**Introduction**

In an era where information is as valuable as currency, the integrity and security of a company's network architecture are paramount. Advertising Company, a progressive advertising firm, has recognized the need to enhance its current network infrastructure to protect its assets, streamline operations, and maintain competitive advantage. The company's workforce, which is the linchpin in driving customer engagement through online services, is operating on a flat network topology. This outdated setup exposes the company to significant security vulnerabilities, particularly concerning sensitive customer management data and HR, payroll, finance, and senior management information. Furthermore, the necessity for employees to manage two computers each to access disparate networks could be more efficient and counterproductive. This report proposes a comprehensive redesign of [Company Name]'s network to a more hierarchical and segmented model, addressing the outlined security concerns and operational inefficiencies while enabling secure remote access for employees.

**Proposed Solution**

The crux of the proposed solution involves transitioning from a flat network to a segmented network topology using Virtual Local Area Networks (VLANs). VLANs create logical separations within the physical network, effectively compartmentalizing different business functions, enhancing security through isolation, and reducing unnecessary traffic.

The proposed network comprises two primary VLANs — one dedicated to Sales and Marketing and the other encompassing Customer Management, HR, Payroll, Finance, and Senior Management. These VLANs will be implemented on a Multi-Layer Switch (MLS) that serves as the Core of our network, enabling efficient inter-VLAN routing and leveraging the Spanning Tree Protocol (STP) to prevent network loops and broadcast storms.

**Critical Components of the Proposed Network Architecture:**

1. **MLS (Core Layer)**: Acts as the central hub for all VLANs, configured with Layer 3 capabilities for inter-VLAN routing and VLAN Trunking Protocol (VTP) to manage VLAN databases across the network.
2. **Distribution Switches**: As intermediaries between the MLS and access switches, forwarding data based on Layer 2 information.
3. **Access Switches**: Connect end-user devices to the network. Each employee will have one computer connected to an access switch, with port assignments corresponding to the appropriate VLAN.
4. **Firewall and Router**: Form the gateway between the internal network and the Internet. The firewall will be configured with strict access control lists (ACLs) to regulate traffic flow. At the same time, the router will facilitate external connections, implementing Network Address Translation (NAT) for internet access and Virtual Private Network (VPN) capabilities for remote employees.
5. **Remote Access**: VPNs will enable secure, encrypted connections for employees working remotely, ensuring they can access their emails and files safely.
6. **Security Protocols**: Implement robust password policies, SSH for secure management, and port security on access switches. The firewall will be configured to restrict access to sensitive resources and to monitor for malicious traffic.

This solution is aimed at fortifying the network's defenses and enhancing overall productivity by allowing a seamless and secure workflow for the employees, both on-premises and remotely.

**VLAN Table**

The VLAN table identifies each VLAN's purpose, corresponding to a particular department within the company:

|  |  |  |
| --- | --- | --- |
| **VLAN ID** | **VLAN Name** | **Department** |
| 10 | SalesMarketing | Sales & Marketing |
| 20 | CustomerMgmt | Customer Management |
| 30 | HRFinance | HR, Payroll & Finance |
| 40 | SeniorMgmt | Senior Management |
| 50 | IT | IT & Network AdminIP Addressing Scheme |

The IP addressing scheme is structured to allocate a unique subnet for each VLAN:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **VLAN ID** | **Subnet** | **Subnet Mask** | **Default Gateway** | **DHCP Range** | **Reserved Range** |
| 10 | 192.168.10.0/24 | 255.255.255.0 | 192.168.10.1 | 192.168.10.50 - 192.168.10.200 | 192.168.10.2 - 192.168.10.49 |
| 20 | 192.168.20.0/24 | 255.255.255.0 | 192.168.20.1 | 192.168.20.50 - 192.168.20.200 | 192.168.20.2 - 192.168.20.49 |
| 30 | 192.168.30.0/24 | 255.255.255.0 | 192.168.30.1 | 192.168.30.50 - 192.168.30.200 | 192.168.30.2 - 192.168.30.49 |
| 40 | 192.168.40.0/24 | 255.255.255.0 | 192.168.40.1 | 192.168.40.50 - 192.168.40.200 | 192.168.40.2 - 192.168.40.49 |
| 50 | 192.168.50.0/24 | 255.255.255.0 | 192.168.50.1 | 192.168.50.50 - 192.168.50.200 | 192.168.50.2 - 192.168.50.49 |

**Detailed Configurations**

VLAN Configuration on Multi-Layer Switch (MLS)

|  |
| --- |
| enable  configure terminal  vtp mode server  vtp domain ad-company  vtp password securepass  VLAN 10  name SalesMarketing  VLAN 20  name CustomerMgmt  VLAN 30  name HRFinance  VLAN 40  name SeniorMgmt  VLAN 50  name IT  exit |

**Inter-VLAN Routing Configuration on MLS**

|  |
| --- |
| interface Vlan10  IP address 192.168.10.1 255.255.255.0  no shutdown  interface Vlan20  IP address 192.168.20.1 255.255.255.0  no shutdown  interface Vlan30  IP address 192.168.30.1 255.255.255.0  no shutdown  interface Vlan40  IP address 192.168.40.1 255.255.255.0  no shutdown  interface Vlan50  IP address 192.168.50.1 255.255.255.0  no shutdown |

**DHCP Configuration for VLANs on MLS**

|  |
| --- |
| ip dhcp excluded-address 192.168.10.1 192.168.10.49  ip dhcp excluded-address 192.168.20.1 192.168.20.49  ip dhcp excluded-address 192.168.30.1 192.168.30.49  ip dhcp excluded-address 192.168.40.1 192.168.40.49  ip dhcp excluded-address 192.168.50.1 192.168.50.49  ip dhcp pool SalesMarketing  network 192.168.10.0 255.255.255.0  default-router 192.168.10.1  DNS-server 192.168.50.100  ip dhcp pool CustomerMgmt  network 192.168.20.0 255.255.255.0  default-router 192.168.20.1  DNS-server 192.168.50.100  ip dhcp pool HRFinance  network 192.168.30.0 255.255.255.0  default-router 192.168.30.1  DNS-server 192.168.50.100  ip dhcp pool SeniorMgmt  network 192.168.40.0 255.255.255.0  default-router 192.168.40.1  DNS-server 192.168.50.100  ip dhcp pool IT  network 192.168.50.0 255.255.255.0  default-router 192.168.50.1  DNS-server 192.168.50.100 |

**Security Configurations**

|  |
| --- |
| username admin secret admin123  enable secret class  line console 0  password cisco  login  line vty 0 15  password cisco  login local  transport input ssh  service password-encryption  crypto key generates rsa modulus 2048  no ip http server  no ip http secure-server |

**Spanning Tree and Trunk Configuration**

|  |
| --- |
| spanning-tree mode rapid-pvst  interface range fa0/1 - 4  switch port mode trunk  switch port trunk allowed vlan 10,20,30,40,50 |

The configurations above provide the foundational setup for VLANs, DHCP, routing, and security on the network's MLS. The configurations for access switches, routing protocols, and remote access VPN would follow similar patterns, adjusted for their specific roles within the network.

This part of the report should include additional explanations for each configuration command, the reasoning behind each protocol and security measure chosen, and the expected outcomes from implementing these configurations.

**Network Hierarchy and Redundancy**

**Network Hierarchy**

The network architecture for **the Advertising Company** has been meticulously designed to align with the hierarchical network model, providing scalability, manageability, and predictability. This model is structured into three distinct layers:

1. **Core Layer**: The network's backbone, responsible for fast and reliable transportation of large amounts of data. The Multi-Layer Switch (MLS) at this layer handles high-speed routing, quality of service (QoS), and inter-VLAN routing, ensuring that data packets reach their destination swiftly and efficiently.
2. **Distribution Layer**: This layer aggregates data from the Access Layer before transmitting it to the Core Layer. The Distribution Switches in this layer enforce policies, segment traffic, and perform routing between VLANs. They serve as intermediaries, controlling network traffic flow between the subnets and the core network.
3. **Access Layer**: The final layer where end devices, such as workstations, laptops, and printers, connect to the network. Access Switches at this layer provide ports to which the devices directly connect. They offer port security and VLAN assignment, enabling fine-grained control over the users and devices that can access the network.

**Redundancy and Trunking**

Redundancy is a crucial aspect of our network design, ensuring continuous availability of the network services even in the event of hardware failure or link disruption. The following measures have been implemented:

1. **Link Redundancy**: To ensure continuous connectivity, redundant links between the MLS and Distribution Switches have been provided. These links are configured with Spanning Tree Protocol (STP) to prevent loops and provide automatic backup paths if an active link fails.
2. **Trunk Redundancy**: All links between the switches are configured as trunks to carry traffic for multiple VLANs. The trunk links between the Core and Distribution layers are crucial as they have the VLAN information and ensure the proper distribution of traffic across the network. Redundant trunks are provided to maintain connectivity in case one of the trunk links goes down.
3. **STP Configuration**: STP has been configured to prevent loops that can occur with redundant links. It ensures a single active path between two network devices while blocking redundant paths until needed. The MLS is configured as the root bridge for all VLANs to control the flow of STP and ensure optimal path selection in the network topology.
4. **Switch Redundancy**: Each distribution area has multiple switches configured in a stacked or clustered setup. This configuration provides high availability and load balancing and simplifies management since the stacked switches behave as a single logical switch.

**Network Topology**

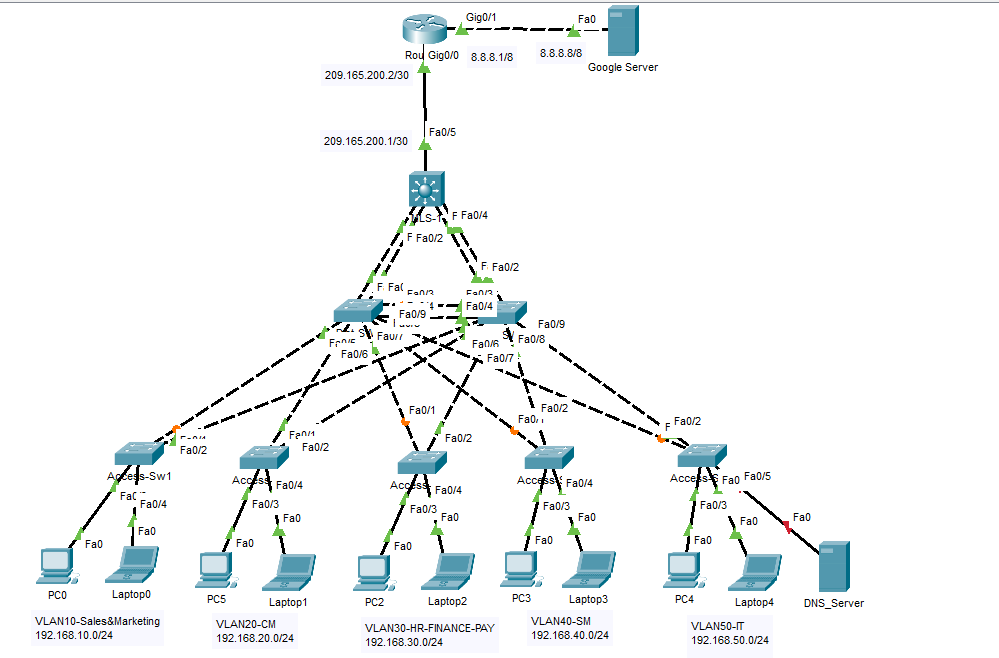


Fig 1: Network Topology

**Network Topology Descriptions**

**Overview**

The network topology of an advertising Company is a structured layout designed to optimize the company's communications and data handling performance, management, and security. The topology is architected to facilitate the distinct operational needs of various departments while ensuring robust data protection and seamless connectivity.

**Core Layer**

At the heart of the network lies the Core Layer, the central point of the topology. The Multi-Layer Switch (MLS) operating within this layer is pivotal for maintaining high-speed connectivity and handling data routing across the entire network. It is the aggregation point for all the VLANs and is responsible for swift inter-VLAN routing facilitated by advanced Layer 3 switching capabilities.

**Distribution Layer**

The Distribution Switches branchbranch out from the Core, which serves as a control center for network traffic flowing to and from the Access Layer. These switches act as gatekeepers, effectively implementing access policies and routing decisions to direct traffic. They provide connectivity to the Access Layer switches. They are also the focal points for VLAN traffic management and redundancy, ensuring the network can withstand and adapt to potential failures.

**Access Layer**

The Access Layer is where end-user devices are connected to the network. Each department's devices are linked to their respective Access Switch, which enforces security policies at the port level through features such as port security and ensures the correct VLAN assignment for each device. The Access Switches are directly connected to the Distribution Switches, which relate to the Core MLS.

**Redundancy and Trunk Links**

The network features redundant trunk links between the Core and Distribution Switches to ensure reliability. These trunks carry multiple VLANs, allowing for a diversified traffic flow across the network. The Spanning Tree Protocol (STP) is implemented to manage these trunks intelligently, ensuring no loops within the network and that backup paths are readily available if a primary link fails.

**Interconnectivity**

The network's topology is designed to maintain interconnectivity between all devices across the enterprise. The MLS facilitates communication across VLANs with Layer 3 routing while connecting to the external router leading to the Internet. The router is safeguarded by a robust firewall that monitors and controls ingress and egress traffic, shielding the internal network from external threats.

**Security Measures**

The topology incorporates extensive security measures. The firewall at the network's perimeter employs Access Control Lists (ACLs) to filter traffic, VPN services provide secure remote access, and the internal VLAN structure segregates sensitive departmental data. Intrusion Prevention Systems (IPS) are strategically placed to detect and prevent malicious activity.

**Project Conclusion**

The undertaking of this network redesign project has been a comprehensive exercise in enhancing the operational capabilities of the Advertising Company through a thorough overhaul of its existing network infrastructure. The project's primary goal was to establish a robust security architecture that protects sensitive company data, streamlines the workflow, and improves overall network performance.

Introducing a hierarchical network design has addressed the fundamental issues inherent in the previous flat network structure. By segmenting the network into distinct VLANs, we have achieved a level of compartmentalization that significantly bolsters security measures. Each VLAN is tailored to the specific needs of different departments, ensuring that sensitive information is segregated and that network traffic is efficiently managed.

The implementation of redundancy at multiple levels of the network topology ensures high availability and resilience. This is critical for maintaining business continuity, a non-negotiable requirement in today's fast-paced and always-online business environments. The redundancy features, including the Spanning Tree Protocol and trunk link duplication, are carefully planned to provide failover capabilities without compromising network performance.

Moreover, the deployment of robust firewall configurations and the introduction of VPN services have fortified the network's defenses against external threats. It has also facilitated secure remote access, a necessity for modern businesses that increasingly rely on remote and flexible working arrangements.

Throughout the project, we have adhered to industry best practices and the latest standards in network security. The configurations and protocols selected have been scrutinized for their reliability and effectiveness. The result is a network that not only meets the current demands of the advertising Company but also provides the scalability to support future growth and technological integration.

In conclusion, this project has successfully delivered a secure, efficient, and scalable network infrastructure that aligns with the strategic objectives of [Company Name]. The network is now well-equipped to handle the various challenges of modern digital business operations, from ensuring data security to enabling a mobile workforce. As advertising companies continue to evolve and expand, the foundation laid by this project will serve as a cornerstone for their continued success and resilience in the face of an ever-changing cyber landscape.

The success of this project should be evaluated not just by the sophistication of the technologies implemented but by the tangible benefits it delivers to the company's day-to-day operations and the enhanced security posture that protects the company's most valuable digital assets.