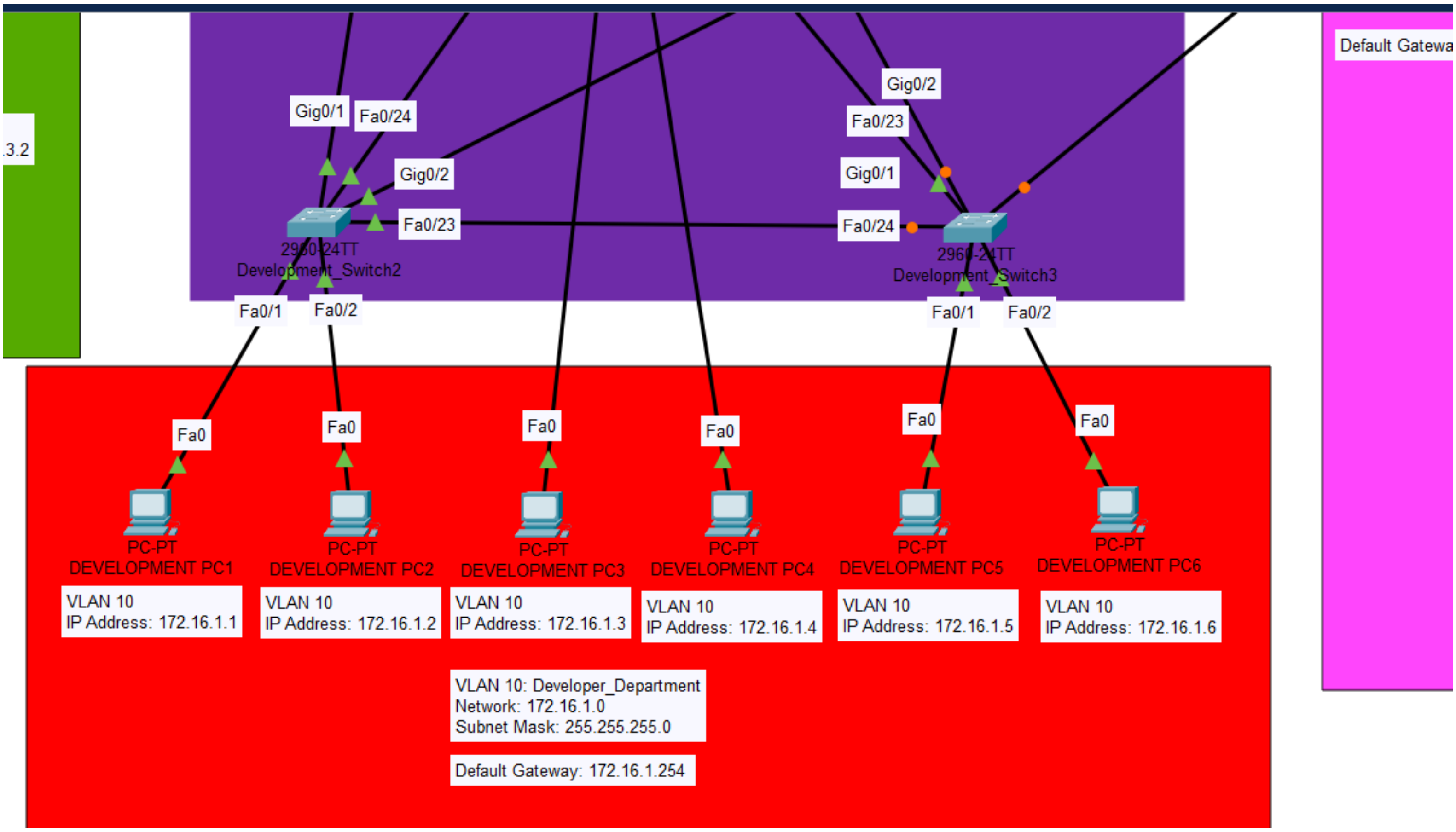


Figure 6. Zoomed in Logical Topology of VLAN 10

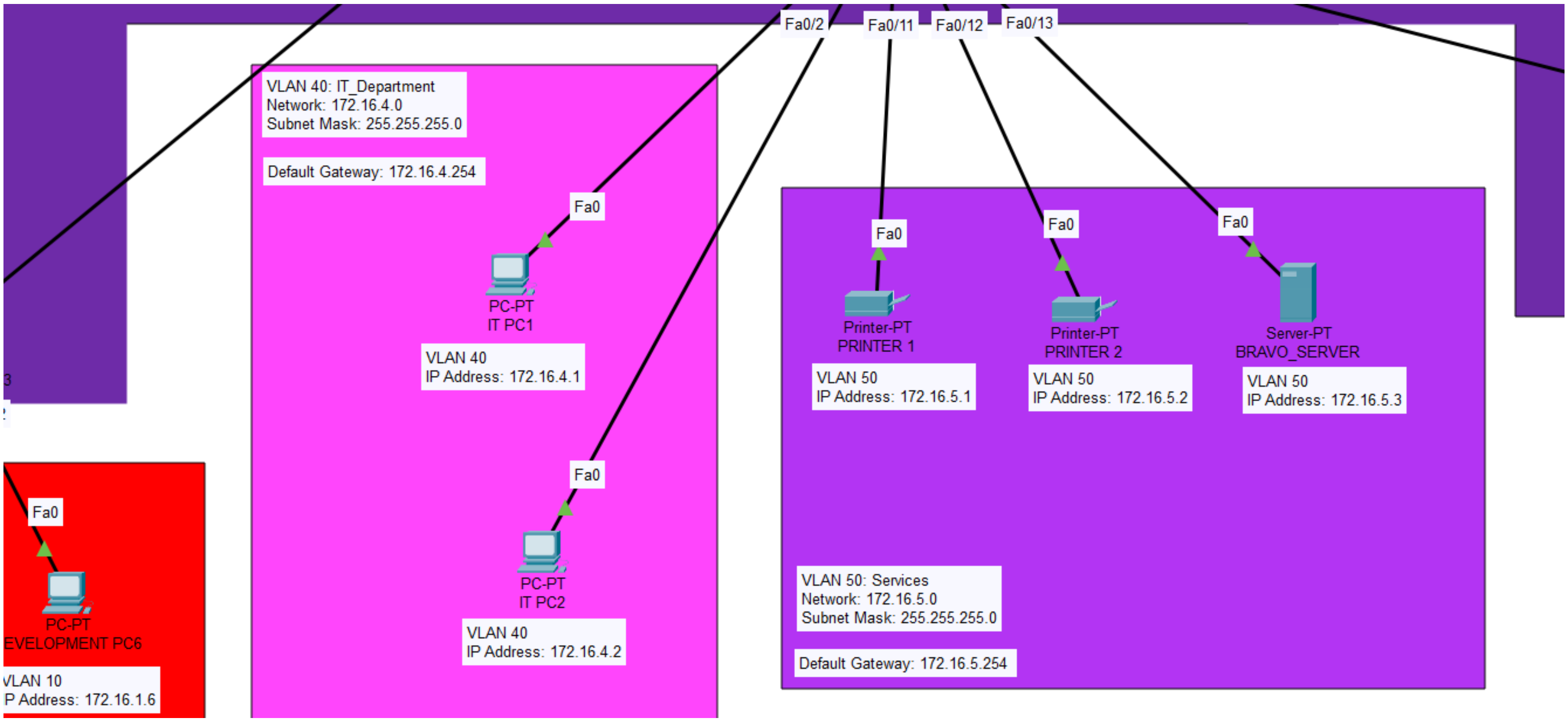


Figure 7. Zoomed in Logical Topology of VLAN 40 and 50

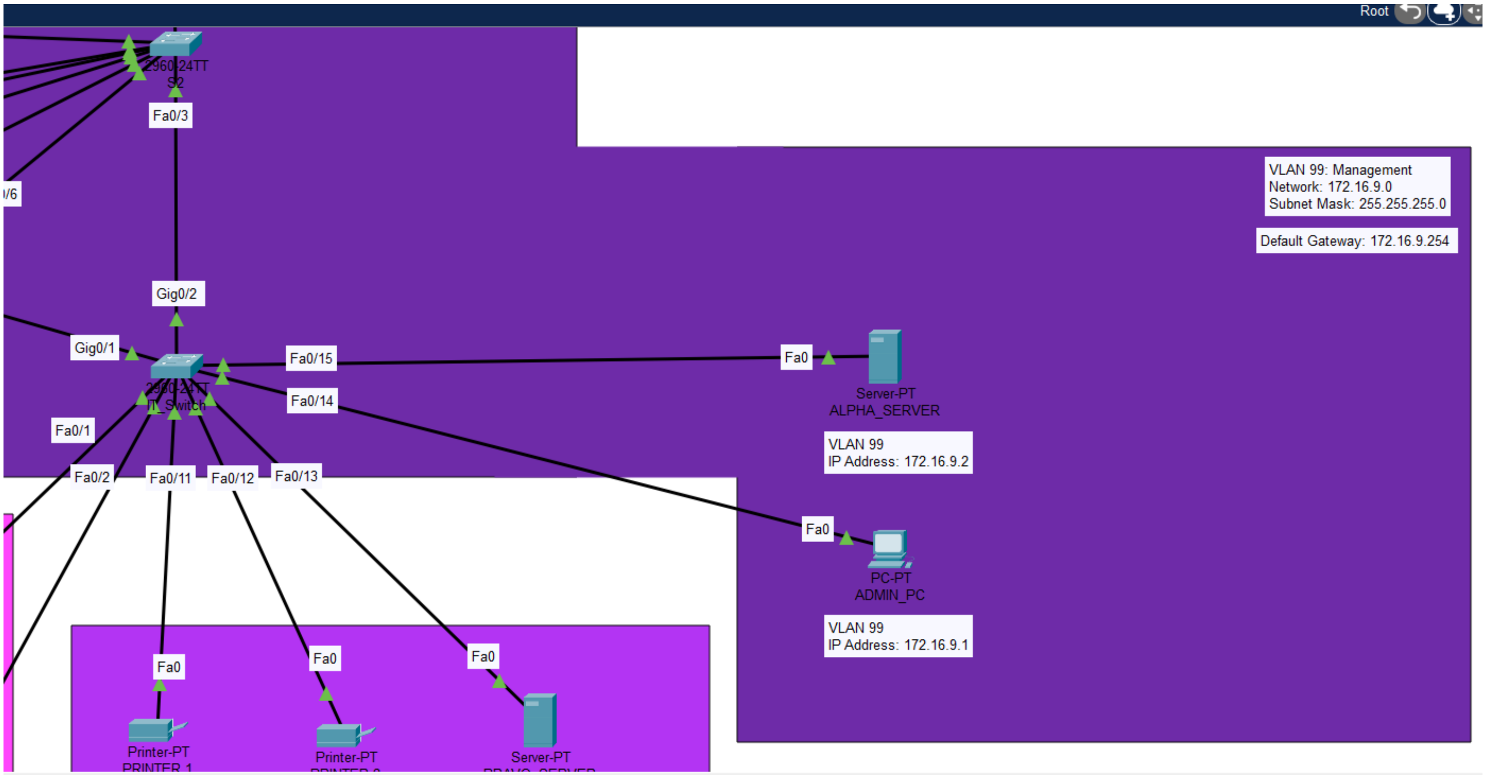


Figure 8. Zoomed in Logical Topology of VLAN 99

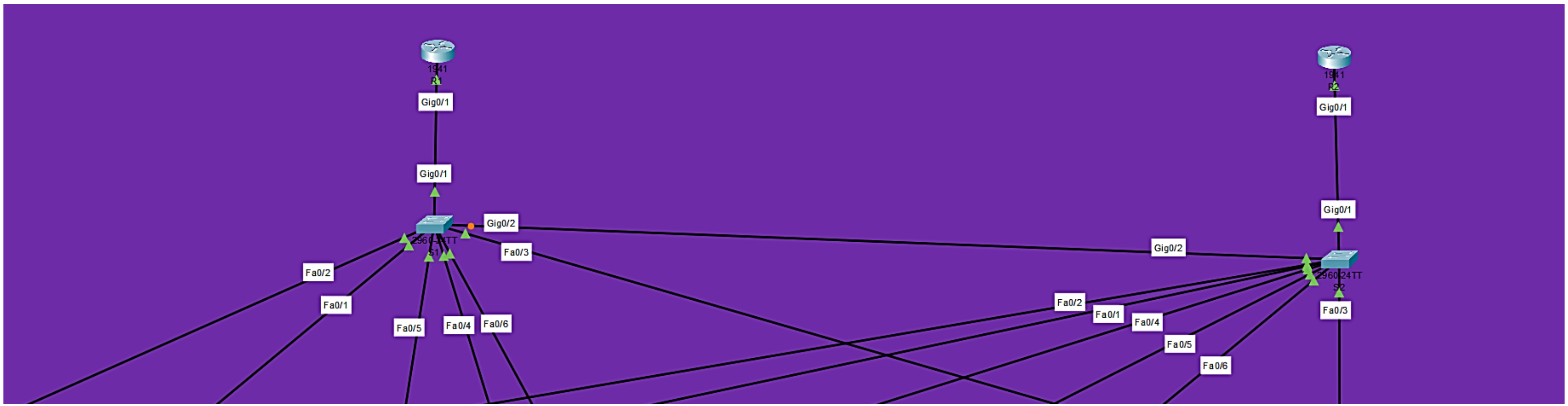
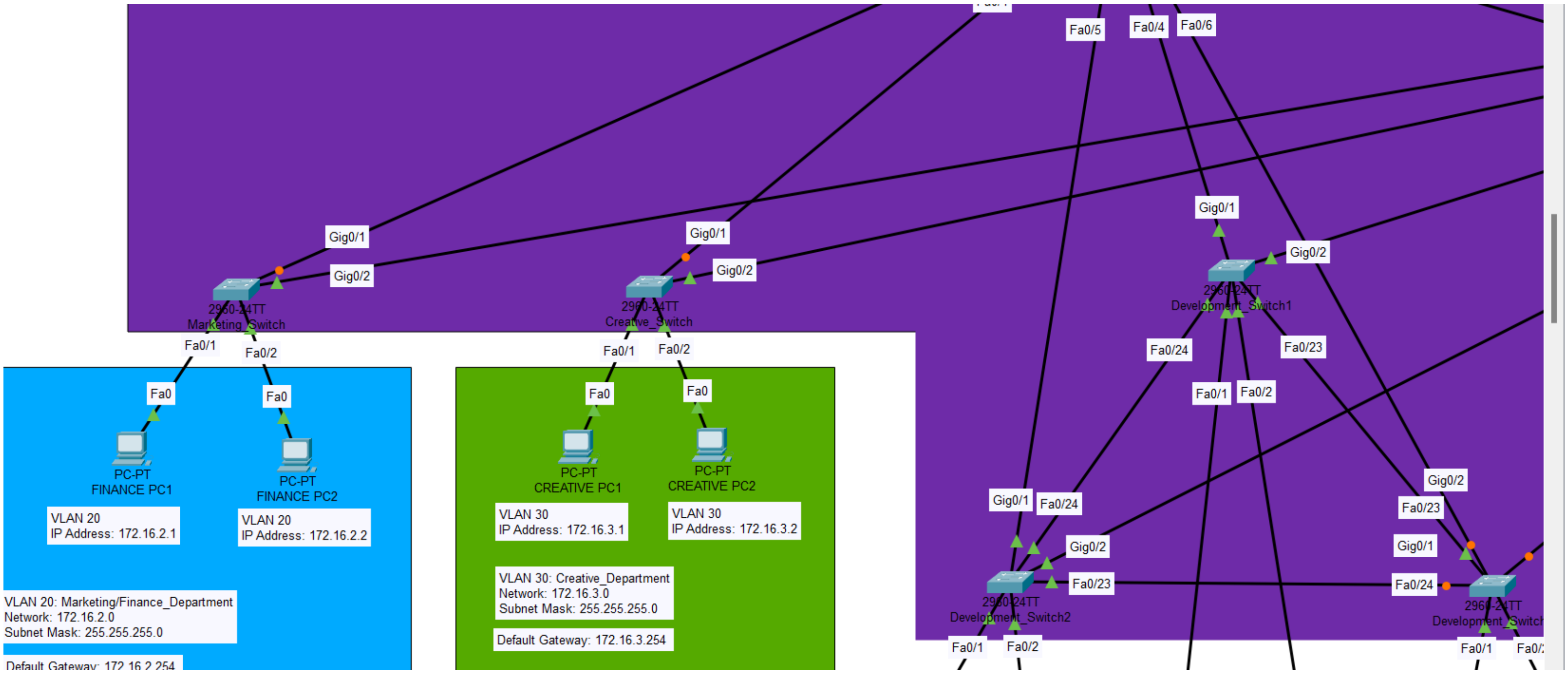


Figure 9. Zoomed in Logical Topology of collapsed core/distribution layer

Figure 10. Zoomed in Logical Topology of left side of the distribution layer



VLAN 20
IP Address: 172.16.2.1

VLAN 20
IP Address: 172.16.2.2

VLAN 20: Marketing/Finance_Department
Network: 172.16.2.0
Subnet Mask: 255.255.255.0

Default Gateway: 172.16.2.254

VLAN 30
IP Address: 172.16.3.1

VLAN 30
IP Address: 172.16.3.2

VLAN 30: Creative_Department
Network: 172.16.3.0
Subnet Mask: 255.255.255.0

Default Gateway: 172.16.3.254

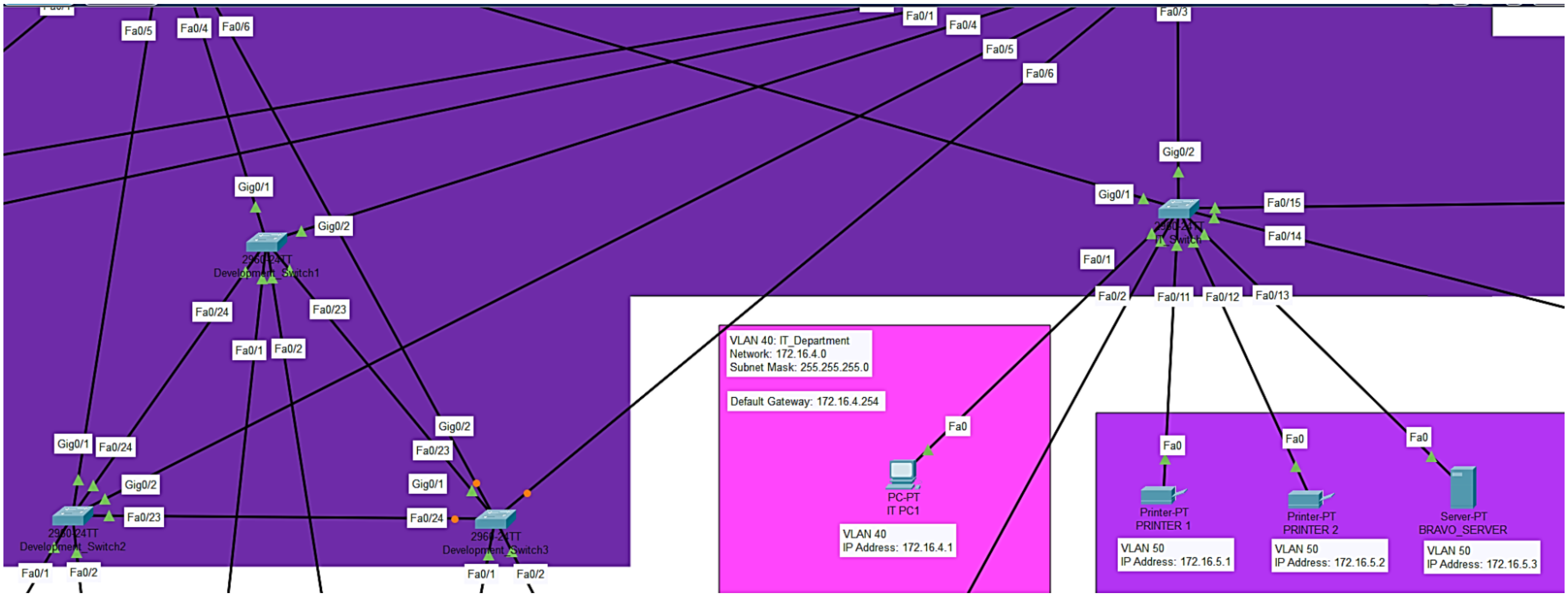


Figure 11. Zoomed in Logical Topology of right side of the distribution layer

Table 12. IP Addressing Table

Network Name	Network Address	Subnet Mask	Host Range	VLAN ID
Developer (28 + 28 hosts)	172.16.1.0	255.255.255.0	172.16.1.1 - 172.16.1.254	10
Marketing and Finance (9 + 9 hosts)	172.16.2.0	255.255.255.0	172.16.2.1 - 172.16.2.254	20
Creative (10 + 10 hosts)	172.16.3.0	255.255.255.0	172.16.3.1 - 172.16.3.254	30
IT (5 + 5 hosts)	172.16.4.0	255.255.255.0	172.16.4.1 - 172.16.4.254	40

Services (3 hosts)	172.16.5.0	255.255.255.0	172.16.5.1 - 172.16.5.254	50
Management (12 hosts)	172.16.9.0	255.255.255.0	172.16.9.1 - 172.16.9.254	99

6. IP Addressing Scheme

This section provides comprehensive details about the IP Addresses of each network, encompassing information such as the device name within the network, the connected interface, its assigned IP address, subnet mask, and default gateway. Following the allocation of the IPv4 address space 172.16.0.0/20 and employing Variable Length Subnet Masking (VLSM), a uniform subnet mask of 255.255.255.0 has been applied across all VLANs/networks. This choice stems from the convenience it affords in allocating the value of the third octet to its respective VLAN. For instance, an IP address like 172.16.1.19 is affiliated with VLAN 10. This approach can be advantageous for administrators in terms of ease of management and reducing the need to remember subnet masks for each VLAN. It simplifies the configuration process and can make troubleshooting and documentation more straightforward. This streamlines the identification of a host device's VLAN and ensures a straightforward scaling process for future departmental additions, each with its designated VLAN. Furthermore, the default gateway for each VLAN is set to the last usable address within the network. This practice aligns with Cisco standards and facilitates a clear understanding of the network's capacity in terms of device accommodation.

Table 13. IP Addressing Assignment Table for Management VLAN

Device Name	Interface	IP Address	Subnet Mask	Default Gateway
MANAGEMENT (VLAN 99)				
R1	G0/0.10	172.16.1.254	255.255.255.0	N/A
	G0/0.20	172.16.2.254	255.255.255.0	
	G0/0.30	172.16.3.254	255.255.255.0	
	G0/0.40	172.16.4.254	255.255.255.0	
	G0/0.50	172.16.5.254	255.255.255.0	
	G0/0.99	172.16.9.254	255.255.255.0	
R2	G0/0.10	172.16.1.254	255.255.255.0	

	G0/0.20	172.16.2.254	255.255.255.0	N/A
	G0/0.30	172.16.3.254	255.255.255.0	
	G0/0.40	172.16.4.254	255.255.255.0	
	G0/0.50	172.16.5.254	255.255.255.0	
	G0/0.99	172.16.9.254	255.255.255.0	
Development_Switch1	VLAN 99	172.16.9.10	255.255.255.0	172.16.9.254
Development_Switch2		172.16.9.11	255.255.255.0	
Development_Switch3		172.16.9.12	255.255.255.0	
Marketing_Switch		172.16.9.20	255.255.255.0	
Creative_Switch		172.16.9.30	255.255.255.0	
IT_Switch		172.16.9.40	255.255.255.0	
S1		172.16.9.50	255.255.255.0	
S2		172.16.9.50	255.255.255.0	

ALPHA_SERVER	F0	172.16.9.1	255.255.255.0	
ADMIN_PC	F0	172.16.9.2	255.255.255.0	

Table 14. IP Addressing Assignment Table for Development Department

Device Name	Interface	IP Address	Subnet Mask	Default Gateway
DEVELOPER DEPARTMENT (VLAN 10)				
DEVELOPMENT PC1	F0	172.16.1.1	255.255.255.0	172.16.1.254
DEVELOPMENT PC2	F0	172.16.1.2	255.255.255.0	172.16.1.254
DEVELOPMENT PC3	F0	172.16.1.3	255.255.255.0	172.16.1.254
DEVELOPMENT PC4	F0	172.16.1.4	255.255.255.0	172.16.1.254
DEVELOPMENT PC5	F0	172.16.1.5	255.255.255.0	172.16.1.254
DEVELOPMENT PC6	F0	172.16.1.6	255.255.255.0	172.16.1.254
DEVELOPMENT PC7	F0	172.16.1.7	255.255.255.0	172.16.1.254
DEVELOPMENT PC8	F0	172.16.1.8	255.255.255.0	172.16.1.254

DEVELOPMENT PC9	F0	172.16.1.9	255.255.255.0	172.16.1.254
DEVELOPMENT PC10	F0	172.16.1.10	255.255.255.0	172.16.1.254
DEVELOPMENT PC11	F0	172.16.1.11	255.255.255.0	172.16.1.254
DEVELOPMENT PC12	F0	172.16.1.12	255.255.255.0	172.16.1.254
DEVELOPMENT PC13	F0	172.16.1.13	255.255.255.0	172.16.1.254
DEVELOPMENT PC14	F0	172.16.1.14	255.255.255.0	172.16.1.254
DEVELOPMENT PC15	F0	172.16.1.15	255.255.255.0	172.16.1.254
DEVELOPMENT PC16	F0	172.16.1.16	255.255.255.0	172.16.1.254
DEVELOPMENT PC17	F0	172.16.1.17	255.255.255.0	172.16.1.254
DEVELOPMENT PC18	F0	172.16.1.18	255.255.255.0	172.16.1.254
DEVELOPMENT PC19	F0	172.16.1.19	255.255.255.0	172.16.1.254
DEVELOPMENT PC20	F0	172.16.1.20	255.255.255.0	172.16.1.254
DEVELOPMENT PC21	F0	172.16.1.21	255.255.255.0	172.16.1.254

DEVELOPMENT PC22	F0	172.16.1.22	255.255.255.0	172.16.1.254
DEVELOPMENT PC23	F0	172.16.1.23	255.255.255.0	172.16.1.254
DEVELOPMENT PC24	F0	172.16.1.24	255.255.255.0	172.16.1.254
DEVELOPMENT PC25	F0	172.16.1.25	255.255.255.0	172.16.1.254
DEVELOPMENT PC26	F0	172.16.1.26	255.255.255.0	172.16.1.254
DEVELOPMENT PC27	F0	172.16.1.27	255.255.255.0	172.16.1.254
DEVELOPMENT PC28	F0	172.16.1.28	255.255.255.0	172.16.1.254
DEVELOPMENT PC29	F0	172.16.1.29	255.255.255.0	172.16.1.254
DEVELOPMENT PC30	F0	172.16.1.30	255.255.255.0	172.16.1.254
DEVELOPMENT PC31	F0	172.16.1.31	255.255.255.0	172.16.1.254
DEVELOPMENT PC32	F0	172.16.1.32	255.255.255.0	172.16.1.254
DEVELOPMENT PC33	F0	172.16.1.33	255.255.255.0	172.16.1.254
DEVELOPMENT PC34	F0	172.16.1.34	255.255.255.0	172.16.1.254

DEVELOPMENT PC35	F0	172.16.1.35	255.255.255.0	172.16.1.254
DEVELOPMENT PC36	F0	172.16.1.36	255.255.255.0	172.16.1.254
DEVELOPMENT PC37	F0	172.16.1.37	255.255.255.0	172.16.1.254
DEVELOPMENT PC38	F0	172.16.1.38	255.255.255.0	172.16.1.254
DEVELOPMENT PC39	F0	172.16.1.39	255.255.255.0	172.16.1.254
DEVELOPMENT PC40	F0	172.16.1.40	255.255.255.0	172.16.1.254
DEVELOPMENT PC41	F0	172.16.1.41	255.255.255.0	172.16.1.254
DEVELOPMENT PC42	F0	172.16.1.42	255.255.255.0	172.16.1.254
DEVELOPMENT PC43	F0	172.16.1.43	255.255.255.0	172.16.1.254
DEVELOPMENT PC44	F0	172.16.1.44	255.255.255.0	172.16.1.254
DEVELOPMENT PC45	F0	172.16.1.45	255.255.255.0	172.16.1.254
DEVELOPMENT PC46	F0	172.16.1.46	255.255.255.0	172.16.1.254
DEVELOPMENT PC47	F0	172.16.1.47	255.255.255.0	172.16.1.254

DEVELOPMENT PC48	F0	172.16.1.48	255.255.255.0	172.16.1.254
DEVELOPMENT PC49	F0	172.16.1.49	255.255.255.0	172.16.1.254
DEVELOPMENT PC50	F0	172.16.1.50	255.255.255.0	172.16.1.254
DEVELOPMENT PC51	F0	172.16.1.51	255.255.255.0	172.16.1.254
DEVELOPMENT PC52	F0	172.16.1.52	255.255.255.0	172.16.1.254
DEVELOPMENT PC53	F0	172.16.1.53	255.255.255.0	172.16.1.254
DEVELOPMENT PC54	F0	172.16.1.54	255.255.255.0	172.16.1.254
DEVELOPMENT PC55	F0	172.16.1.55	255.255.255.0	172.16.1.254
DEVELOPMENT PC56	F0	172.16.1.56	255.255.255.0	172.16.1.254

Table 15. IP Addressing Assignment Table for Marketing and Finance Department

Device Name	Interface	IP Address	Subnet Mask	Default Gateway
MARKETING AND FINANCE DEPARTMENT (VLAN 20)				
FINANCE PC1	F0	172.16.2.1	255.255.255.0	172.16.2.254

FINANCE PC2	F0	172.16.2.2	255.255.255.0	172.16.2.254
FINANCE PC3	F0	172.16.2.3	255.255.255.0	172.16.2.254
FINANCE PC4	F0	172.16.2.4	255.255.255.0	172.16.2.254
FINANCE PC5	F0	172.16.2.5	255.255.255.0	172.16.2.254
FINANCE PC6	F0	172.16.2.6	255.255.255.0	172.16.2.254
FINANCE PC7	F0	172.16.2.7	255.255.255.0	172.16.2.254
FINANCE PC8	F0	172.16.2.8	255.255.255.0	172.16.2.254
FINANCE PC9	F0	172.16.2.9	255.255.255.0	172.16.2.254
FINANCE PC10	F0	172.16.2.10	255.255.255.0	172.16.2.254
FINANCE PC11	F0	172.16.2.11	255.255.255.0	172.16.2.254
FINANCE PC12	F0	172.16.2.12	255.255.255.0	172.16.2.254
FINANCE PC13	F0	172.16.2.13	255.255.255.0	172.16.2.254
FINANCE PC14	F0	172.16.2.14	255.255.255.0	172.16.2.254

FINANCE PC15	F0	172.16.2.15	255.255.255.0	172.16.2.254
FINANCE PC16	F0	172.16.2.16	255.255.255.0	172.16.2.254
LOBBY PC1	F0	172.16.2.17	255.255.255.0	172.16.2.254
LOBBY PC2	F0	172.16.2.18	255.255.255.0	172.16.2.254

Table 16. IP Addressing Assignment Table for Creative Department

Device Name	Interface	IP Address	Subnet Mask	Default Gateway
CREATIVE DEPARTMENT (VLAN 30)				
CREATIVE PC1	F0	172.16.3.1	255.255.255.0	172.16.3.254
CREATIVE PC2	F0	172.16.3.2	255.255.255.0	172.16.3.254
CREATIVE PC3	F0	172.16.3.3	255.255.255.0	172.16.3.254
CREATIVE PC4	F0	172.16.3.4	255.255.255.0	172.16.3.254
CREATIVE PC5	F0	172.16.3.5	255.255.255.0	172.16.3.254
CREATIVE PC6	F0	172.16.3.6	255.255.255.0	172.16.3.254

CREATIVE PC7	F0	172.16.3.7	255.255.255.0	172.16.3.254
CREATIVE PC8	F0	172.16.3.8	255.255.255.0	172.16.3.254
CREATIVE PC9	F0	172.16.3.9	255.255.255.0	172.16.3.254
CREATIVE PC10	F0	172.16.3.10	255.255.255.0	172.16.3.254
CREATIVE PC11	F0	172.16.3.11	255.255.255.0	172.16.3.254
CREATIVE PC12	F0	172.16.3.12	255.255.255.0	172.16.3.254
CREATIVE PC13	F0	172.16.3.13	255.255.255.0	172.16.3.254
CREATIVE PC14	F0	172.16.3.14	255.255.255.0	172.16.3.254
CREATIVE PC15	F0	172.16.3.15	255.255.255.0	172.16.3.254
CREATIVE PC16	F0	172.16.3.16	255.255.255.0	172.16.3.254
CREATIVE PC17	F0	172.16.3.17	255.255.255.0	172.16.3.254
CREATIVE PC18	F0	172.16.3.18	255.255.255.0	172.16.3.254
CREATIVE PC19	F0	172.16.3.19	255.255.255.0	172.16.3.254

CREATIVE PC20	F0	172.16.3.20	255.255.255.0	172.16.3.254

Table 17. IP Addressing Assignment Table for IT Department

Device Name	Interface	IP Address	Subnet Mask	Default Gateway
IT DEPARTMENT (VLAN 40)				
IT PC1	F0	172.16.4.1	255.255.255.0	172.16.4.254
IT PC2	F0	172.16.4.2	255.255.255.0	172.16.4.254
IT PC3	F0	172.16.4.3	255.255.255.0	172.16.4.254
IT PC4	F0	172.16.4.4	255.255.255.0	172.16.4.254
IT PC5	F0	172.16.4.5	255.255.255.0	172.16.4.254
IT PC6	F0	172.16.4.6	255.255.255.0	172.16.4.254
IT PC7	F0	172.16.4.7	255.255.255.0	172.16.4.254
IT PC8	F0	172.16.4.8	255.255.255.0	172.16.4.254
IT PC9	F0	172.16.4.9	255.255.255.0	172.16.4.254

IT PC10	F0	172.16.4.10	255.255.255.0	172.16.4.254

Table 18. IP Addressing Assignment Table for Services VLAN

Device Name	Interface	IP Address	Subnet Mask	Default Gateway
SERVICES (VLAN 50)				
PRINTER1	F0	172.16.5.1	255.255.255.0	172.16.5.254
PRINTER2	F0	172.16.5.2	255.255.255.0	172.16.5.254
BRAVO_SERVER	F0	172.16.5.3	255.255.255.0	172.16.5.254

7. Security Configuration

Network security is a critical aspect of any network infrastructure. Without proper safeguards, networks are vulnerable to numerous threats, including DHCP snooping, DHCP starvation attacks, ARP poisoning attacks and many more. Furthermore, unauthorized infiltrators can illicitly retrieve vital network data, potentially leading to financial losses and reputational damage. Given these potential vulnerabilities, prioritizing network security is of utmost importance.

In response to these challenges, we have implemented a comprehensive suite of security measures. The first line of defense is the configuration of all routers and switches with initial device settings, adhering to best practices for manageability and security. For secure remote access, all routers and switches are configured to allow SSH instead of Telnet. Additionally, all switches are configured with VLAN Trunk Protocol (VTP) to ensure consistency and accuracy of VLAN configuration across the network. This also optimizes the use of trunk links by pruning unnecessary broadcast traffic from VLANs not present on downstream switches.

To streamline network administration, both routers function as DHCP servers, centralizing the control of IP address distribution. This facilitates easier monitoring and management of network configurations. Trunk ports are also configured to disable DTP negotiation, preventing the sending of DTP frames when the neighboring device does not support DTP. Moreover, access ports in a switch are secured from unauthorized access by observing incoming source MAC addresses on a configured port, dynamically learning them, and adding them to the running configuration. All unused ports are also assigned to a blackhole VLAN. Furthermore, to enhance security, IP DHCP snooping is enabled to prevent breaches and attacks such as DHCP Starvation and DHCP spoofing. ARP inspection is also enabled to validate ARP packets in the network, thereby preventing data theft, unauthorized monitoring, ARP spoofing attacks, and other threats that exploit ARP weaknesses.

Finally, Access Control Lists (ACLs) are implemented to prevent unauthorized access to certain VLANs and to organize traffic, thereby improving network efficiency. Coupled with secure password practices and basic housekeeping, these measures ensure the robustness of our network security. This comprehensive approach to network security ensures that Xcite’s network remains secure, efficient, and resilient in the face of potential threats. By prioritizing security, we can protect the network and the valuable data it carries, ensuring the continued success of Xcite's operations.

Table 19. Security Measures Implemented

Requirement	Security Measure Implemented
All routers and switches must be configured with initial device settings as a primary line of defense against unauthorized access to a network and its sensitive data following best practices for manageability and security.	§ Set up a banner message warning users of unauthorized access § Set privileged exec, console and line VTY passwords § All network devices have their own unique passwords § Implement password encryption § Used passwords with the following characteristics: 1. Minimum length of 8 characters with all passwords having a length of 16 characters for additional security. 2. Included lowercase and uppercase letters. 3. Always begins with a letter. 4. Included a mix of symbols except the '?' 5. No similar, duplicate or sequential characters § Shutdown unused ports
All routers and switches must be configured to allow for SSH instead of Telnet to remotely access the devices securely.	§ Had all network devices' IP domain set to xcite.com § Generated an RSA Key with 2048 bits § Set the SSH version to 2 to gain full access to all the features § Set a unique username and password for each network device § Each username has the word "Admin" to indicate that only the admin is allowed access to the SSH. § Used unique passwords with the following characteristics: 1. Minimum length of 8 characters with all passwords having a length of 16 characters for additional security. 2. Included lowercase and uppercase letters. 3. Always begins with a letter. 4. Included a mix of symbols except the '?' 5. No similar, duplicate or sequential characters

	§ Configure the virtual terminal lines (VTY) on a Cisco device to accept incoming SSH connections only § Configure the VTY lines to enable the SSH protocol on the VTY lines and require local authentication using the local username database. § Set the maximum idle time of the connection for 3 minutes § (Router only) Set the VTY lines' blocking duration to 300 seconds for 5 incorrect login attempts within 120 seconds.
All switches must be configured with VTP to maintain consistency and accuracy of VLAN configuration by propagating any changes made on one switch to all other switches in the domain. This also allows for efficient use of trunk links by pruning unnecessary broadcast traffic from VLANs that are not present on the downstream switches.	§ Set S1 and S2 as the VTP server since they are the common switches that all the departments are connected to. § All other department switches are the VTP clients § Set the VTP domain name as xcite.com § Used a common VTP password with the following characteristics: 1. Minimum length of 8 characters with all passwords having a length of 16 characters for additional security. 2. Included lowercase and uppercase letters. 3. Always begins with a letter. 4. Included a mix of symbols except the '?' 5. No similar, duplicate or sequential characters § Set the VTP version to 2, since version 2 can perform additional consistency checks and support Token Ring networks.
Both routers function as the DHCP server to simplify the process of assigning and managing IP addresses within a network. This simplifies network administration by centralizing the control of IP address distribution, making it easier to monitor and manage network configurations.	§ Create a DHCP pool for each VLAN with its corresponding department name § Excluded the network, broadcast address, and default gateway for VLAN 10, 20, 30, 40 and 50 § Excluded the network, broadcast address, default gateway and IP address of the network devices for VLAN 99 § Excluded the first 127 usable IP address of VLAN 10,20,30,40 and 50 for R1 § Excluded the last 127 usable IP address of VLAN 10,20,30,40 and 50 for R2 § Excluded the first 127 usable IP address of

	VLAN 99 for R1 § Excluded the last 127 usable IP address of VLAN 99 for R2 § Specify the corresponding network for each VLAN § Specify the corresponding default gateway assigned for each VLAN
Configure the trunk ports to disable DTP negotiation to stop it from sending DTP frames when the neighboring device does not support DTP.	§ Issue the switchport trunk nonegotiate command
Secure all the access ports in a switch from unauthorized access by observing the incoming source MAC addresses on a configured port, dynamically learning it and adding them to the running configuration. Assign all unused ports to a blackhole VLAN to prevent VLAN hopping attacks, isolate traffic in the data flow, and restrict user access within the network.	§ Enable port security § Set the maximum number of MAC addresses allowed on each port to 2 § Set the maximum number of MAC addresses allowed on the admin port to 1 § Enable the sticky learning of MAC addresses § Set the action to take when a violation occurs to restrict to drop the packets but not shutdown the port. § Set the action to take when a violation occurs to shutdown for the admin port for increased security. § Assign the unused ports to VLAN 100 or the blackhole VLAN
Enable IP DHCP snooping to prevent security breaches and attacks such as DHCP Starvation attack and DHCP spoofing attack.	§ Enable DHCP snooping globally on the switch § Enable DHCP snooping on the specified VLANs that will pass through the switch. § Configure the selected interfaces that are connected to switches or routers as trusted interfaces § Set a rate limit for DHCP packets on the selected interfaces that are access ports to 2. If the number of DHCP packets received per second exceeds this limit, the extra packets will be dropped.

Enable ARP inspection to check the validity of ARP packets in a network. This stops data theft, unauthorized monitoring, ARP spoofing attacks, and other threats that use ARP weaknesses.	§ Enable Dynamic ARP Inspection (DAI) on the specified VLANs that will pass through the switch. § Configure the selected interfaces that are connected to switches or routers as trusted interfaces so the switch does not check ARP packets that it receives on the trusted interface.
Implement Access Control Lists (ACLs) to prevent unauthorized access to certain VLANs and organize traffic to improve network efficiency.	§ Add a remark to know the function of the ACL and which VLANs are restricted. § Number the ACL according to the VLAN number § Configure the allowed VLANs in the corresponding ACL § Configure a deny statement to block all traffic that doesn’t match the permitted IP addresses § Assign the ACL to the corresponding sub interface § Apply the ACL to outbound traffic on the selected interface

Table 20. Access Control Matrix

Department	Development	Marketing and Finance	Creative	IT	Services	Management
Development	✓	🟥	✓	✓	✓	🟥
Marketing and Finance	🟥	✓	🟥	✓	✓	🟥
Creative	✓	🟥	✓	✓	✓	🟥
IT	✓	✓	✓	✓	✓	🟥
Services	✓	✓	✓	✓	✓	🟥
Management	🟥	🟥	🟥	🟥	🟥	✓

Table 21. Usernames and Password

Device	Enable Secret	Console	VTY	VTP
S1	yH[UsMBubqQ362w%	r%<H6WBT/>ZnkLU.	Username: AdminS1 Password: pS58-E7~%`tgC>=e	Server Password: Mz$NruW2,7f~[:'Y
S2	yH[UsMBubqQ362w%	r%<H6WBT/>ZnkLU.	Username: AdminS2 Password: pS58-E7~%`tgC>=e	Server Password: Mz$NruW2,7f~[:'Y
DEVELOPMENT_SWITCH 1	v<9x=dD-4~ncML7J	zW*96`.:U2;AdS'E	Username: AdminDevelopment1 Password: y%j5*r;t)mzD2GAd	Client Password: Mz$NruW2,7f~[:'Y
DEVELOPMENT_ SWITCH 2	Kt&.8h;rbU9W_S6d	U"KMp:g9';2Q84{L	Username: AdminDevelopment2 Password: qAEKc'Y{43FX2mrU	Client Password: Mz$NruW2,7f~[:'Y
DEVELOPMENT_ SWITCH 3	g/y)n5-[F}Q(Se7%	L)<3vjg}bnQeyRN6	Username: AdminDevelopment3 Password: qLQD=Cb3Tv*c7@6R	Client Password: Mz$NruW2,7f~[:'Y
MARKETING_ SWITCH	F6QqS9U$te]2d"WR	hy4'(.9H"[B-rz%~	Username: AdminMarketing	Client Password:

			Password: SxLG$YDeu9mUft[P	Mz$NruW2,7f~[:'Y
CREATIVE_ SWITCH	c'h)PuHDL]4N8RVm	YcMWQ!r;2sH3K}a8	Username: AdminCreative Password: TLNG&FxU5H#@.jX_	Client Password: Mz$NruW2,7f~[:'Y
IT_SWITCH	tC%qDmxgz5GAU,B}	R$+~B*PVCv8.N!k3	Username: AdminIT Password: s,h<grX(uD+[5j%v	Client Password: Mz$NruW2,7f~[:'Y
R1	a3@h+4Tzk/rFVBvC	VZ$"[4{,muph5eLc	Username: AdminR1 Password: TtX5{u73V6-G^4Lb	IP Domain Name: xcite.com Crypto Key RSA:2048
R2	a3@h+4Tzk/rFVBvC	VZ$"[4{,muph5eLc	Username: AdminR2 Password: TtX5{u73V6-G^4Lb	IP Domain Name: xcite.com Crypto Key RSA:2048

8. Device Running Configuration

Table 21. Device Configuration

Device Name: R1

```
Current configuration : 4941 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 16
!
hostname R1
!
login block-for 300 attempts 5 within 120
!
enable secret 5 $1$mERr$S02MYM.h6rz9962O2Ext7/
!
ip dhcp relay information trust-all
!
ip dhcp excluded-address 172.16.1.0
ip dhcp excluded-address 172.16.1.254
ip dhcp excluded-address 172.16.1.255
ip dhcp excluded-address 172.16.2.0
ip dhcp excluded-address 172.16.2.254
ip dhcp excluded-address 172.16.2.255
ip dhcp excluded-address 172.16.3.0
ip dhcp excluded-address 172.16.3.254
ip dhcp excluded-address 172.16.3.255
ip dhcp excluded-address 172.16.4.0
ip dhcp excluded-address 172.16.4.254
ip dhcp excluded-address 172.16.4.255
ip dhcp excluded-address 172.16.5.0
ip dhcp excluded-address 172.16.5.254
ip dhcp excluded-address 172.16.5.255
ip dhcp excluded-address 172.16.9.0
ip dhcp excluded-address 172.16.9.10
ip dhcp excluded-address 172.16.9.11
ip dhcp excluded-address 172.16.9.12
ip dhcp excluded-address 172.16.9.20
ip dhcp excluded-address 172.16.9.30
ip dhcp excluded-address 172.16.9.40
ip dhcp excluded-address 172.16.9.50
ip dhcp excluded-address 172.16.9.254
ip dhcp excluded-address 172.16.9.255
ip dhcp excluded-address 172.16.1.128 172.16.1.253
ip dhcp excluded-address 172.16.2.128 172.16.2.253
ip dhcp excluded-address 172.16.3.128 172.16.3.253
ip dhcp excluded-address 172.16.4.128 172.16.4.253
ip dhcp excluded-address 172.16.5.128 172.16.5.253
ip dhcp excluded-address 172.16.9.128 172.16.9.253
!
ip dhcp pool DEVELOPER
network 172.16.1.0 255.255.255.0
default-router 172.16.1.254
ip dhcp pool MARKETING
network 172.16.2.0 255.255.255.0
default-router 172.16.2.254
ip dhcp pool CREATIVE
network 172.16.3.0 255.255.255.0
default-router 172.16.3.254
ip dhcp pool IT
network 172.16.4.0 255.255.255.0
default-router 172.16.4.254
ip dhcp pool SERVICES
network 172.16.5.0 255.255.255.0
default-router 172.16.5.254
ip dhcp pool MANAGEMENT
network 172.16.9.0 255.255.255.0
default-router 172.16.9.254
!
ip cef
no ipv6 cef
!
username AdminR1 privilege 15 secret 5 $1$mERr$dCLLeDqh8A2bEBqsDJIV80
!
license udi pid CISCO1941/K9 sn FTX1524SJHC-
!
ip ssh version 2
no ip domain-lookup
ip domain-name xcite.com
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
```

```
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/1.10
encapsulation dot1Q 10
ip address 172.16.1.254 255.255.255.0
ip access-group 1 out
!
interface GigabitEthernet0/1.20
encapsulation dot1Q 20
ip address 172.16.2.254 255.255.255.0
ip access-group 2 out
!
interface GigabitEthernet0/1.30
encapsulation dot1Q 30
ip address 172.16.3.254 255.255.255.0
ip access-group 3 out
!
interface GigabitEthernet0/1.40
encapsulation dot1Q 40
ip address 172.16.4.254 255.255.255.0
ip access-group 4 out
!
interface GigabitEthernet0/1.50
encapsulation dot1Q 50
ip address 172.16.5.254 255.255.255.0
ip access-group 5 out
!
interface GigabitEthernet0/1.99
encapsulation dot1Q 99
ip address 172.16.9.254 255.255.255.0
ip access-group 9 out
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
```

```
ip access-list extended sl_def_acl
deny tcp any any eq telnet
deny tcp any any eq www
deny tcp any any eq 22
permit tcp any any eq 22
access-list 1 remark Deny Marketing
access-list 1 permit 172.16.1.0 0.0.0.255
access-list 1 permit 172.16.3.0 0.0.0.255
access-list 1 permit 172.16.4.0 0.0.0.255
access-list 1 permit 172.16.5.0 0.0.0.255
access-list 1 deny any
access-list 2 remark Only Marketing
access-list 2 permit 172.16.2.0 0.0.0.255
access-list 2 permit 172.16.4.0 0.0.0.255
access-list 2 permit 172.16.5.0 0.0.0.255
access-list 3 remark Deny Marketing
access-list 3 permit 172.16.1.0 0.0.0.255
access-list 3 permit 172.16.3.0 0.0.0.255
access-list 3 permit 172.16.4.0 0.0.0.255
access-list 3 permit 172.16.5.0 0.0.0.255
access-list 4 remark Allow All
access-list 4 permit 172.16.1.0 0.0.0.255
access-list 4 permit 172.16.2.0 0.0.0.255
access-list 4 permit 172.16.3.0 0.0.0.255
access-list 4 permit 172.16.4.0 0.0.0.255
access-list 4 permit 172.16.5.0 0.0.0.255
access-list 5 remark Allow All
access-list 5 permit 172.16.1.0 0.0.0.255
access-list 5 permit 172.16.2.0 0.0.0.255
access-list 5 permit 172.16.3.0 0.0.0.255
access-list 5 permit 172.16.4.0 0.0.0.255
access-list 5 permit 172.16.5.0 0.0.0.255
access-list 9 remark Only Management
access-list 9 permit 172.16.9.0 0.0.0.255
!
banner motd ^CAuthorized Access Only!^C
!
line con 0
password 7 0817760A4B22510C5E061914227E210430
login
!
line aux 0
!
line vty 0 4
```

```
exec-timeout 3 0
password 7 0817760A4B22510C5E061914227E210430
login local
transport input ssh
line vty 5 15
exec-timeout 3 0
password 7 0817760A4B22510C5E061914227E210430
login local
transport input ssh
!
end
```

Device Name: R2

```
Current configuration : 4929 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 16
!
hostname R2
!
login block-for 300 attempts 5 within 120
!
enable secret 5 $1$mERr$S02MYM.h6rz9962O2Ext7/
!
ip dhcp relay information trust-all
!
ip dhcp excluded-address 172.16.1.0
ip dhcp excluded-address 172.16.1.254
ip dhcp excluded-address 172.16.1.255
ip dhcp excluded-address 172.16.2.0
ip dhcp excluded-address 172.16.2.254
ip dhcp excluded-address 172.16.2.255
ip dhcp excluded-address 172.16.3.0
ip dhcp excluded-address 172.16.3.254
ip dhcp excluded-address 172.16.3.255
ip dhcp excluded-address 172.16.4.0
ip dhcp excluded-address 172.16.4.254
ip dhcp excluded-address 172.16.4.255
ip dhcp excluded-address 172.16.5.0
ip dhcp excluded-address 172.16.5.254
ip dhcp excluded-address 172.16.5.255
ip dhcp excluded-address 172.16.9.0
ip dhcp excluded-address 172.16.9.10
ip dhcp excluded-address 172.16.9.11
ip dhcp excluded-address 172.16.9.12
ip dhcp excluded-address 172.16.9.20
ip dhcp excluded-address 172.16.9.30
ip dhcp excluded-address 172.16.9.40
ip dhcp excluded-address 172.16.9.50
ip dhcp excluded-address 172.16.9.254
ip dhcp excluded-address 172.16.9.255
ip dhcp excluded-address 172.16.1.1 172.16.1.127
ip dhcp excluded-address 172.16.2.1 172.16.2.127
ip dhcp excluded-address 172.16.3.1 172.16.3.127
ip dhcp excluded-address 172.16.4.1 172.16.4.127
ip dhcp excluded-address 172.16.5.1 172.16.5.127
ip dhcp excluded-address 172.16.9.1 172.16.9.127
!
ip dhcp pool DEVELOPER
network 172.16.1.0 255.255.255.0
default-router 172.16.1.254
ip dhcp pool MARKETING
network 172.16.2.0 255.255.255.0
default-router 172.16.2.254
ip dhcp pool CREATIVE
network 172.16.3.0 255.255.255.0
default-router 172.16.3.254
ip dhcp pool IT
network 172.16.4.0 255.255.255.0
default-router 172.16.4.254
ip dhcp pool SERVICES
network 172.16.5.0 255.255.255.0
default-router 172.16.5.254
ip dhcp pool MANAGEMENT
network 172.16.9.0 255.255.255.0
default-router 172.16.9.254
!
ip cef
no ipv6 cef
!
username AdminR2 privilege 15 secret 5 $1$mERr$dCLLeDqh8A2bEBqsDJIV80
```

```
!
license udi pid CISCO1941/K9 sn FTX1524270V-
!
ip ssh version 2
no ip domain-lookup
ip domain-name xcite.com
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/1.10
encapsulation dot1Q 10
ip address 172.16.1.254 255.255.255.0
ip access-group 1 out
!
interface GigabitEthernet0/1.20
encapsulation dot1Q 20
ip address 172.16.2.254 255.255.255.0
ip access-group 2 out
!
interface GigabitEthernet0/1.30
encapsulation dot1Q 30
ip address 172.16.3.254 255.255.255.0
ip access-group 3 out
!
interface GigabitEthernet0/1.40
encapsulation dot1Q 40
ip address 172.16.4.254 255.255.255.0
ip access-group 4 out
!
interface GigabitEthernet0/1.50
encapsulation dot1Q 50
ip address 172.16.5.254 255.255.255.0
ip access-group 5 out
```

```
!
interface GigabitEthernet0/1.99
encapsulation dot1Q 99
ip address 172.16.9.254 255.255.255.0
ip access-group 9 out
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
ip access-list extended sl_def_acl
deny tcp any any eq telnet
deny tcp any any eq www
deny tcp any any eq 22
permit tcp any any eq 22
access-list 1 remark Deny Marketing
access-list 1 permit 172.16.1.0 0.0.0.255
access-list 1 permit 172.16.3.0 0.0.0.255
access-list 1 permit 172.16.4.0 0.0.0.255
access-list 1 permit 172.16.5.0 0.0.0.255
access-list 1 deny any
access-list 2 remark Only Marketing
access-list 2 permit 172.16.2.0 0.0.0.255
access-list 2 permit 172.16.4.0 0.0.0.255
access-list 2 permit 172.16.5.0 0.0.0.255
access-list 3 remark Deny Marketing
access-list 3 permit 172.16.1.0 0.0.0.255
access-list 3 permit 172.16.3.0 0.0.0.255
access-list 3 permit 172.16.4.0 0.0.0.255
access-list 3 permit 172.16.5.0 0.0.0.255
access-list 4 remark Allow All
access-list 4 permit 172.16.1.0 0.0.0.255
access-list 4 permit 172.16.2.0 0.0.0.255
access-list 4 permit 172.16.3.0 0.0.0.255
access-list 4 permit 172.16.4.0 0.0.0.255
access-list 4 permit 172.16.5.0 0.0.0.255
access-list 5 remark Allow All
access-list 5 permit 172.16.1.0 0.0.0.255
access-list 5 permit 172.16.2.0 0.0.0.255
access-list 5 permit 172.16.3.0 0.0.0.255
```

```
access-list 5 permit 172.16.4.0 0.0.0.255
access-list 5 permit 172.16.5.0 0.0.0.255
access-list 9 remark Only Management
access-list 9 permit 172.16.9.0 0.0.0.255
!
banner motd ^CAuthorized Access Only!^C
!
line con 0
password 7 0817760A4B22510C5E061914227E210430
login
!
line aux 0
!
line vty 0 4
exec-timeout 3 0
password 7 0817760A4B22510C5E061914227E210430
login local
transport input ssh
line vty 5 15
exec-timeout 3 0
password 7 0817760A4B22510C5E061914227E210430
login local
transport input ssh
!
end
```

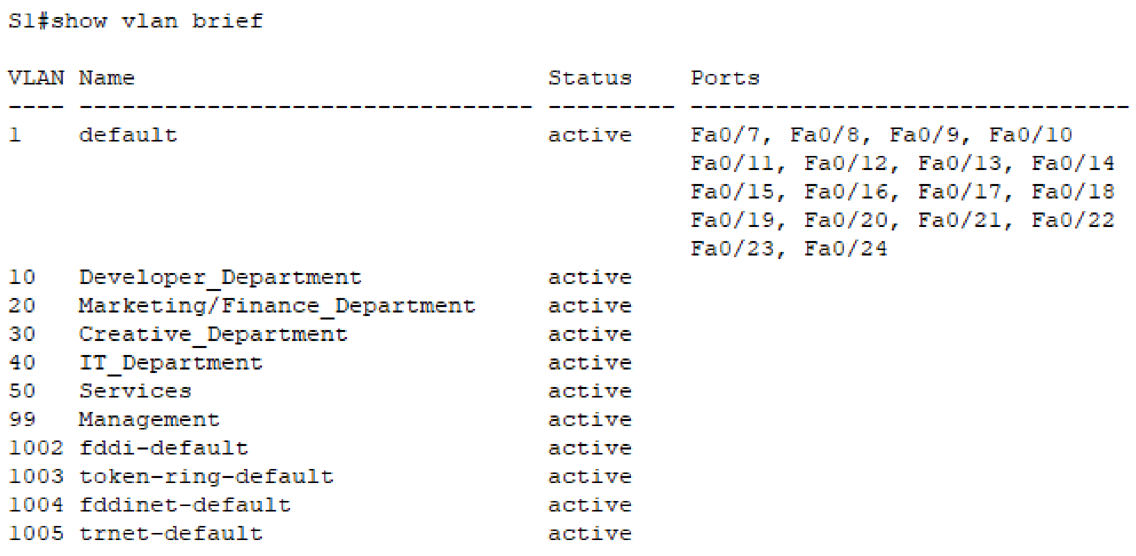
Device Name: S1

```
Current configuration : 3966 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$Vm5c/fQEXCLoYvIay41lo0
!
ip ssh version 2
no ip domain-lookup
ip domain-name xcite.com
!
username AdminS1 secret 5 $1$mERr$JdrCCEqWyv04WPRoQKGzk/
!
ip arp inspection vlan 10,20,30,40,50,99
!
ip dhcp snooping vlan 10,20,30,40,50,99
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/2
switchport trunk allowed vlan 20,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/3
switchport trunk allowed vlan 10,20,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/4
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/5
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/6
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/7
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/8
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/9
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/10
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/11
```

```
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/12
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/13
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/14
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/15
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/16
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/17
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/18
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/19
switchport access vlan 100
switchport mode access
shutdown
!
```

```
interface FastEthernet0/20
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/21
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/22
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/23
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/24
switchport access vlan 100
switchport mode access
shutdown
!
interface GigabitEthernet0/1
switchport trunk allowed vlan 10,20,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet0/2
switchport trunk allowed vlan 10,20,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface Vlan1
no ip address
shutdown
!
interface Vlan99
```

```
ip address 172.16.9.50 255.255.255.0
!
ip default-gateway 172.16.9.254
!
banner motd ^CAuthorized Access Only!^C
!
line con 0
password 7 08330912214F32352644523E2420081D7D
login
!
line vty 0 4
exec-timeout 3 0
password 7 08330912214F32352644523E2420081D7D
login local
transport input ssh
line vty 5 15
exec-timeout 3 0
password 7 08330912214F32352644523E2420081D7D
login local
transport input ssh
!
end
```



```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
10   Developer_Department             active
20   Marketing/Finance_Department     active
30   Creative_Department              active
40   IT_Department                    active
50   Services                         active
99   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Device Name: S2

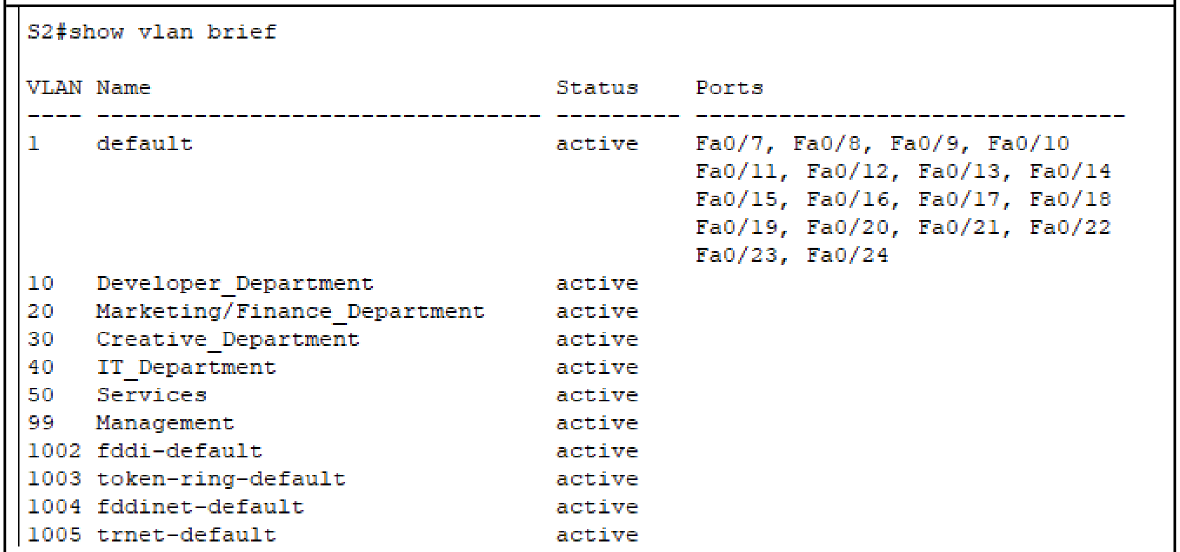
```
Current configuration : 3966 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S2
!
enable secret 5 $1$mERr$Vm5c/fQEXCLoYvIay41lo0
!
ip ssh version 2
no ip domain-lookup
ip domain-name xcite.com
!
username AdminS2 secret 5 $1$mERr$JdrCCEqWyv04WPRoQKGzk/
!
ip arp inspection vlan 10,20,30,40,50,99
!
ip dhcp snooping vlan 10,20,30,40,50,99
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/2
switchport trunk allowed vlan 20,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
```

```
interface FastEthernet0/3
switchport trunk allowed vlan 10,20,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/4
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/5
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/6
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/7
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/8
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/9
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/10
```

```
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/11
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/12
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/13
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/14
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/15
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/16
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/17
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/18
switchport access vlan 100
switchport mode access
shutdown
!
```

```
interface FastEthernet0/19
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/20
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/21
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/22
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/23
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/24
switchport access vlan 100
switchport mode access
shutdown
!
interface GigabitEthernet0/1
switchport trunk allowed vlan 10,20,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet0/2
switchport trunk allowed vlan 10,20,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
```

```
interface Vlan1
no ip address
shutdown
!
interface Vlan99
ip address 172.16.9.50 255.255.255.0
!
ip default-gateway 172.16.9.254
!
banner motd ^CAuthorized Access Only!^C
!
line con 0
password 7 08330912214F32352644523E2420081D7D
login
!
line vty 0 4
exec-timeout 3 0
password 7 08330912214F32352644523E2420081D7D
login local
transport input ssh
line vty 5 15
exec-timeout 3 0
password 7 08330912214F32352644523E2420081D7D
login local
transport input ssh
!
end
```



```
S2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
10   Developer_Department             active
20   Marketing/Finance_Department     active
30   Creative_Department              active
40   IT_Department                    active
50   Services                         active
99   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Device Name: Development_Switch1

```
Current configuration : 7087 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Development_Switch1
!
enable secret 5 $1$mERr$1Lq7DOa259aGculcw/Do50
!
ip ssh version 2
no ip domain-lookup
ip domain-name xcite.com
!
username AdminDevelopment1 secret 5 $1$mERr$OpHAf1u2qTi1w5ENcwp.C1
!
ip arp inspection vlan 10,30,40,50,99
!
ip dhcp snooping vlan 10,30,40,50,99
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 10
ip dhcp snooping limit rate 2
```

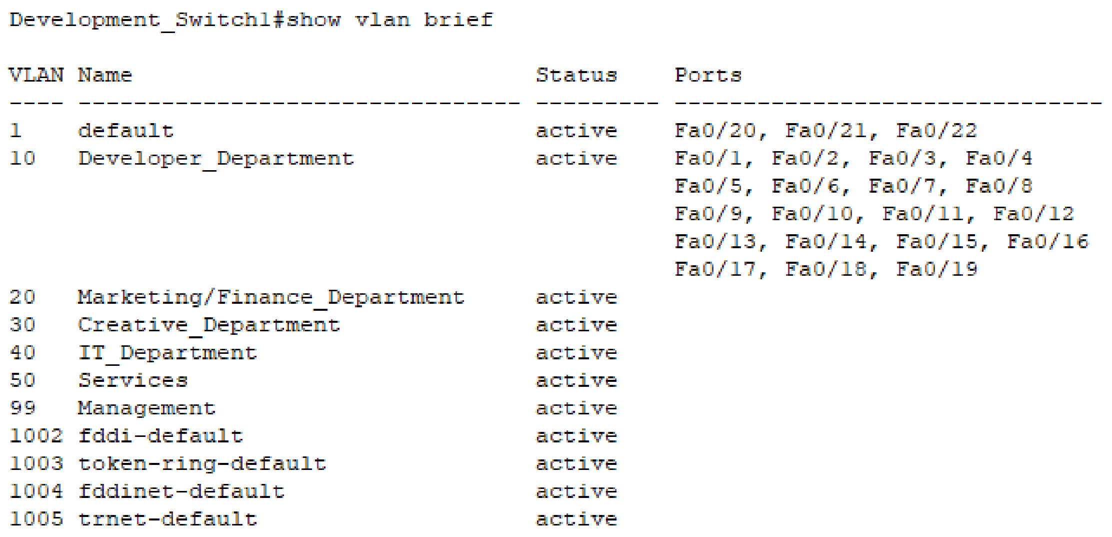
```
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0001.96AC.35BC
!
interface FastEthernet0/2
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0040.0B94.E258
!
interface FastEthernet0/3
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/4
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/5
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
```

```
interface FastEthernet0/6
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/7
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/8
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/9
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/10
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
```

```
!
interface FastEthernet0/11
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/12
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/13
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/14
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/15
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/16
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/17
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/18
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/19
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/20
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/21
```

```
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/22
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/23
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/24
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet0/1
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet0/2
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface Vlan1
no ip address
shutdown
!
interface Vlan99
ip address 172.16.9.10 255.255.255.0
!
```

```
ip default-gateway 172.16.9.254
!
banner motd ^CAuthorized Access Only!^C
!
line con 0
password 7 083B7B04504F0559483E5E5F0B2F176F16
login
!
line vty 0 4
exec-timeout 3 0
password 7 083B7B04504F0559483E5E5F0B2F176F16
login local
transport input ssh
line vty 5 15
exec-timeout 3 0
password 7 083B7B04504F0559483E5E5F0B2F176F16
login local
transport input ssh
!
end
```



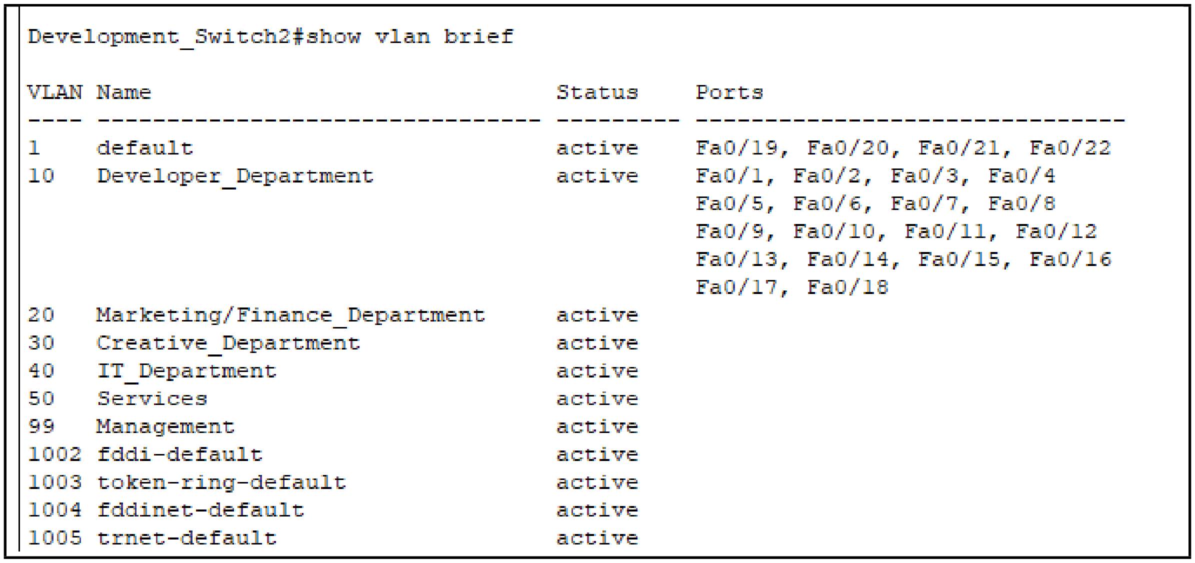
```
Development_Switch1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/20, Fa0/21, Fa0/22
10   Developer_Department             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19
20   Marketing/Finance_Department     active
30   Creative_Department              active
40   IT_Department                    active
50   Services                         active
99   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Device Name: Development_Switch2

```
Current configuration : 6913 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Development_Switch2
!
enable secret 5 $1$mERr$vSjaI31AdKpnlIq4V50FJ0
!
ip ssh version 2
no ip domain-lookup
ip domain-name xcite.com
!
username AdminDevelopment2 secret 5 $1$mERr$pwAgrlYXcHJAyKPPmr//Z0
!
ip arp inspection vlan 10,30,40,50,99
!
ip dhcp snooping vlan 10,30,40,50,99
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0001.C778.E5A8
!
interface FastEthernet0/2
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0030.F26D.2BB8
```

```
!
interface FastEthernet0/3
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/4
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/5
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/6
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/7
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/8
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/9
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/10
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/11
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/12
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/13
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/14
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/15
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/16
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/17
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/18
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/19
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/20
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/21
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/22
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/23
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/24
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
```

```
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet0/1
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet0/2
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface Vlan1
no ip address
shutdown
!
interface Vlan99
ip address 172.16.9.11 255.255.255.0
!
ip default-gateway 172.16.9.254
!
banner motd ^CAuthorized Access Only!^C
!
line con 0
password 7 08140E6524095F104B4C57561B7370331F
login
!
line vty 0 4
exec-timeout 3 0
password 7 08140E6524095F104B4C57561B7370331F
login local
transport input ssh
line vty 5 15
exec-timeout 3 0
password 7 08140E6524095F104B4C57561B7370331F
login local
transport input ssh
!
end
```



```
Development_Switch2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/19, Fa0/20, Fa0/21, Fa0/22
10   Developer_Department             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18
20   Marketing/Finance_Department     active
30   Creative_Department              active
40   IT_Department                    active
50   Services                         active
99   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

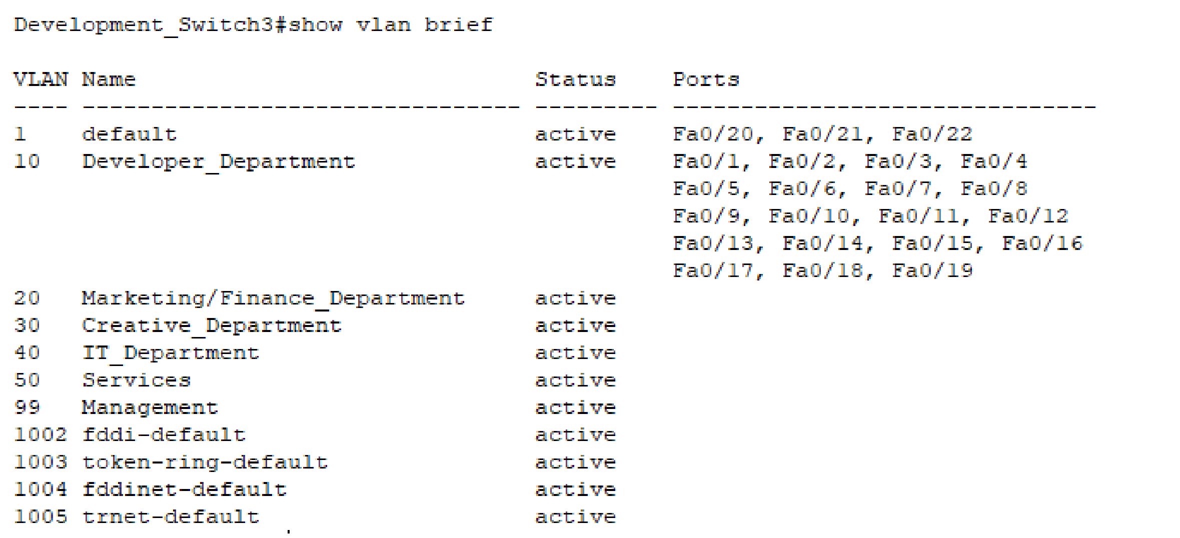
Device Name: Development_Switch3

```
Current configuration : 7087 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Development_Switch3
!
enable secret 5 $1$mERr$hNTcc2ZOodREuC.OmtAvv0
!
ip ssh version 2
no ip domain-lookup
ip domain-name xcite.com
!
username AdminDevelopment3 secret 5 $1$mERr$HNBQ8hMUtJRUfN5Y2NWsF.
!
ip arp inspection vlan 10,30,40,50,99
!
ip dhcp snooping vlan 10,30,40,50,99
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
```

```
!
interface FastEthernet0/1
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0090.0C57.97AE
!
interface FastEthernet0/2
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 000C.CF34.2434
!
interface FastEthernet0/3
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/4
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/5
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/6
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/7
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/8
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/9
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/10
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/11
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/12
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/13
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/14
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/15
switchport access vlan 10
ip dhcp snooping limit rate 2
```

```
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/16
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/17
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/18
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/19
switchport access vlan 10
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/20
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/21
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/22
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/23
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/24
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet0/1
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet0/2
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface Vlan1
no ip address
shutdown
```

```
!
interface Vlan99
ip address 172.16.9.12 255.255.255.0
!
ip default-gateway 172.16.9.254
!
banner motd ^CAuthorized Access Only!^C
!
line con 0
password 7 080D05125A0F0F100F0902352F32160665
login
!
line vty 0 4
exec-timeout 3 0
password 7 080D05125A0F0F100F0902352F32160665
login local
transport input ssh
line vty 5 15
exec-timeout 3 0
password 7 080D05125A0F0F100F0902352F32160665
login local
transport input ssh
!
end
```



```
Development_Switch3#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/20, Fa0/21, Fa0/22
10   Developer_Department             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19
20   Marketing/Finance_Department     active
30   Creative_Department              active
40   IT_Department                    active
50   Services                         active
99   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Device Name: Creative_Switch

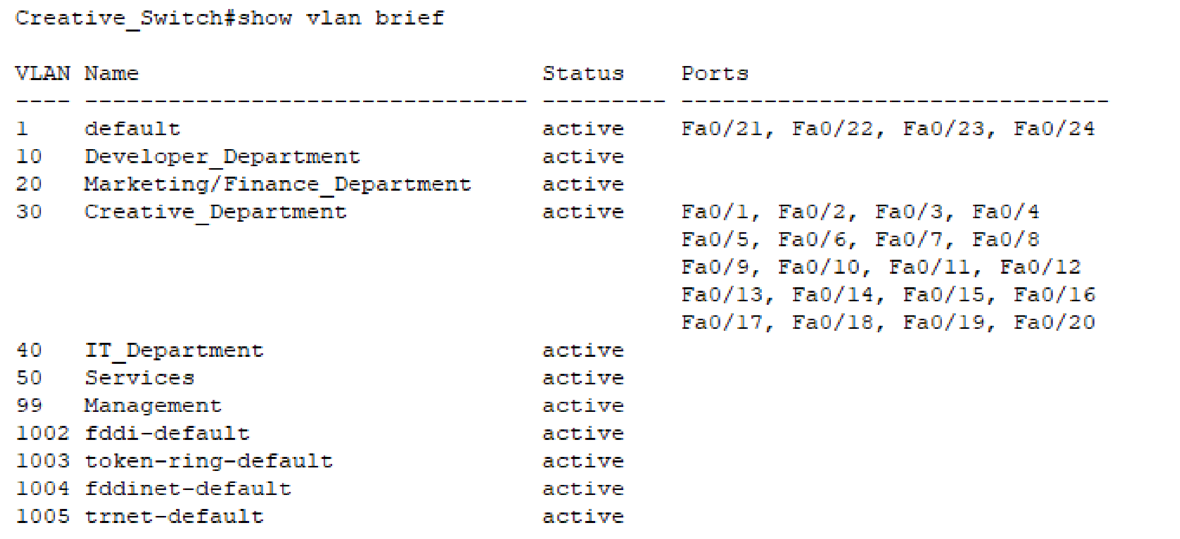
```
Current configuration : 7093 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Creative_Switch
!
enable secret 5 $1$mERr$IUMyvLM3OXQS9GJUYsSDM.
!
ip ssh version 2
no ip domain-lookup
ip domain-name xcite.com
!
username AdminCreative secret 5 $1$mERr$85zN34vFNeZKuzQt9tFKf.
!
ip arp inspection vlan 10,30,40,50,99
!
ip dhcp snooping vlan 10,30,40,50,99
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0060.2F7B.4C0A
!
interface FastEthernet0/2
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0000.0CBB.4E08
!
interface FastEthernet0/3
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/4
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/5
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/6
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/7
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/8
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/9
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/10
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/11
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/12
switchport access vlan 30
ip dhcp snooping limit rate 2
```

```
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/13
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/14
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/15
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/16
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/17
switchport access vlan 30
```

```
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/18
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/19
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/20
switchport access vlan 30
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/21
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/22
switchport access vlan 100
switchport mode access
shutdown
!
```

```
interface FastEthernet0/23
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/24
switchport access vlan 100
switchport mode access
shutdown
!
interface GigabitEthernet0/1
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet0/2
switchport trunk allowed vlan 10,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface Vlan1
no ip address
shutdown
!
interface Vlan99
ip address 172.16.9.30 255.255.255.0
!
ip default-gateway 172.16.9.254
!
banner motd ^CAuthorized Access Only!^C
!
line con 0
password 7 08184F633E28440549591F2C790039296B
login
!
line vty 0 4
exec-timeout 3 0
password 7 08184F633E28440549591F2C790039296B
login local
transport input ssh
```

```
line vty 5 15
exec-timeout 3 0
password 7 08184F633E28440549591F2C790039296B
login local
transport input ssh
!
end
```



```
Creative_Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   Developer_Department             active
20   Marketing/Finance_Department     active
30   Creative_Department              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
40   IT_Department                    active
50   Services                         active
99   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

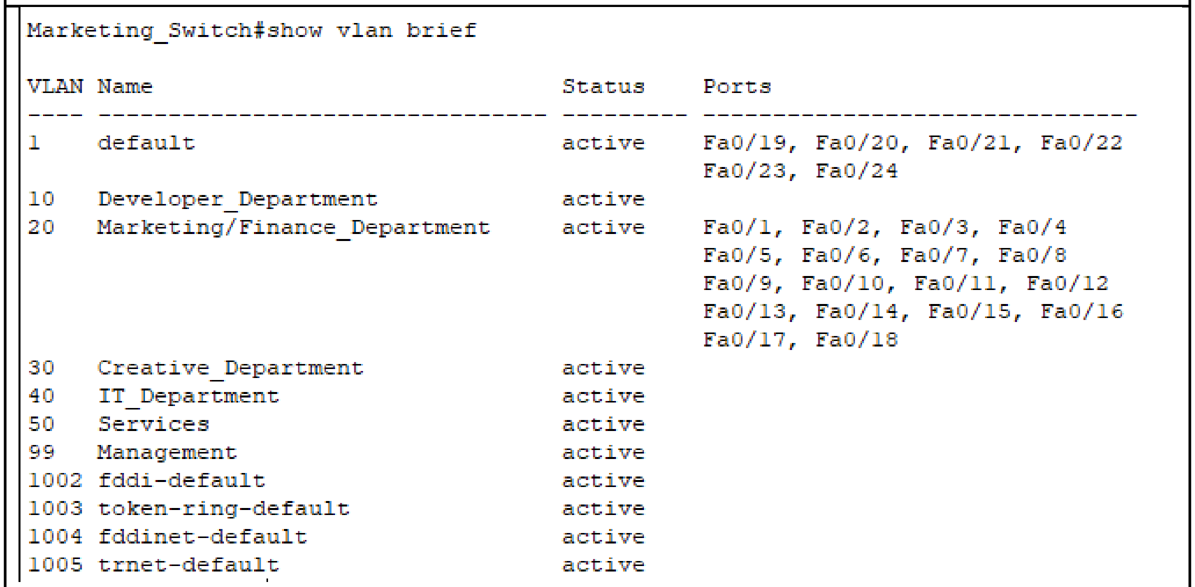
Device Name: Marketing_Switch

```
Current configuration : 6735 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Marketing_Switch
!
enable secret 5 $1$mERr$cekW/bu6/97Aq9lnrTnTd/
!
ip ssh version 2
no ip domain-lookup
ip domain-name xcite.com
!
username AdminMarketing secret 5 $1$mERr$nooLEi4eZkDZZABEsDpJb/
!
```

```
ip arp inspection vlan 20,40,50,99
!
ip dhcp snooping vlan 20,40,50,99
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 000A.F3E6.7A20
!
interface FastEthernet0/2
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0000.0CA5.516C
!
interface FastEthernet0/3
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/4
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/5
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/6
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/7
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/8
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/9
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/10
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/11
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/12
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/13
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/14
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/15
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/16
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/17
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/18
switchport access vlan 20
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/19
switchport access vlan 100
switchport mode access
shutdown
```

```
!
interface FastEthernet0/20
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/21
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/22
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/23
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/24
switchport access vlan 100
switchport mode access
shutdown
!
interface GigabitEthernet0/1
switchport trunk allowed vlan 20,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet0/2
switchport trunk allowed vlan 20,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface Vlan1
no ip address
shutdown
!
```

```
interface Vlan99
ip address 172.16.9.20 255.255.255.0
!
ip default-gateway 172.16.9.254
!
banner motd ^CAuthorized Access Only!^C
!
line con 0
password 7 0829551A4E514B4E3A49372667393E6D2D
login
!
line vty 0 4
exec-timeout 3 0
password 7 0829551A4E514B4E3A49372667393E6D2D
login local
transport input ssh
line vty 5 15
exec-timeout 3 0
password 7 0829551A4E514B4E3A49372667393E6D2D
login local
transport input ssh
!
end
```



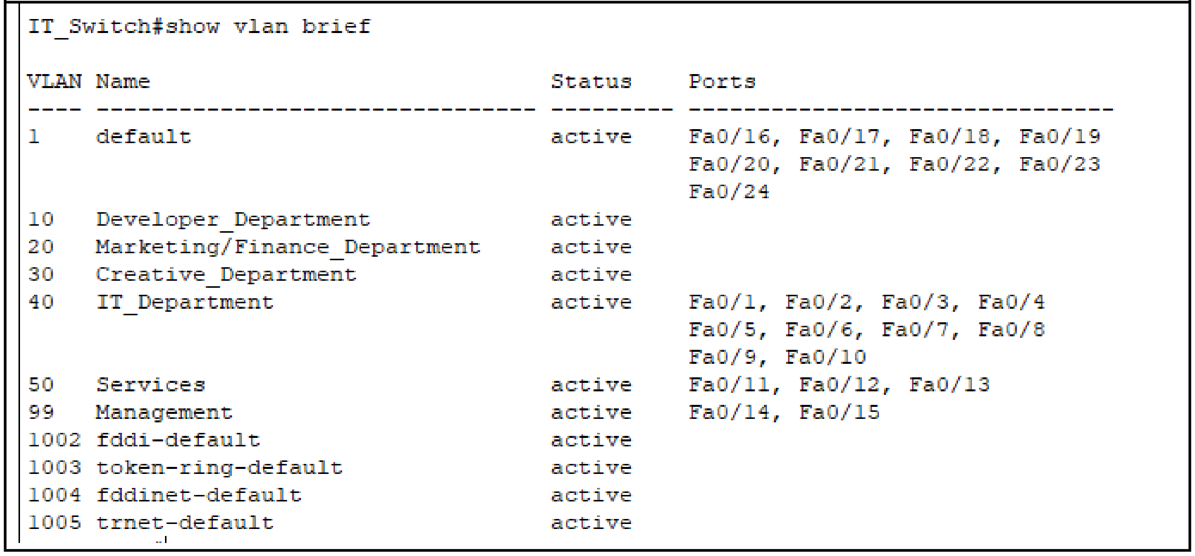
```
Marketing_Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
10   Developer_Department             active
20   Marketing/Finance_Department     active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18
30   Creative_Department              active
40   IT_Department                    active
50   Services                         active
99   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Device Name: IT_Switch

```
Current configuration : 6331 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname IT_Switch
!
enable secret 5 $1$mERr$Hv015FqqxGo5sn.VRoX2k/
!
ip ssh version 2
no ip domain-lookup
ip domain-name xcite.com
!
username AdminIT secret 5 $1$mERr$qGVQh4G8Cut0HlT3PSALl/
!
ip arp inspection vlan 10,20,30,40,50,99
!
ip dhcp snooping vlan 10,20,30,40,50,99
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 40
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0003.E43C.79C8
!
interface FastEthernet0/2
switchport access vlan 40
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0003.E4E3.34D0
```

```
!
interface FastEthernet0/3
switchport access vlan 40
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/4
switchport access vlan 40
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/5
switchport access vlan 40
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/6
switchport access vlan 40
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/7
switchport access vlan 40
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/8
switchport access vlan 40
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/9
switchport access vlan 40
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/10
switchport access vlan 40
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/11
switchport access vlan 50
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0002.4A46.3BA1
!
interface FastEthernet0/12
switchport access vlan 50
ip dhcp snooping limit rate 2
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 00D0.D3C8.1401
!
interface FastEthernet0/13
switchport access vlan 50
ip arp inspection trust
ip dhcp snooping trust
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0001.970D.D86A
!
interface FastEthernet0/14
switchport access vlan 99
ip arp inspection trust
ip dhcp snooping trust
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 00D0.5860.77C5
!
interface FastEthernet0/15
switchport access vlan 99
ip arp inspection trust
ip dhcp snooping trust
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0004.9A9C.2C26
!
interface FastEthernet0/16
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/17
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/18
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/19
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/20
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/21
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/22
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/23
switchport access vlan 100
switchport mode access
shutdown
!
interface FastEthernet0/24
switchport access vlan 100
switchport mode access
shutdown
!
interface GigabitEthernet0/1
switchport trunk allowed vlan 10,20,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet0/2
switchport trunk allowed vlan 10,20,30,40,50,99
ip arp inspection trust
ip dhcp snooping trust
```

```
switchport mode trunk
switchport nonegotiate
!
interface Vlan1
no ip address
shutdown
!
interface Vlan99
ip address 172.16.9.40 255.255.255.0
!
ip default-gateway 172.16.9.254
!
banner motd ^CAuthorized Access Only!^C
!
line con 0
password 7 08130805173B4F2724281A5C6405652360
login
!
line vty 0 4
exec-timeout 3 0
password 7 08130805173B4F2724281A5C6405652360
login local
transport input ssh
line vty 5 15
exec-timeout 3 0
password 7 08130805173B4F2724281A5C6405652360
login local
transport input ssh
!
end
```



```
IT_Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24
10   Developer_Department             active
20   Marketing/Finance_Department     active
30   Creative_Department              active
40   IT_Department                    active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10
50   Services                         active    Fa0/11, Fa0/12, Fa0/13
99   Management                       active    Fa0/14, Fa0/15
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```