Simulating Cyber Threats for Resilience and Analysis of Network Security in Earthlink Service Provider

Table of Contents

List of Figures

List of Tables

Introduction

Leading telecom provider EarthLink Service Provider offers its wide range of customers comprehensive connectivity solutions. In this case, EarthLink Service Provider is managing the opportunities and difficulties of developing its service portfolio to satisfy the escalating needs of the digital age. EarthLink Service Provider, a prominent telecommunications company, operates with a strategic presence in two main branches: London and California, with the head office located in California. It has around 1500 – 2000 employees. EarthLink Service Provider is currently dealing with a serious cybersecurity issue. Valuable data has been lost, and this has led to a loss of trust from clients. The company, well-known in the telecommunications industry with branches in London and California, is now navigating the aftermath of a cyber-attack that has left its network vulnerable and compromised.

Potential risks are shown by the existing infrastructure, such as a weak network design that is vulnerable to cyberattacks. EarthLink highlights weaknesses that need to be improved, including the lack of zone segmentation, compromised firewall health, and absence of redundancy techniques. The system also uses a single GRE tunnel without IPsec encryption, operates access points without a Wireless LAN Controller (WLC), depends on a single-layer OSPF setup, and lacks multilayer switches, among other critical components.

To overcome this challenge, EarthLink must encourage advanced cybersecurity technologies. This involves remediating the impact of the breach and fortifying the network against future attacks. The approach includes implementing advanced intrusion detection systems, encryption protocols, and conducting comprehensive security audits to identify vulnerabilities.

The research that follows will concentrate on specific methods to strengthen security, add redundancy, and put resilient technology in place to protect against cyberattacks while maintaining the data integrity and trust which are essential to EarthLink's operations.

Proposed Solution

I’m implementing a hierarchical LAN design model with a three-tier architecture in this project. An organizational structure known as a hierarchical LAN (Local Area Network) design model divides network components into distinct layers or tiers, each of which has a specific purpose. This design technique improves the scalability, manageability, and efficiency of the network.

A fully meshed, flat network with every node connected is not necessary with a hierarchical LAN design. Changes to the network typically impact a high number of systems in fully meshed network topologies. By limiting network changes to a subset of the network, which impacts fewer systems, simplifies management, and boosts resilience, hierarchical architecture offers fault containment. Because network components in a modular layer architecture can be added or removed from service with little or no impact to the network as a whole, troubleshooting, problem isolation, and network management are made easier (franklin, 2 Aug, 2022).

Hierarchical LAN design consists of three layers:

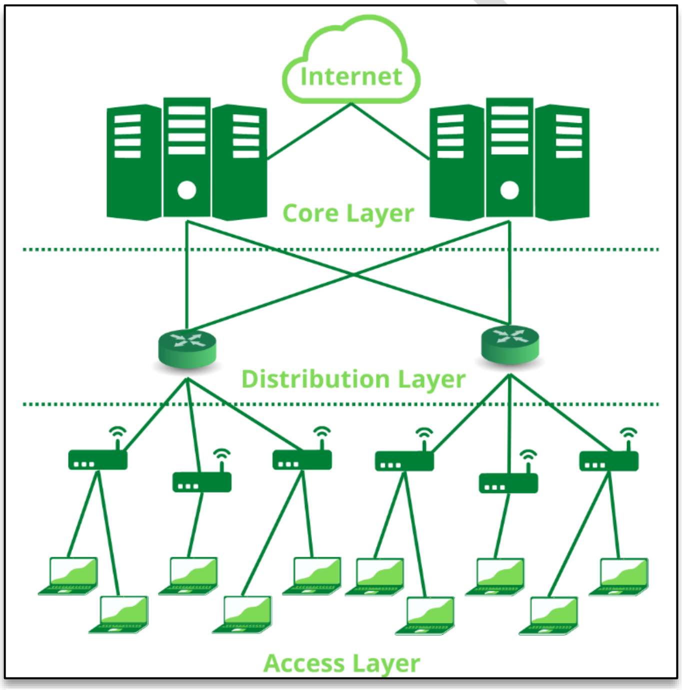
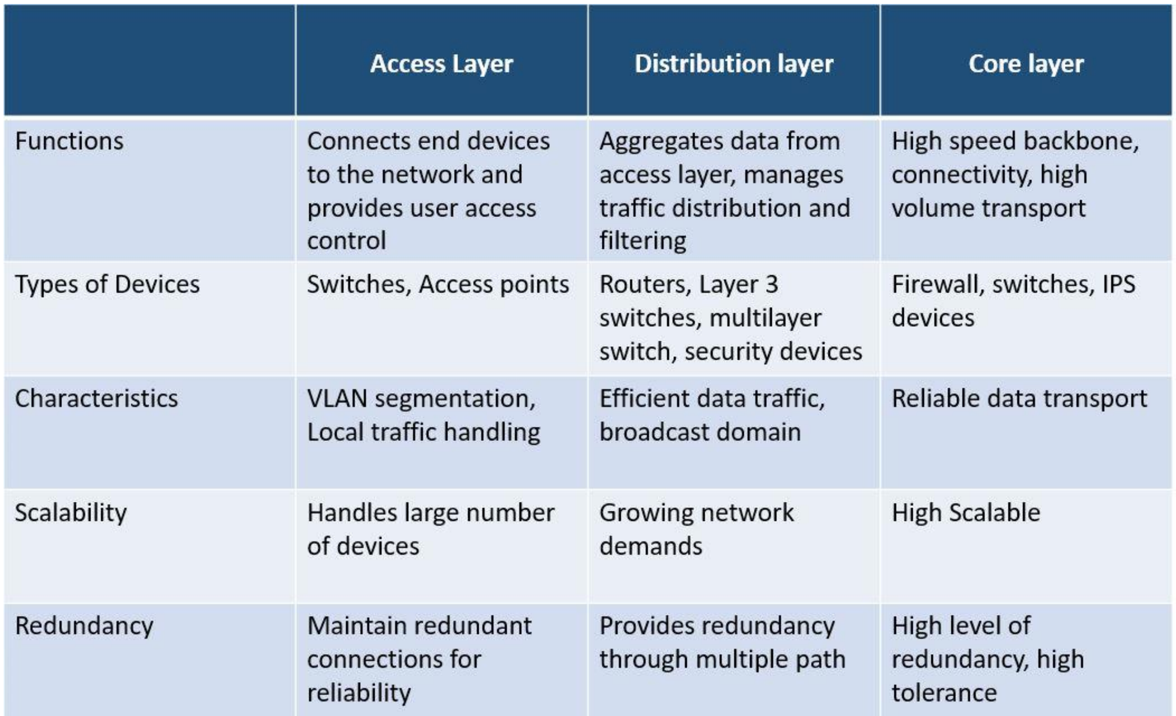


Figure 1 Hierarchical LAN Design

1. Access layer - Allows users and endpoints to access the network directly.
2. Distribution layer - Serves as a services and control boundary between the access layer and the core layer, acting as an aggregation point for the access layer.
3. Core layer – Establishes connections between distribution layers for wide environments.



	Access Layer	Distribution layer	Core layer
Functions	Connects end devices to the network and provides user access control	Aggregates data from access layer, manages traffic distribution and filtering	High speed backbone, connectivity, high volume transport
Types of Devices	Switches, Access points	Routers, Layer 3 switches, multilayer switch, security devices	Firewall, switches, IPS devices
Characteristics	VLAN segmentation, Local traffic handling	Efficient data traffic, broadcast domain	Reliable data transport
Scalability	Handles large number of devices	Growing network demands	High Scalable
Redundancy	Maintain redundant connections for reliability	Provides redundancy through multiple path	High level of redundancy, high tolerance

Figure 2 Layers with Functions and charecteristics

Enterprise network Architecture options:

- Two tier architecture
- Three tier architecture
- Layer 2 access layer (STP based)
- Layer 3 access layer (routed based)
- Simplified campus design
- Software defined access (SD access)

The Three-tier Architecture is used to implement the network in this company (Earthlink service provider). In order to maximize network performance and effectively manage traffic, this particular architectural design incorporates three separate layers. Such as access layer, distribution layer, and core layer. Each of these layers has a specialized purpose.

Three tier Architecture

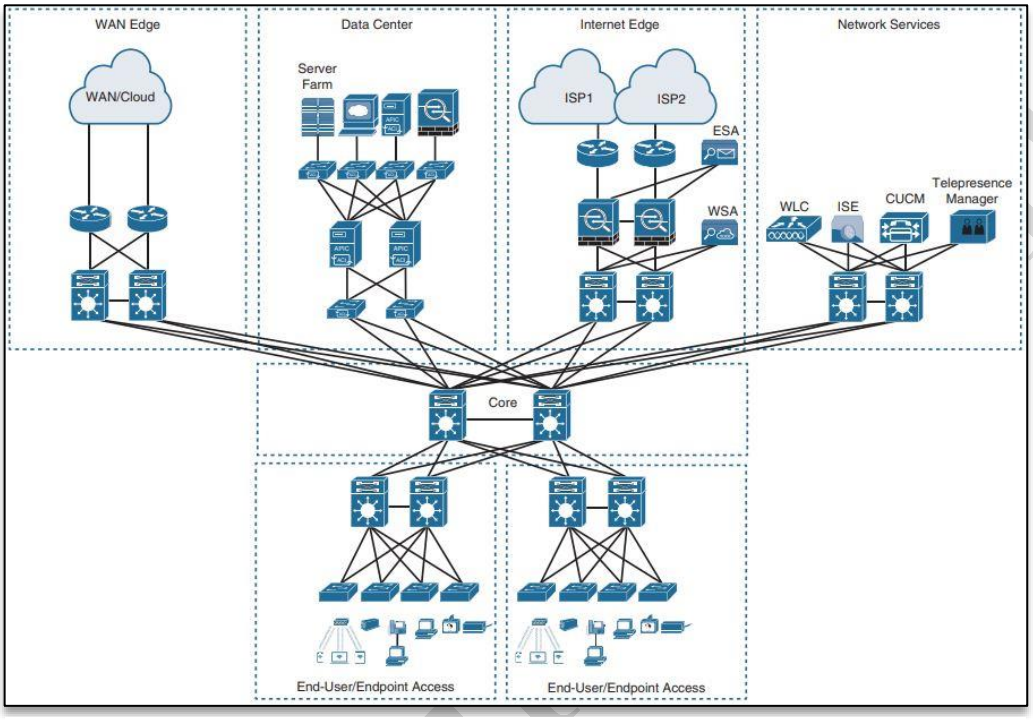


Figure 3 Three tier architecture

Three tier design divides distribution and core layers and are recommended when more than two pairs of distribution switches are needed.

The three-tier architecture improves network scalability, efficiency, and redundancy through the segregation of distinct functions into specialized layers. This approach guarantees a resilient and well-structured network infrastructure in this Earthlink service provider, and fostering enhanced performance and adaptability.

Implementing a three-tier architecture in EarthLink service provider offers several advantages. Firstly, it enhances scalability by organizing network functions into dedicated layers, allowing for easy expansion and adaptation to growing service demands.

In order to maximize network performance, the distribution layer also effectively handles traffic by gathering and filtering data. As a result, there is an increase in efficiency and enhanced data flow throughout the infrastructure of the service provider. Furthermore, an amount of redundancy is provided by the segmentation of functions, improving network resilience and reducing the chance of disruptions.

In conclusion, EarthLink's three-tier architecture supports scalability, efficiency, and reliability all essential elements of providing users with trustworthy, high-quality services.

Design

Physical and logical network diagrams are designed based on studies of the existing network infrastructure and user requirements. The physical topology of the new network infrastructure for the organization is shown in the below figure.

Earthlink Service Provider’s Network Design

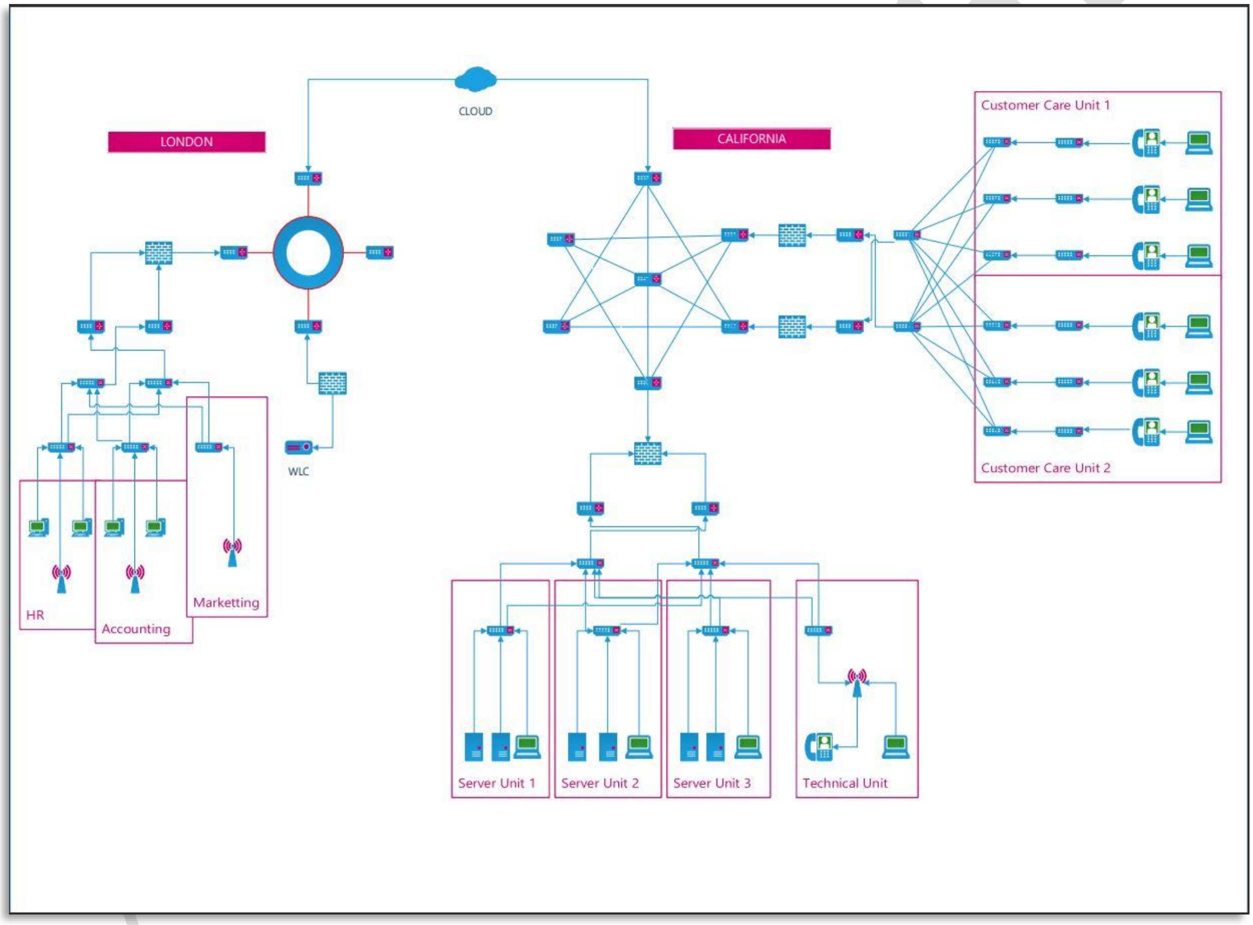


Figure 4 Earthlink Service Provider's Network Diagram

Earthlink Service Provider’s Network Topology

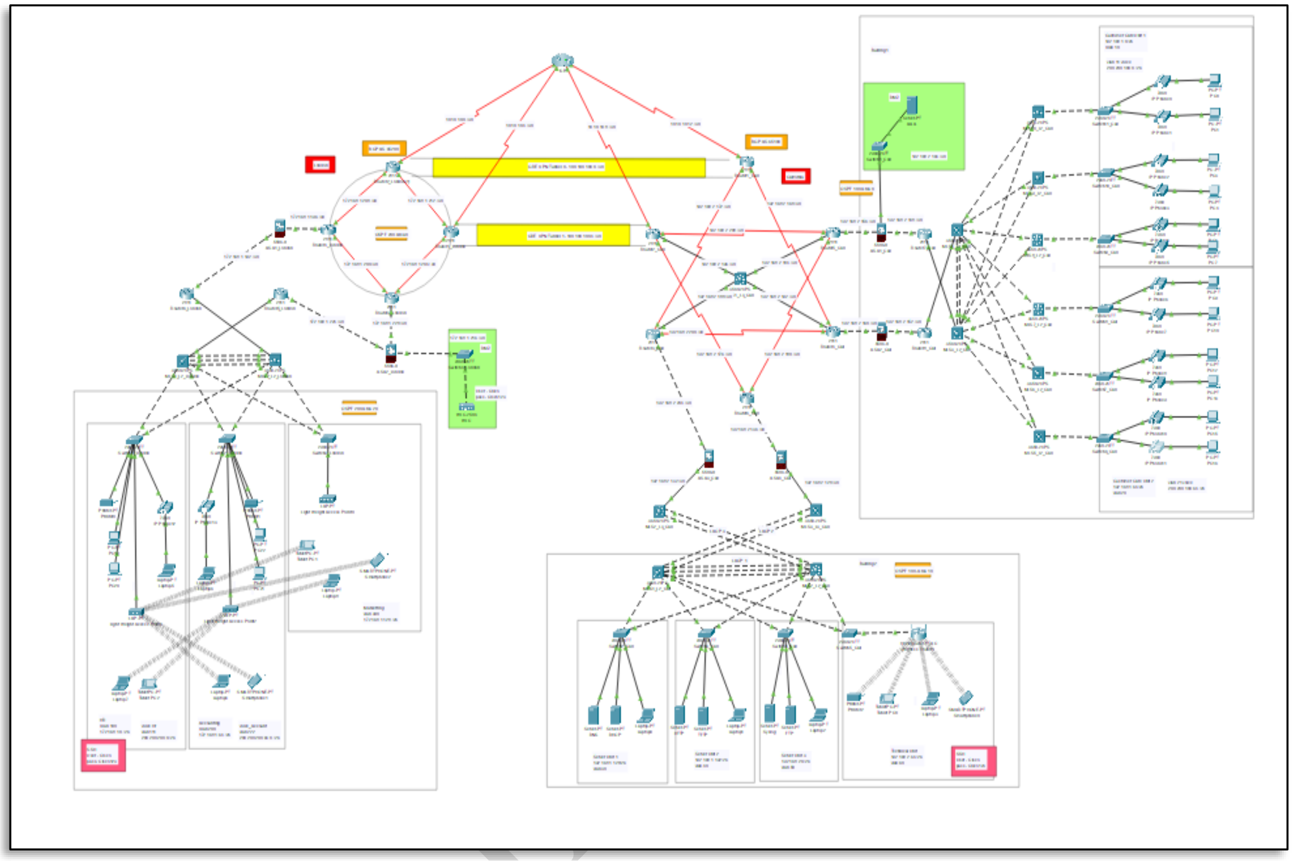


Figure 5 Earthlink service provider's Network Topology

IP Table

Table 1 IP Allocations

Departments	Network IP	1st IP	2nd IP	Broadcast IP
London Branch				
HR	172.168.1.0 /26	172.168.1.2	172.168.1.62	172.168.1.63
Accounting	172.168.1.64 /26	172.168.1.65	172.168.1.126	172.168.1.127
Marketing	172.168.1.128 /26	172.168.1.129	172.168.1.190	172.168.1.191
Serial_01	172.168.1.192/30	172.168.1.193	172.168.1.194	172.168.1.195
Serial_02	172.168.1.196/30	172.168.1.197	172.168.1.198	172.168.1.199
Serial_03	172.168.1.200/30	172.168.1.201	172.168.1.202	172.168.1.203
Serial_04	172.168.1.204/30	172.168.1.205	172.168.1.206	172.168.1.207
Serial_05	172.168.1.208/30	172.168.1.209	172.168.1.210	172.168.1.211
Serial_06	172.168.1.212/30	172.168.1.213	172.168.1.214	172.168.1.215
DMZ	172.168.1.216/30	172.168.1.217	172.168.1.218	172.168.1.219
Serial_08	172.168.1.220/30	172.168.1.221	172.168.1.222	172.168.1.223
Serial_08	172.168.1.224/30	172.168.1.225	172.168.1.226	172.168.1.227
Serial_09	172.168.1.228/30	172.168.1.229	172.168.1.230	172.168.1.231
Voice-HR	200.200.200.0/26	200.200.200.1	200.200.200.62	200.200.200.63
Voice Accounting	200.200.200.64/26	200.200.200.65	200.200.200.126	200.200.200.127
Califonia_Branch_Bulding_01				
Custom_Care_U_1	192.168.1.0/26	192.168.1.1	192.168.1.62	192.168.1.63
Custom_Care_U_2	192.168.1.64/26	192.168.1.65	192.168.1.126	192.168.1.127
Vlan_11_Voice	200.200.100.0/26	200.200.100.1	200.200.100.62	200.200.100.63
Vlan_21_Voice	200.200.100.64/26	200.200.100.65	200.200.100.126	200.200.100.127
Califonia_Branch_Bulding_02				
Server_U_1	192.168.1.128/26	192.168.1.129	192.168.1.190	192.168.1.191
Server_U_2	192.168.1.192/26	192.168.1.193	192.168.1.254	192.168.1.255

Server_U_3	192.168.2.0/26	192.168.2.1	192.168.2.62	192.168.2.63
Tech-Unit	192.168.2.64/26	192.168.2.65	192.168.2.126	192.168.2.127
Serial_01	192.168.2.128/30	192.168.2.129	192.168.2.130	192.168.2.131
Serial_02	192.168.2.132/30	192.168.2.133	192.168.2.134	192.168.2.135
Serial_03	192.168.2.136/30	192.168.2.137	192.168.2.138	192.168.2.139
Serial_04	192.168.2.140/30	192.168.2.141	192.168.2.142	192.168.2.143
Serial_05	192.168.2.144/30	192.168.2.145	192.168.2.146	192.168.2.147
Serial_06	192.168.2.148/30	192.168.2.149	192.168.2.150	192.168.2.151
Serial_07	192.168.2.152/30	192.168.2.153	192.168.2.154	192.168.2.155
Serial_08	192.168.2.156/30	192.168.2.157	192.168.2.158	192.168.2.159
Serial_09	192.168.2.160/30	192.168.2.161	192.168.2.162	192.168.2.163
DMZ	192.168.2.164/30	192.168.2.165	192.168.2.166	192.168.2.167
Serial_11	192.168.2.168/30	192.168.2.169	192.168.2.170	192.168.2.171
Serial_12	192.168.2.172/30	192.168.2.173	192.168.2.174	192.168.2.175
Serial_13	192.168.2.176/30	192.168.2.177	192.168.2.178	192.168.2.179
Serial_14	192.168.2.180/30	192.168.2.181	192.168.2.182	192.168.2.183
Serial_15	192.168.2.184/30	192.168.2.158	192.168.2.186	192.168.2.187
Serial_16	192.168.2.188/30	192.168.2.189	192.168.2.190	192.168.2.191
Serial_17	192.168.2.192/30	192.168.2.193	192.168.2.194	192.168.2.195
Serial_18	192.168.2.196/30	192.168.2.197	192.168.2.198	192.168.2.199
Serial_19	192.168.2.200/30	192.168.2.201	192.168.2.202	192.168.2.203
Serial_20	192.168.2.204/30	192.168.2.205	192.168.2.206	192.168.2.207
Serial_21	192.168.2.208/30	192.168.2.209	192.168.2.210	192.168.2.211

Design Techniques

Below table describes the design technologies used in Earthlink Service Provider network infrastructure, their purposes, and the advantages that associated with each.

Table 2 Design Techniques

Design Techniques	Purpose	Advantages
VPN	Securely connect remote users or branch offices to the network	Ensure secure and encrypted communication over the internet and facilitates remote access without compromising data privacy.
Firewall	Control and monitor incoming and outgoing network traffic	Enhances network security by preventing unauthorized access and monitors and filters traffic to protect against potential threats.
Port security	Restrict access to network devices based on MAC addresses	Prevents unauthorized devices from connecting to the network and enhances physical network security by controlling access to specific switch ports.
SSH	Secure remote access and command-line interfaces	Provides encrypted and secure access to network devices and mitigates security risks associated with plaintext protocols like telnet.

Access list	Control traffic flow based on defined rules	Enables fine grained control over network traffic and enhances security by restricting or permitting specific types of communication
WLAN	Wireless local area network for wireless connectivity	Enables flexible and mobile access to the network and facilitates the implementation of wireless devices and supports mobility within the network
VLAN	Logical segmentation of a network for improved management	Enhances network scalability and flexibility by logically grouping devices and improves security by isolating traffic within specific VLANs
Servers (AAA, HTTP, DNS, DHCP, Syslog, NTP, FTP)	Provide various network services	AAA- Authentication, Authorization and Accounting for secure access. DNS- Resolves domain names to IP addresses. DHCP – Automates IP address allocation. NTP – Synchronizes time across the network. FTP – Facilitates file transfer. Syslog – Logs network events for monitoring and troubleshooting. HTTP – supports web services and applications.

BGP	Exterior gateway protocol for routing between autonomous systems	Provides scalable and flexible routing in large networks and facilitates communication between different autonomous systems.
OSPF	Interior gateway protocol for dynamic routing within autonomous system	Enables efficient and dynamic routing within the network and adapts to changes network topology, ensuring optimal routing paths.
Etherchannel	Bundling multiple physical links to increase bandwidth	Enhances network performance by aggregating bandwidth and provides load balancing and fault tolerance for improved reliability
VTP	VLAN Trunking Protocol for VLAN configuration management	Simplifies VLAN management by propagating VLAN configurations across the network and Ensures consistency in VLAN configurations
Telephony service	Supports voice communication over the network	Enables voice services and communication over the same network infrastructure and Integrates voice and data services for streamlined communication

System Overview

EarthLink Service Provider operates across two branches, with the main office situated in California and other branch in London, comprising departments such as Marketing, HR, and Accounting. California has two buildings, each with distinct departments. Building 1 accommodates Customer Care Unit 1 and Customer Care Unit 2, while Building 2 hosts Server Unit 1, Server Unit 2, Server Unit 3, and Technical Unit 4. The London branch's infrastructure features a network configuration of 4 Layer 2 switches and 2 Multilayer switches for Layer 2 connectivity, complemented by 6 routers and 2 firewalls for Layer 3 connectivity. The implementation of OSPF 200 in Area 0 and Area 20 facilitates streamlined management. Wireless connectivity is ensured through lightweight access points in each department, overseen by a Wireless LAN Controller (WLC) in the DMZ zone. IP phones are deployed for telecommunication purposes.

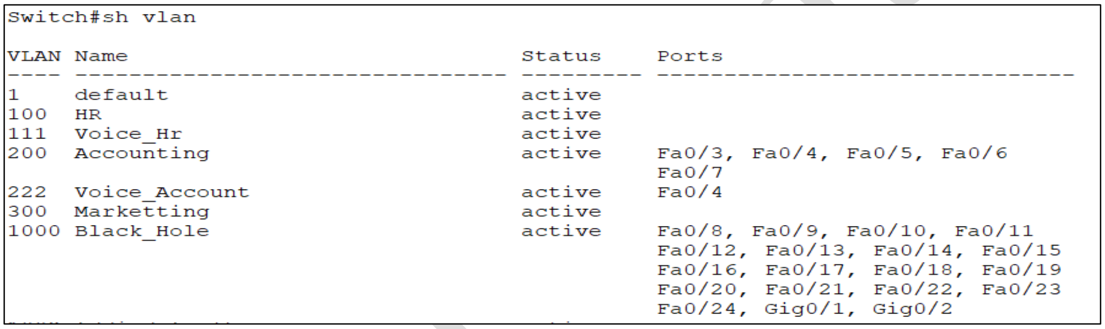
In California, a robust infrastructure includes 11 Layer 2 switches and 10 Multilayer switches for Layer 2 connectivity, alongside 3 Multilayer switches and 9 routers for Layer 3 connectivity. Security is reinforced through 6 firewalls and 7 servers, offering services such as AAA, DHCP, DNS, FTP, Syslog, TFTP, and HTTP. Routing configuration involves OSPF 100 Area 0 in Building 1 and OSPF 100 Area 10 in Building 2 for efficient management. Both branches are interconnected with ISP connectivity and maintain a GRE IPSec VPN tunnel running on the BGP protocol for redundancy. High availability is ensured with the implementation of a Wireless LAN Controller (WLC). Additional services encompass telephony services, VPN, Blackhole VLAN, Etherchannel, DHCP, DNS, and various others, contributing to a comprehensive and secure network infrastructure.

Product Implementation/Artifact

In this chapter we'll look at the network we've implemented to build and how well we implemented it. The most important phase of the project is when it is implemented. Before implementing the plan, we need to make sure that we have all the necessary equipment and that it is secure. This include fulfilling the specific requirements of the company, satisfying functional requirements, and making sure that regulations, physical restrictions, and service level agreements are followed.

1. VLAN

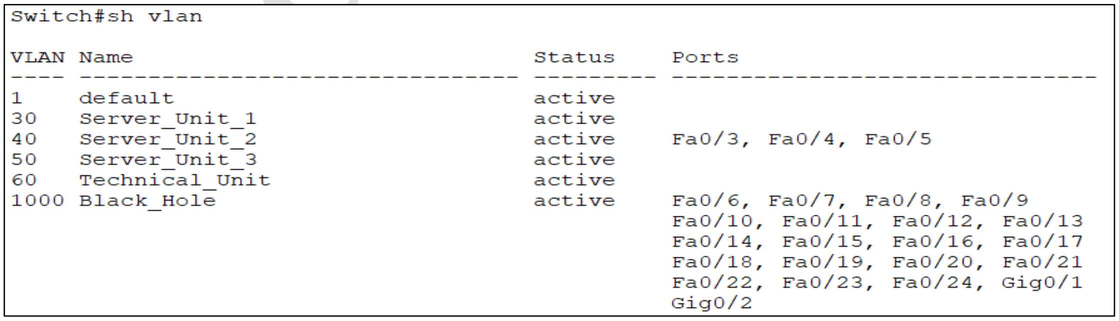
London:



```
Switch#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    
100  HR                               active    
111  Voice_Hr                         active    
200  Accounting                       active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7
222  Voice_Account                    active    Fa0/4
300  Marketting                       active    
1000 Black_Hole                       active    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, Gig0/1, Gig0/2
```

Figure 6 VLAN Implementation London Branch

California:



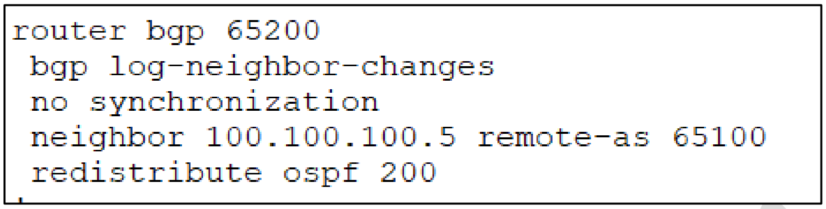
```
Switch#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    
30   Server_Unit_1                    active    
40   Server_Unit_2                    active    Fa0/3, Fa0/4, Fa0/5
50   Server_Unit_3                    active    
60   Technical_Unit                   active    
1000 Black_Hole                       active    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, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
```

Figure 7 VLAN Implementation California Branch

2. Routing

2.1. BGP

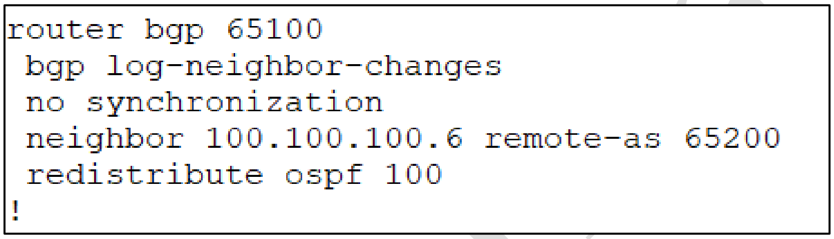
London:



```
router bgp 65200
 bgp log-neighbor-changes
 no synchronization
 neighbor 100.100.100.5 remote-as 65100
 redistribute ospf 200
```

Figure 8 BGP Protocol London Branch

California:

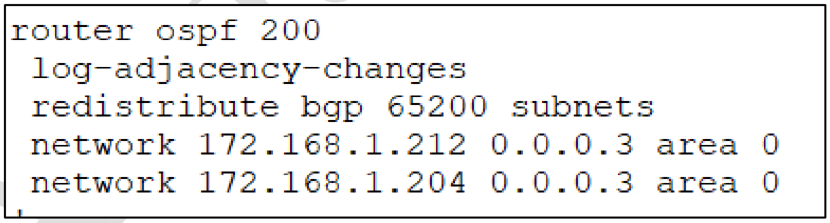


```
router bgp 65100
 bgp log-neighbor-changes
 no synchronization
 neighbor 100.100.100.6 remote-as 65200
 redistribute ospf 100
!
```

Figure 9 BGP Protocol California Branch

2.2. OSPF

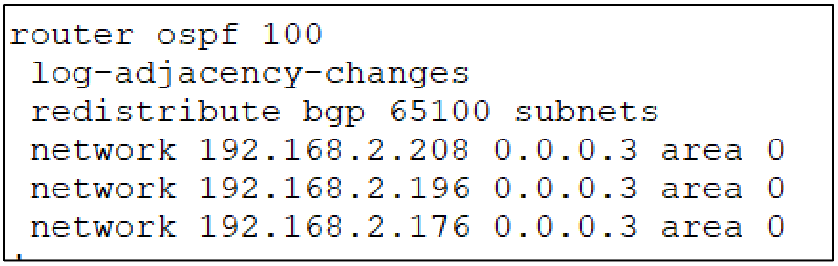
London:



```
router ospf 200
 log-adjacency-changes
 redistribute bgp 65200 subnets
 network 172.168.1.212 0.0.0.3 area 0
 network 172.168.1.204 0.0.0.3 area 0
```

Figure 10 OSPF London Branch

California:

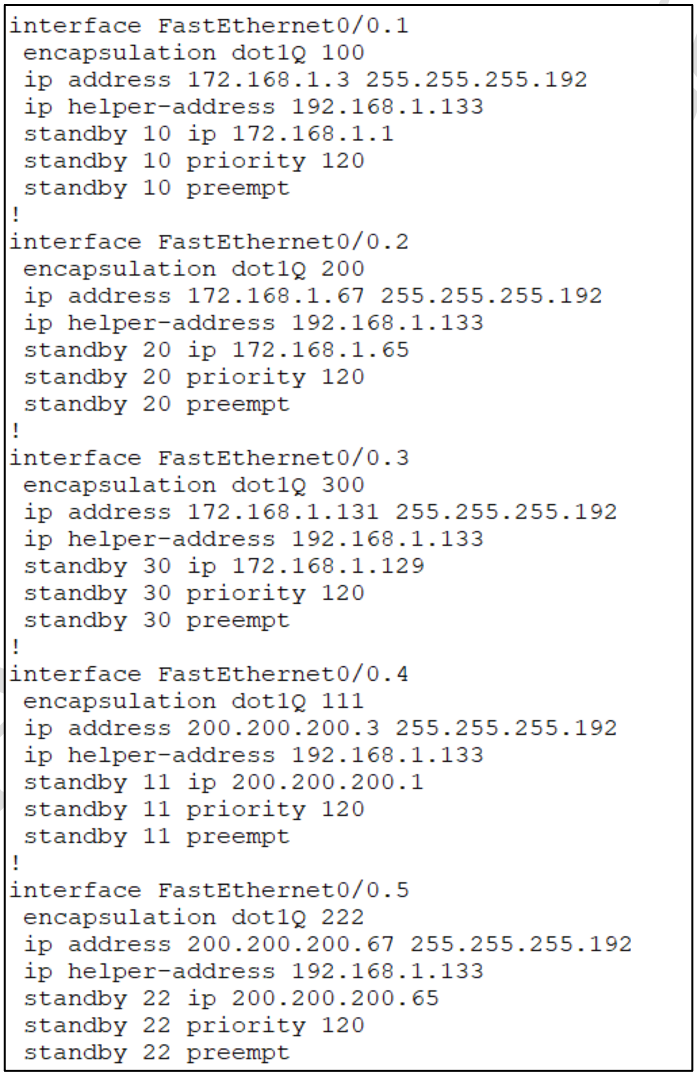


```
router ospf 100
 log-adjacency-changes
 redistribute bgp 65100 subnets
 network 192.168.2.208 0.0.0.3 area 0
 network 192.168.2.196 0.0.0.3 area 0
 network 192.168.2.176 0.0.0.3 area 0
```

Figure 11 OSPF California Branch

2.3. Inter VLAN Routing

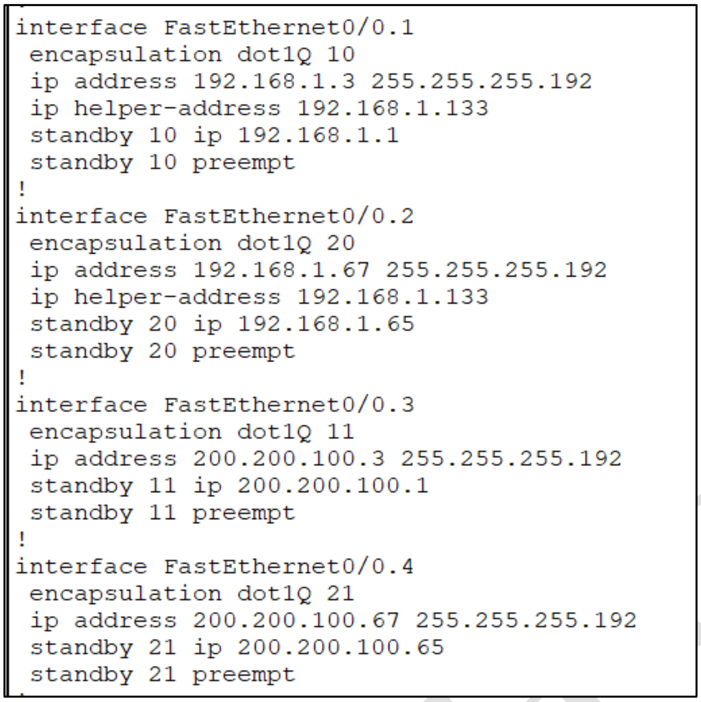
London:



```
interface FastEthernet0/0.1
 encapsulation dot1Q 100
 ip address 172.168.1.3 255.255.255.192
 ip helper-address 192.168.1.133
 standby 10 ip 172.168.1.1
 standby 10 priority 120
 standby 10 preempt
!
interface FastEthernet0/0.2
 encapsulation dot1Q 200
 ip address 172.168.1.67 255.255.255.192
 ip helper-address 192.168.1.133
 standby 20 ip 172.168.1.65
 standby 20 priority 120
 standby 20 preempt
!
interface FastEthernet0/0.3
 encapsulation dot1Q 300
 ip address 172.168.1.131 255.255.255.192
 ip helper-address 192.168.1.133
 standby 30 ip 172.168.1.129
 standby 30 priority 120
 standby 30 preempt
!
interface FastEthernet0/0.4
 encapsulation dot1Q 111
 ip address 200.200.200.3 255.255.255.192
 ip helper-address 192.168.1.133
 standby 11 ip 200.200.200.1
 standby 11 priority 120
 standby 11 preempt
!
interface FastEthernet0/0.5
 encapsulation dot1Q 222
 ip address 200.200.200.67 255.255.255.192
 ip helper-address 192.168.1.133
 standby 22 ip 200.200.200.65
 standby 22 priority 120
 standby 22 preempt
```

Figure 12 Inter VLAN Routing London Branch

California:



```
interface FastEthernet0/0.1
 encapsulation dot1Q 10
 ip address 192.168.1.3 255.255.255.192
 ip helper-address 192.168.1.133
 standby 10 ip 192.168.1.1
 standby 10 preempt
!
interface FastEthernet0/0.2
 encapsulation dot1Q 20
 ip address 192.168.1.67 255.255.255.192
 ip helper-address 192.168.1.133
 standby 20 ip 192.168.1.65
 standby 20 preempt
!
interface FastEthernet0/0.3
 encapsulation dot1Q 11
 ip address 200.200.100.3 255.255.255.192
 standby 11 ip 200.200.100.1
 standby 11 preempt
!
interface FastEthernet0/0.4
 encapsulation dot1Q 21
 ip address 200.200.100.67 255.255.255.192
 standby 21 ip 200.200.100.65
 standby 21 preempt
```

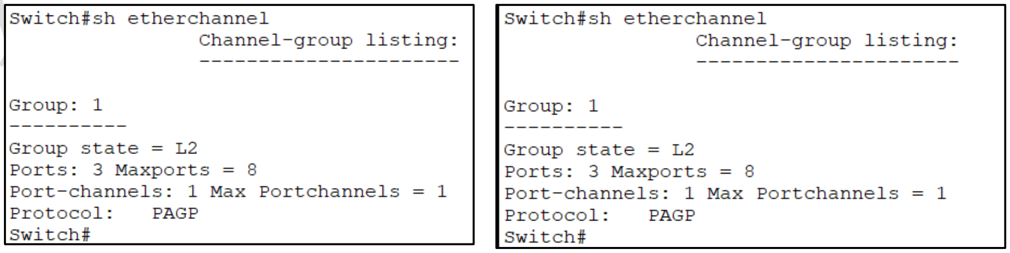
Figure 13 Inter VLAN Routing California Branch

3.0 Redundancy

for this project, I'm considering the idea of adding redundancy to increase its reliability and guarantee continuous operation.

3.1 EtherChannel

London:

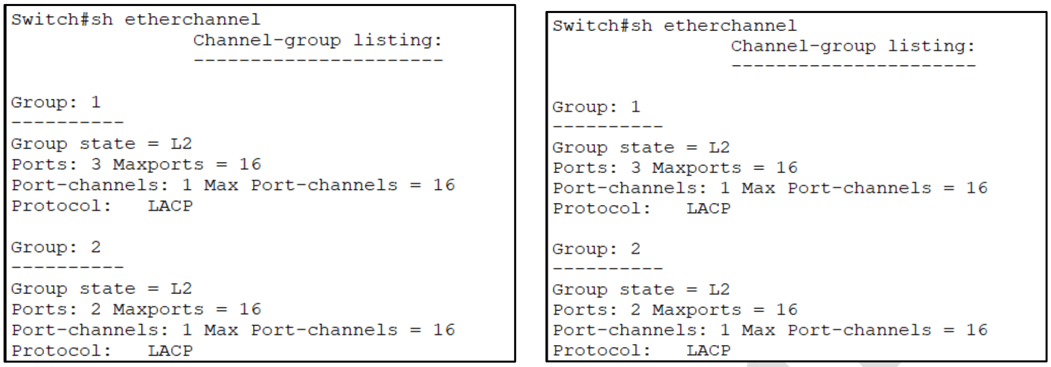


```
Switch#sh etherchannel
                Channel-group listing:
                ----------------------

Group: 1
----------
Group state = L2
Ports: 3 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol:   PAGP
Switch#
```

```
Switch#sh etherchannel
                Channel-group listing:
                ----------------------

Group: 1
----------
Group state = L2
Ports: 3 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol:   PAGP
Switch#
```

Figure 14 Etherchannel London Branch

California:



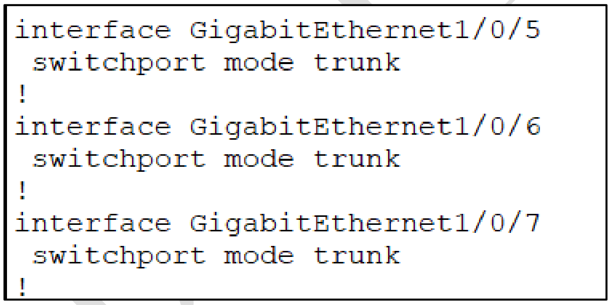
```
Switch#sh etherchannel
                Channel-group listing:
                ----------------------

Group: 1
----------
Group state = L2
Ports: 3 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP

Group: 2
----------
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP
```

```
Switch#sh etherchannel
                Channel-group listing:
                ----------------------

Group: 1
----------
Group state = L2
Ports: 3 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP

Group: 2
----------
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP
```

Figure 15 Etherchannel California Branch

3.2 Trunking protocols

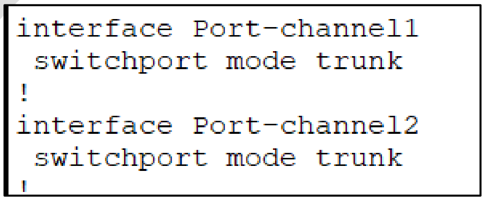
London:



```
interface GigabitEthernet1/0/5
 switchport mode trunk
!
interface GigabitEthernet1/0/6
 switchport mode trunk
!
interface GigabitEthernet1/0/7
 switchport mode trunk
!
```

Figure 16 Trunking Protocol London Branch

California:

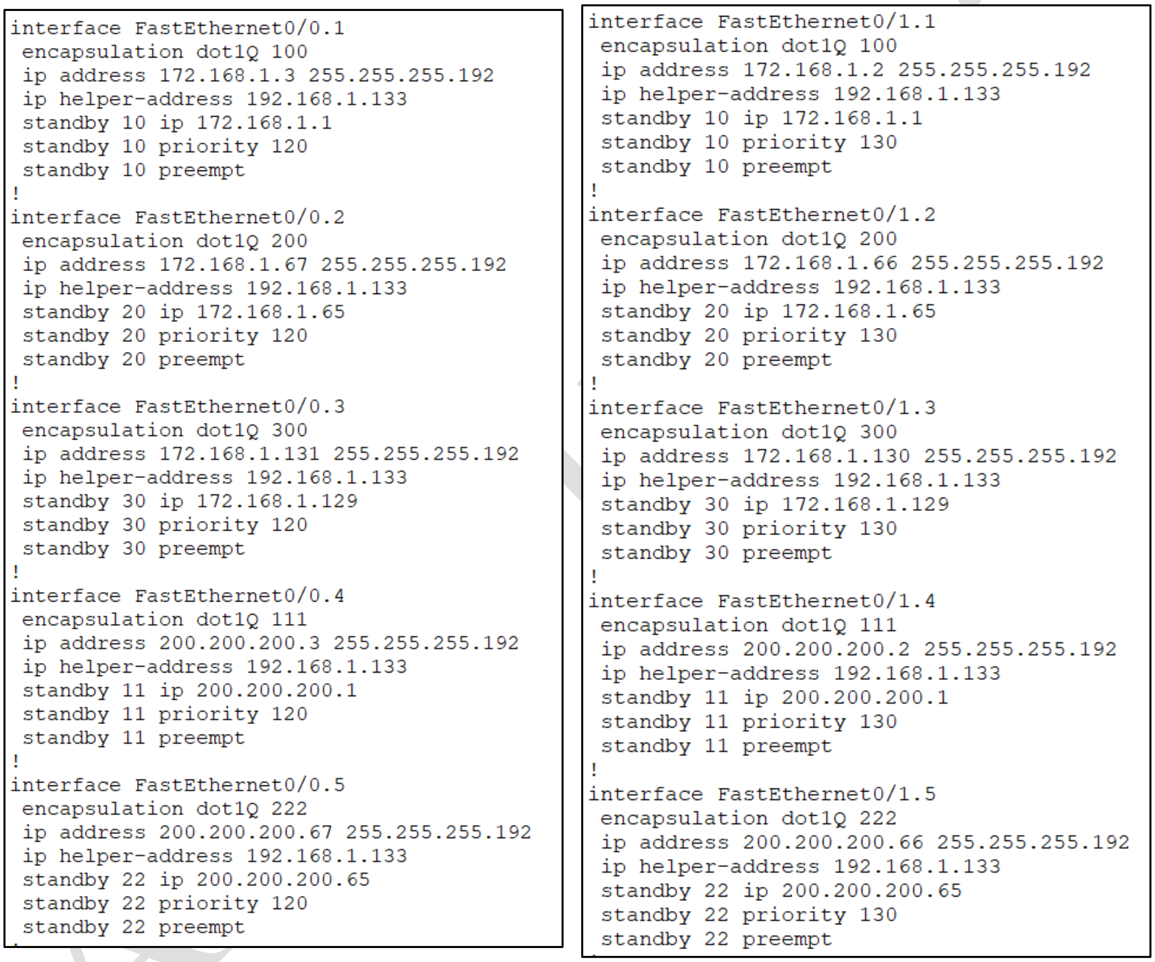


```
interface Port-channel1
 switchport mode trunk
!
interface Port-channel2
 switchport mode trunk
!
```

Figure 17 Trunking Protocol California Branch

3.3 FHRP

London:

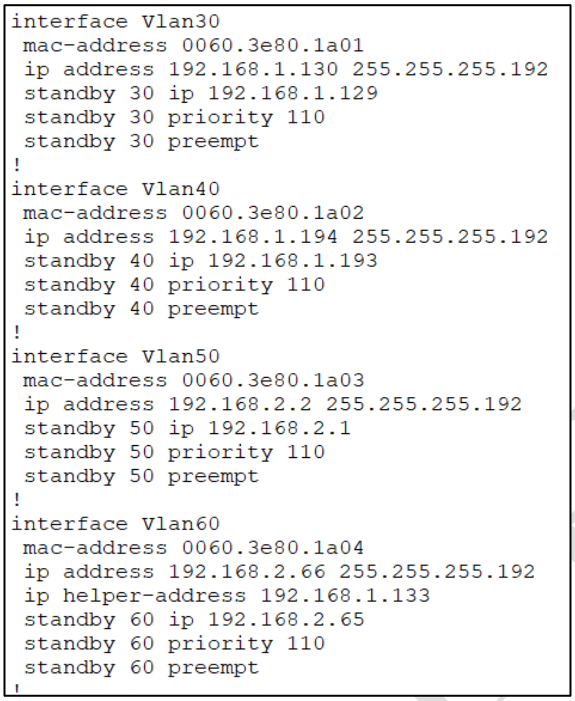


```
interface FastEthernet0/0.1
 encapsulation dot1Q 100
 ip address 172.168.1.3 255.255.255.192
 ip helper-address 192.168.1.133
 standby 10 ip 172.168.1.1
 standby 10 priority 120
 standby 10 preempt
!
interface FastEthernet0/0.2
 encapsulation dot1Q 200
 ip address 172.168.1.67 255.255.255.192
 ip helper-address 192.168.1.133
 standby 20 ip 172.168.1.65
 standby 20 priority 120
 standby 20 preempt
!
interface FastEthernet0/0.3
 encapsulation dot1Q 300
 ip address 172.168.1.131 255.255.255.192
 ip helper-address 192.168.1.133
 standby 30 ip 172.168.1.129
 standby 30 priority 120
 standby 30 preempt
!
interface FastEthernet0/0.4
 encapsulation dot1Q 111
 ip address 200.200.200.3 255.255.255.192
 ip helper-address 192.168.1.133
 standby 11 ip 200.200.200.1
 standby 11 priority 120
 standby 11 preempt
!
interface FastEthernet0/0.5
 encapsulation dot1Q 222
 ip address 200.200.200.67 255.255.255.192
 ip helper-address 192.168.1.133
 standby 22 ip 200.200.200.65
 standby 22 priority 120
 standby 22 preempt
```

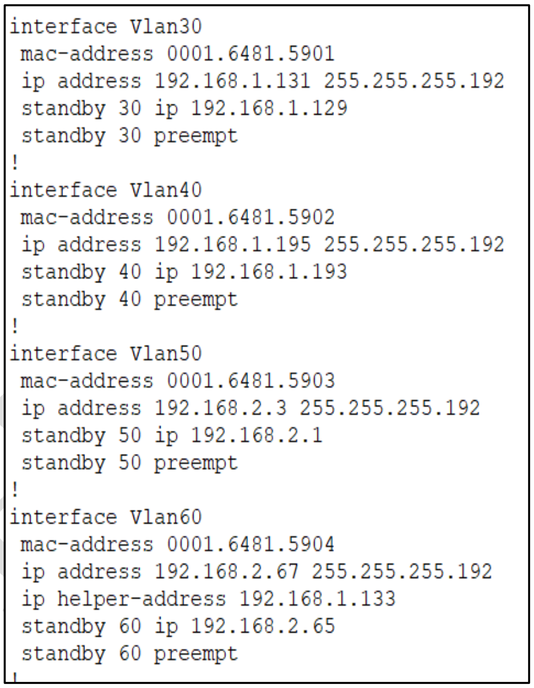
```
interface FastEthernet0/1.1
 encapsulation dot1Q 100
 ip address 172.168.1.2 255.255.255.192
 ip helper-address 192.168.1.133
 standby 10 ip 172.168.1.1
 standby 10 priority 130
 standby 10 preempt
!
interface FastEthernet0/1.2
 encapsulation dot1Q 200
 ip address 172.168.1.66 255.255.255.192
 ip helper-address 192.168.1.133
 standby 20 ip 172.168.1.65
 standby 20 priority 130
 standby 20 preempt
!
interface FastEthernet0/1.3
 encapsulation dot1Q 300
 ip address 172.168.1.130 255.255.255.192
 ip helper-address 192.168.1.133
 standby 30 ip 172.168.1.129
 standby 30 priority 130
 standby 30 preempt
!
interface FastEthernet0/1.4
 encapsulation dot1Q 111
 ip address 200.200.200.2 255.255.255.192
 ip helper-address 192.168.1.133
 standby 11 ip 200.200.200.1
 standby 11 priority 130
 standby 11 preempt
!
interface FastEthernet0/1.5
 encapsulation dot1Q 222
 ip address 200.200.200.66 255.255.255.192
 ip helper-address 192.168.1.133
 standby 22 ip 200.200.200.65
 standby 22 priority 130
 standby 22 preempt
```

Figure 18 FHRP London Branch

California:



```
interface Vlan30
 mac-address 0060.3e80.1a01
 ip address 192.168.1.130 255.255.255.192
 standby 30 ip 192.168.1.129
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan40
 mac-address 0060.3e80.1a02
 ip address 192.168.1.194 255.255.255.192
 standby 40 ip 192.168.1.193
 standby 40 priority 110
 standby 40 preempt
!
interface Vlan50
 mac-address 0060.3e80.1a03
 ip address 192.168.2.2 255.255.255.192
 standby 50 ip 192.168.2.1
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan60
 mac-address 0060.3e80.1a04
 ip address 192.168.2.66 255.255.255.192
 ip helper-address 192.168.1.133
 standby 60 ip 192.168.2.65
 standby 60 priority 110
 standby 60 preempt
!
```

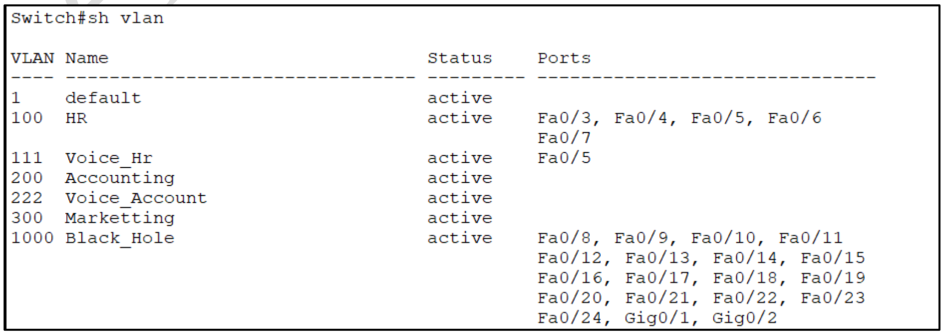


```
interface Vlan30
 mac-address 0001.6481.5901
 ip address 192.168.1.131 255.255.255.192
 standby 30 ip 192.168.1.129
 standby 30 preempt
!
interface Vlan40
 mac-address 0001.6481.5902
 ip address 192.168.1.195 255.255.255.192
 standby 40 ip 192.168.1.193
 standby 40 preempt
!
interface Vlan50
 mac-address 0001.6481.5903
 ip address 192.168.2.3 255.255.255.192
 standby 50 ip 192.168.2.1
 standby 50 preempt
!
interface Vlan60
 mac-address 0001.6481.5904
 ip address 192.168.2.67 255.255.255.192
 ip helper-address 192.168.1.133
 standby 60 ip 192.168.2.65
 standby 60 preempt
!
```

Figure 19 FHRP California Branch

4. Black Hole VLAN

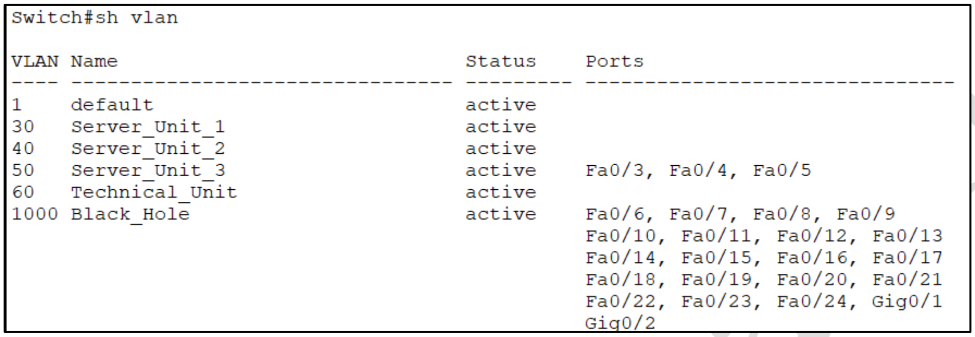
London:



```
Switch#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
100  HR                               active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7
111  Voice_Hr                         active    Fa0/5
200  Accounting                       active
222  Voice_Account                    active
300  Marketting                       active
1000 Black_Hole                       active    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, Gig0/1, Gig0/2
```

Figure 20 Blackhole VLAN London

California:



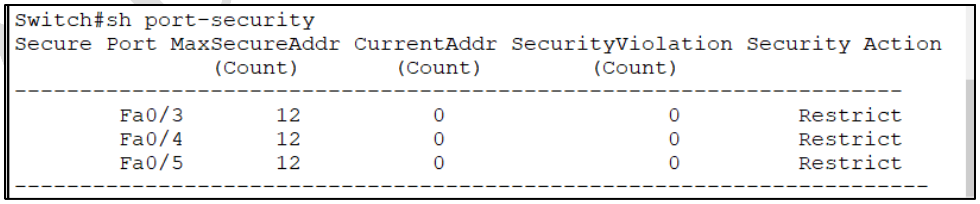
```
Switch#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
30   Server_Unit_1                    active
40   Server_Unit_2                    active
50   Server_Unit_3                    active    Fa0/3, Fa0/4, Fa0/5
60   Technical_Unit                   active
1000 Black_Hole                       active    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, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
```

Figure 21 Blackhole VLAN California

5. Port security

port security - Port security is a network security feature that is implemented at the switch port level to control access to a network by limiting the number of devices that can connect through a specific switch port. The primary goal of port security is to enhance the security of the network by preventing unauthorized or unauthenticated devices from gaining access to the network.

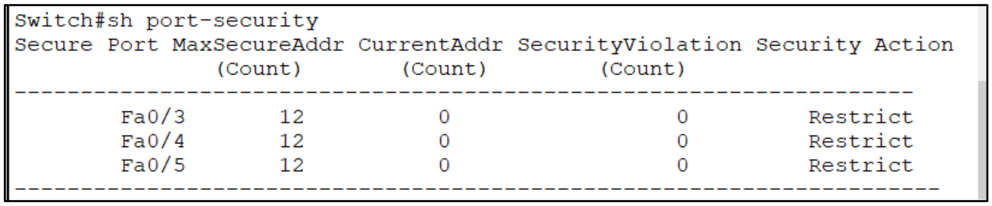
London:



```
Switch#sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)       (Count)        (Count)
--------------------------------------------------------------------
        Fa0/3        12          0                  0         Restrict
        Fa0/4        12          0                  0         Restrict
        Fa0/5        12          0                  0         Restrict
----------------------------------------------------------------------
```

Figure 22 Port security London Branch

California:



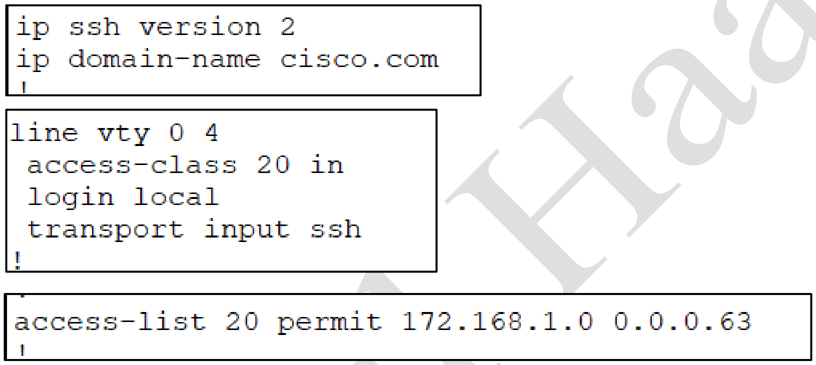
```
Switch#sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)       (Count)        (Count)
--------------------------------------------------------------------
        Fa0/3        12          0                  0         Restrict
        Fa0/4        12          0                  0         Restrict
        Fa0/5        12          0                  0         Restrict
----------------------------------------------------------------------
```

Figure 23 Port security California Branch

6. SSH

SSH - SSH, or Secure Shell, is a cryptographic network protocol used for secure communication over an unsecured network. It is widely used for remote administration of network devices and servers. SSH provides a secure and encrypted connection, allowing users to access and manage systems securely.

London:



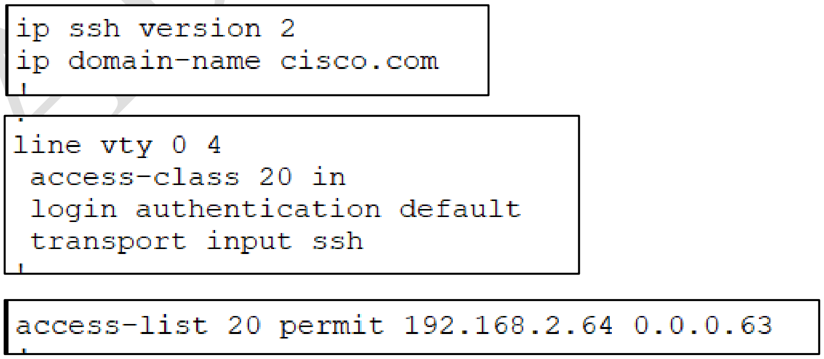
```
ip ssh version 2
ip domain-name cisco.com
!
```

```
line vty 0 4
 access-class 20 in
 login local
 transport input ssh
!
```

```
access-list 20 permit 172.168.1.0 0.0.0.63
!
```

Figure 24 SSH London Branch

California:



```
ip ssh version 2
ip domain-name cisco.com
!
```

```
line vty 0 4
 access-class 20 in
 login authentication default
 transport input ssh
!
```

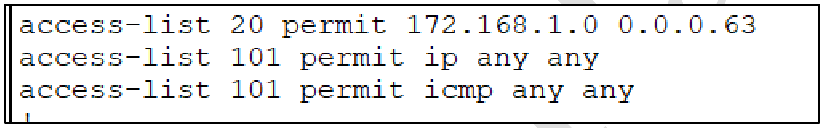
```
access-list 20 permit 192.168.2.64 0.0.0.63
```

Figure 25 SSH California Branch

7. Access-list

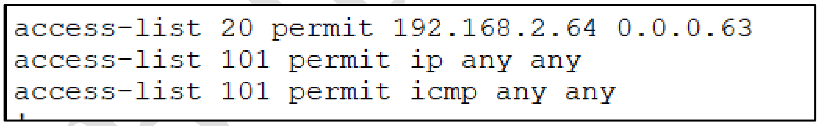
ACL- ACLs, or access control lists, are setups or sets of rules used to filter and manage network traffic according to predetermined standards. ACLs are frequently used in firewalls, switches, and routers to specify the types of traffic that are allow or deny from passing through the device. Usually, these rules depend on variables like protocols, port numbers, source and destination IP addresses.

London:



```
access-list 20 permit 172.168.1.0 0.0.0.63
access-list 101 permit ip any any
access-list 101 permit icmp any any
!
```

Figure 26 Access-list London Branch 1



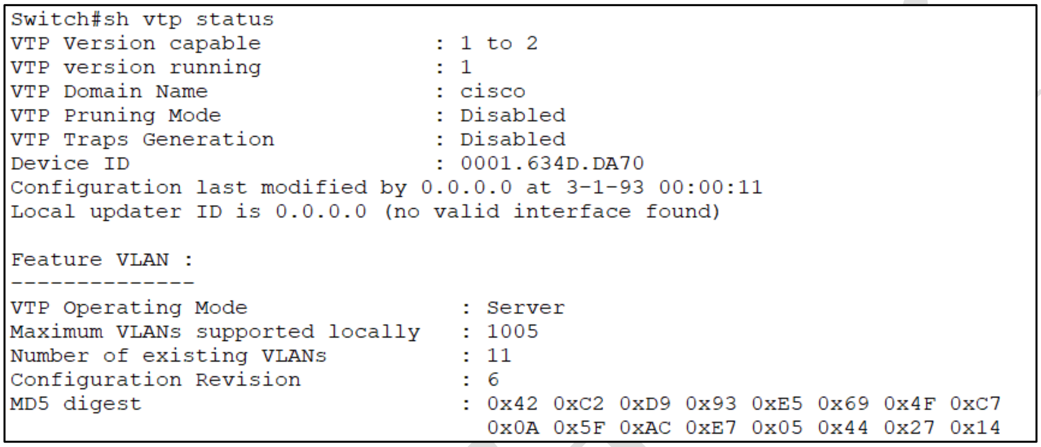
```
access-list 20 permit 192.168.2.64 0.0.0.63
access-list 101 permit ip any any
access-list 101 permit icmp any any
!
```

Figure 27 Access-list London Branch 2

8. VTP

VTP - VTP, or VLAN Trucking Protocol, is a proprietary protocol from Cisco used in networks to distribute and manage VLAN configuration data. Through the ability to configure VLANs on a single switch (referred to as the VTP server) and the automatic propagation of that configuration information to other switches in the network, it streamlines the administration of VLANs (Virtual Local Area Networks).

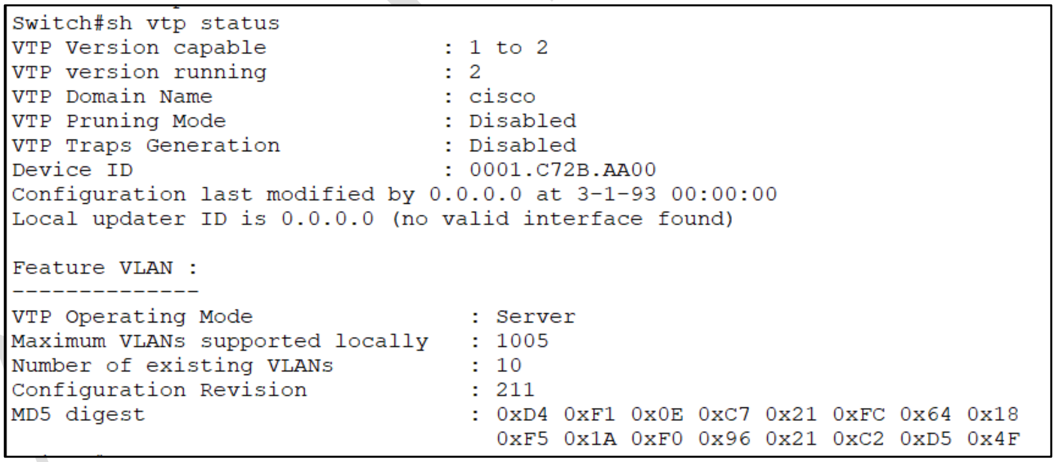
London:



```
Switch#sh vtp status
VTP Version capable              : 1 to 2
VTP version running              : 1
VTP Domain Name                  : cisco
VTP Pruning Mode                 : Disabled
VTP Traps Generation             : Disabled
Device ID                        : 0001.634D.DA70
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:11
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
--------------
VTP Operating Mode                 : Server
Maximum VLANs supported locally    : 1005
Number of existing VLANs           : 11
Configuration Revision             : 6
MD5 digest                         : 0x42 0xC2 0xD9 0x93 0xE5 0x69 0x4F 0xC7
                                     0x0A 0x5F 0xAC 0xE7 0x05 0x44 0x27 0x14
```

Figure 28 VTP London Branch

California:



```
Switch#sh vtp status
VTP Version capable              : 1 to 2
VTP version running              : 2
VTP Domain Name                  : cisco
VTP Pruning Mode                 : Disabled
VTP Traps Generation             : Disabled
Device ID                        : 0001.C72B.AA00
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
--------------
VTP Operating Mode                 : Server
Maximum VLANs supported locally    : 1005
Number of existing VLANs           : 10
Configuration Revision             : 211
MD5 digest                         : 0xD4 0xF1 0x0E 0xC7 0x21 0xFC 0x64 0x18
                                     0xF5 0x1A 0xF0 0x96 0x21 0xC2 0xD5 0x4F
```

Figure 29 VTP California Branch

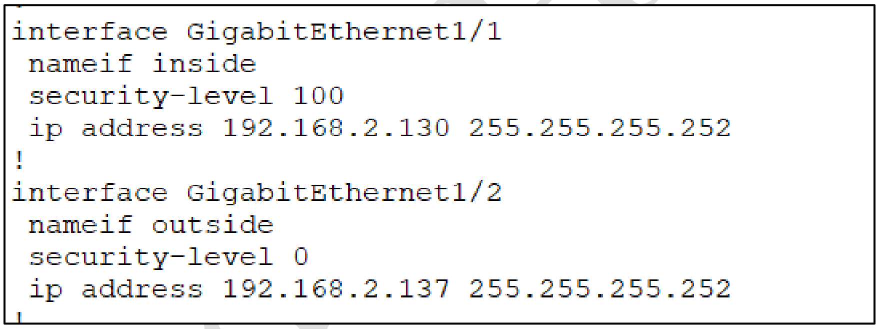
9. Firewall

firewall ACL - A Firewall's Access Control List (ACL) is a collection of rules designed to manage and monitor network traffic on the firewall. Conditions including source and destination addresses, port numbers, and protocols are specified by each ACL rule. These rules are used by the firewall to decide which kinds of traffic to allow or prohibit. ACLs enable administrators to specify exactly how various types of traffic should be addressed at the network border, which is essential for implementing security policies and securing networks.

9.1. Zone

A firewall zone is a logical grouping or segmentation of systems or network devices according to their trust levels and security requirements. Incoming and outgoing network traffic is monitored and controlled by firewalls, which are network security devices, in accordance with pre-established security rules. In order to effectively monitor and execute security regulations, administrators frequently build firewall zones when organizing these rules.

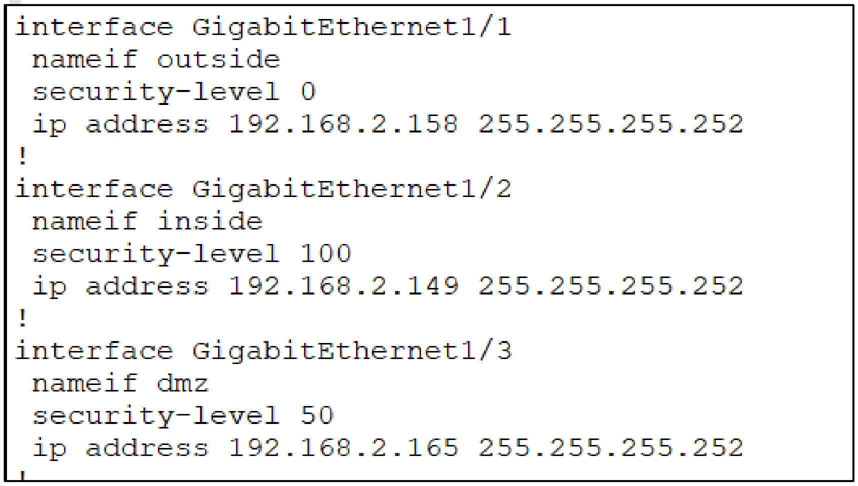
London:



```
interface GigabitEthernet1/1
 nameif inside
 security-level 100
 ip address 192.168.2.130 255.255.255.252
!
interface GigabitEthernet1/2
 nameif outside
 security-level 0
 ip address 192.168.2.137 255.255.255.252
```

Figure 30 Firewall Zone London Branch

California:

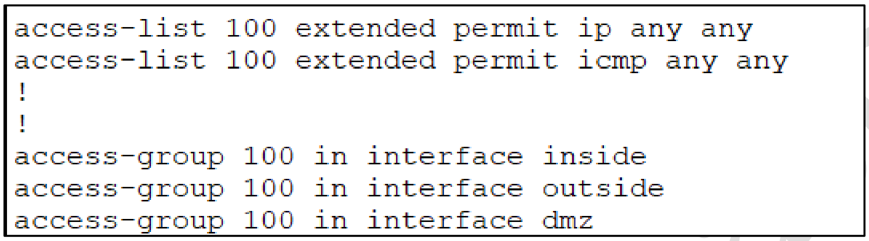


```
interface GigabitEthernet1/1
 nameif outside
 security-level 0
 ip address 192.168.2.158 255.255.255.252
!
interface GigabitEthernet1/2
 nameif inside
 security-level 100
 ip address 192.168.2.149 255.255.255.252
!
interface GigabitEthernet1/3
 nameif dmz
 security-level 50
 ip address 192.168.2.165 255.255.255.252
```

Figure 31 Firewall Zone California Branch

9.2. Access-list

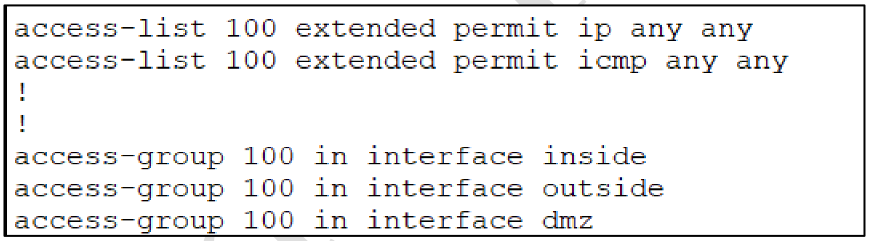
London:



```
access-list 100 extended permit ip any any
access-list 100 extended permit icmp any any
!
!
access-group 100 in interface inside
access-group 100 in interface outside
access-group 100 in interface dmz
```

Figure 32 Firewall ACL London Branch

California:



```
access-list 100 extended permit ip any any
access-list 100 extended permit icmp any any
!
!
access-group 100 in interface inside
access-group 100 in interface outside
access-group 100 in interface dmz
```

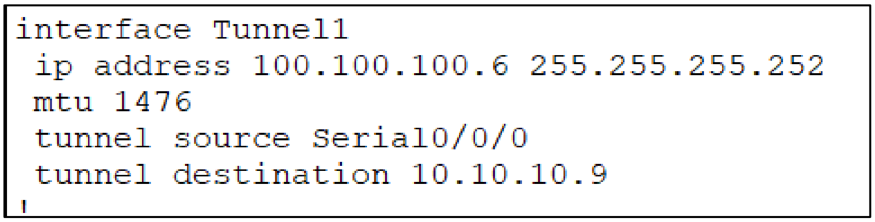
Figure 33 Firewall ACL California Branch

10. VPN

GRE tunnel - A VPN GRE (Generic Routing Encapsulation) tunnel is a type of virtual private network (VPN) that uses GRE protocol to encapsulate and transport data securely between two points over an existing network. GRE itself is a tunneling protocol that allows the encapsulation of a wide variety of network layer protocols inside point-to-point connections.

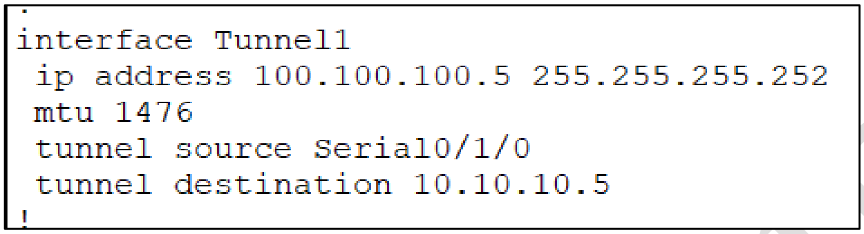
10.1. GRE Tunnel

London:



```
interface Tunnel1
 ip address 100.100.100.6 255.255.255.252
 mtu 1476
 tunnel source Serial0/0/0
 tunnel destination 10.10.10.9
!
```

California:



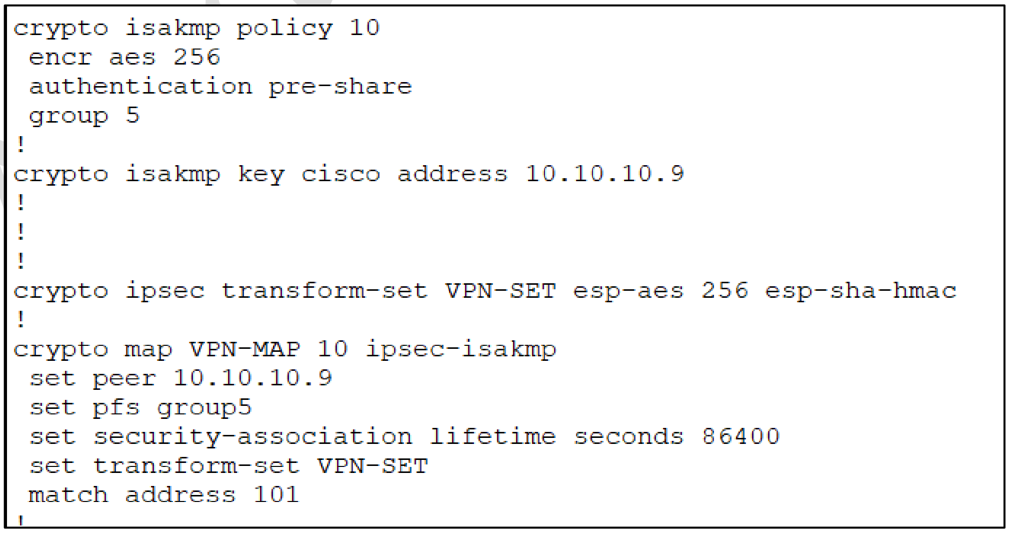
```
!
interface Tunnel1
 ip address 100.100.100.5 255.255.255.252
 mtu 1476
 tunnel source Serial0/1/0
 tunnel destination 10.10.10.5
!
```

Figure 35 VPN GRE Tunnel California Branch

10.2. IP sec

IPSEC - A group of protocols called IPsec, or Internet Protocol Security, is used to protect communications via the Internet Protocol (IP). By offering a range of cryptographic security services at the IP layer, it makes it possible to set up private and secure channels of communication over IP networks like the Internet. Virtual Private Networks (VPNs) frequently utilize IPsec to ensure the validity, integrity, and confidentiality of data transmissions.

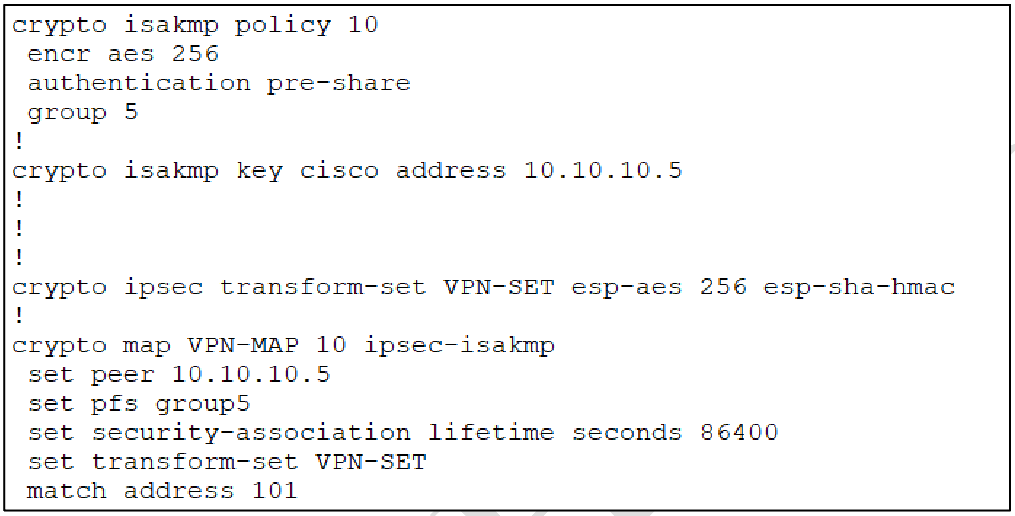
London:



```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key cisco address 10.10.10.9
!
!
!
crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
 set peer 10.10.10.9
 set pfs group5
 set security-association lifetime seconds 86400
 set transform-set VPN-SET
 match address 101
!
```

Figure 36 VPN IP sec London Branch

California:

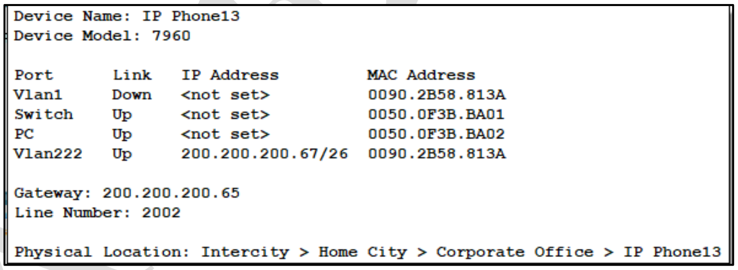


```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key cisco address 10.10.10.5
!
!
!
crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
 set peer 10.10.10.5
 set pfs group5
 set security-association lifetime seconds 86400
 set transform-set VPN-SET
 match address 101
```

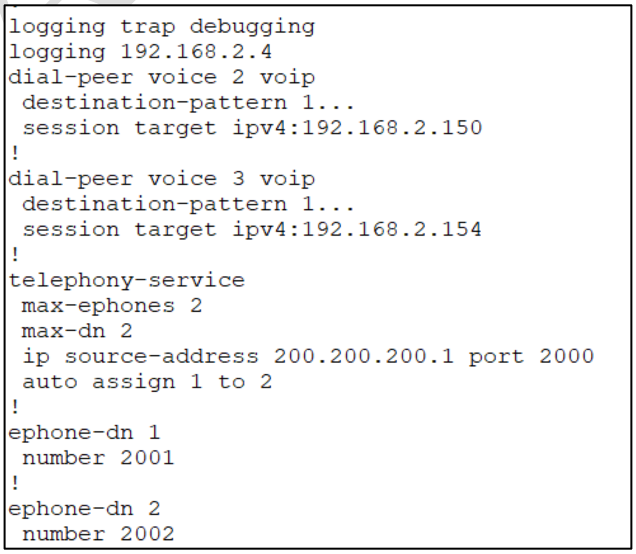
Figure 37 VPN IP sec California Branch

11. Telephony service

London:



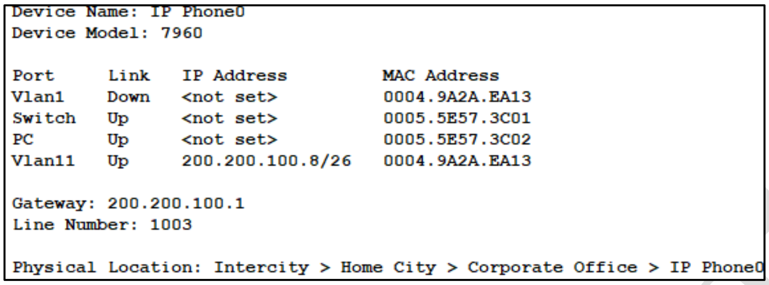
```
Device Name: IP Phone13
Device Model: 7960

Port      Link   IP Address          MAC Address
Vlan1     Down   <not set>           0090.2B58.813A
Switch    Up     <not set>           0050.0F3B.BA01
PC        Up     <not set>           0050.0F3B.BA02
Vlan222   Up     200.200.200.67/26   0090.2B58.813A

Gateway: 200.200.200.65
Line Number: 2002

Physical Location: Intercity > Home City > Corporate Office > IP Phone13
```



```
logging trap debugging
logging 192.168.2.4
dial-peer voice 2 voip
 destination-pattern 1...
 session target ipv4:192.168.2.150
!
dial-peer voice 3 voip
 destination-pattern 1...
 session target ipv4:192.168.2.154
!
telephony-service
 max-ephones 2
 max-dn 2
 ip source-address 200.200.200.1 port 2000
 auto assign 1 to 2
!
ephone-dn 1
 number 2001
!
ephone-dn 2
 number 2002
```

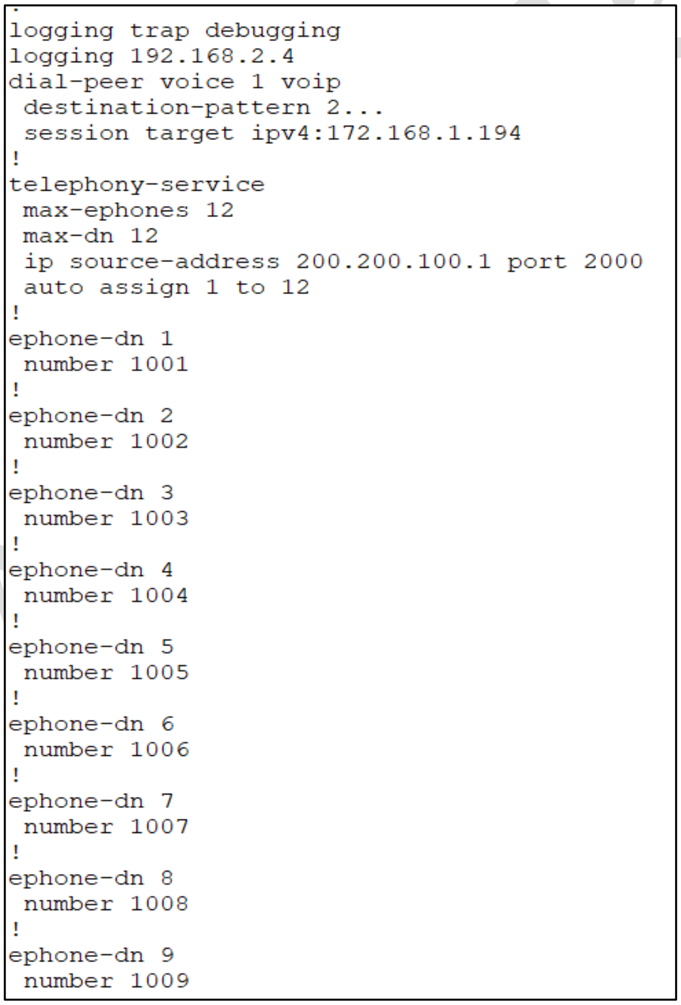
Figure 38 Telephony Service London Branch

California:



```
Device Name: IP Phone0
Device Model: 7960

Port     Link   IP Address         MAC Address
Vlan1    Down   <not set>          0004.9A2A.EA13
Switch   Up     <not set>          0005.5E57.3C01
PC       Up     <not set>          0005.5E57.3C02
Vlan11   Up     200.200.100.8/26   0004.9A2A.EA13

Gateway: 200.200.100.1
Line Number: 1003

Physical Location: Intercity > Home City > Corporate Office > IP Phone0
```

Figure 39 Californian Tell 1

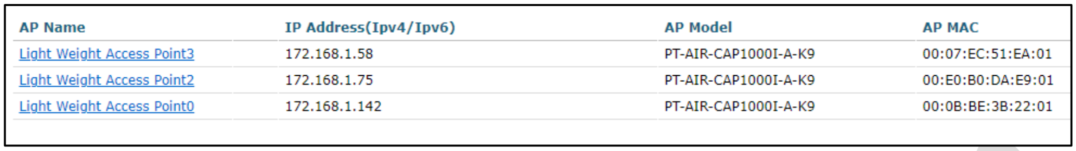


```
logging trap debugging
logging 192.168.2.4
dial-peer voice 1 voip
 destination-pattern 2...
 session target ipv4:172.168.1.194
!
telephony-service
 max-ephones 12
 max-dn 12
 ip source-address 200.200.100.1 port 2000
 auto assign 1 to 12
!
ephone-dn 1
 number 1001
!
ephone-dn 2
 number 1002
!
ephone-dn 3
 number 1003
!
ephone-dn 4
 number 1004
!
ephone-dn 5
 number 1005
!
ephone-dn 6
 number 1006
!
ephone-dn 7
 number 1007
!
ephone-dn 8
 number 1008
!
ephone-dn 9
 number 1009
```

Figure 40Califonian Tell 2

12. WLAC

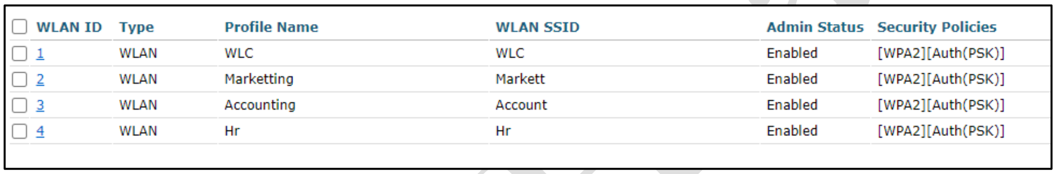
12.1. LAPT



AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC
Light Weight Access Point3	172.168.1.58	PT-AIR-CAP1000I-A-K9	00:07:EC:51:EA:01
Light Weight Access Point2	172.168.1.75	PT-AIR-CAP1000I-A-K9	00:E0:B0:DA:E9:01
Light Weight Access Point0	172.168.1.142	PT-AIR-CAP1000I-A-K9	00:0B:BE:3B:22:01

Figure 41 Light Weight Access Point

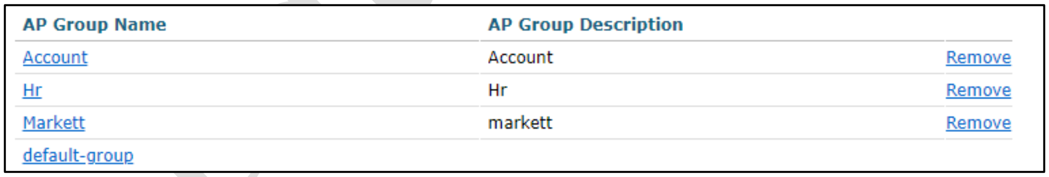
12.2. WLAN profile



□ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
□ 1	WLAN	WLC	WLC	Enabled	[WPA2][Auth(PSK)]
□ 2	WLAN	Marketting	Markett	Enabled	[WPA2][Auth(PSK)]
□ 3	WLAN	Accounting	Account	Enabled	[WPA2][Auth(PSK)]
□ 4	WLAN	Hr	Hr	Enabled	[WPA2][Auth(PSK)]

Figure 42 WLAN Profile

12.3. AP groups

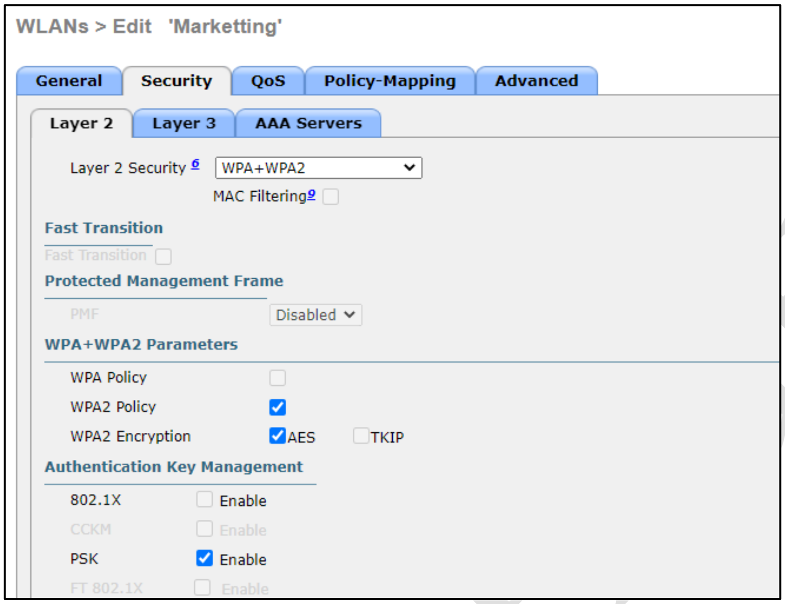


AP Group Name	AP Group Description	
Account	Account	Remove
Hr	Hr	Remove
Markett	markett	Remove
default-group		

Figure 43 AP Groups

12.4. WLAN security

London:



WLANs > Edit 'Marketting'

Layer 2 Security: WPA+WPA2

MAC Filtering □

Fast Transition

Fast Transition □

Protected Management Frame

PMF: Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑ AES □ TKIP

Authentication Key Management

802.1X □ Enable

CCKM □ Enable

PSK ☑ Enable

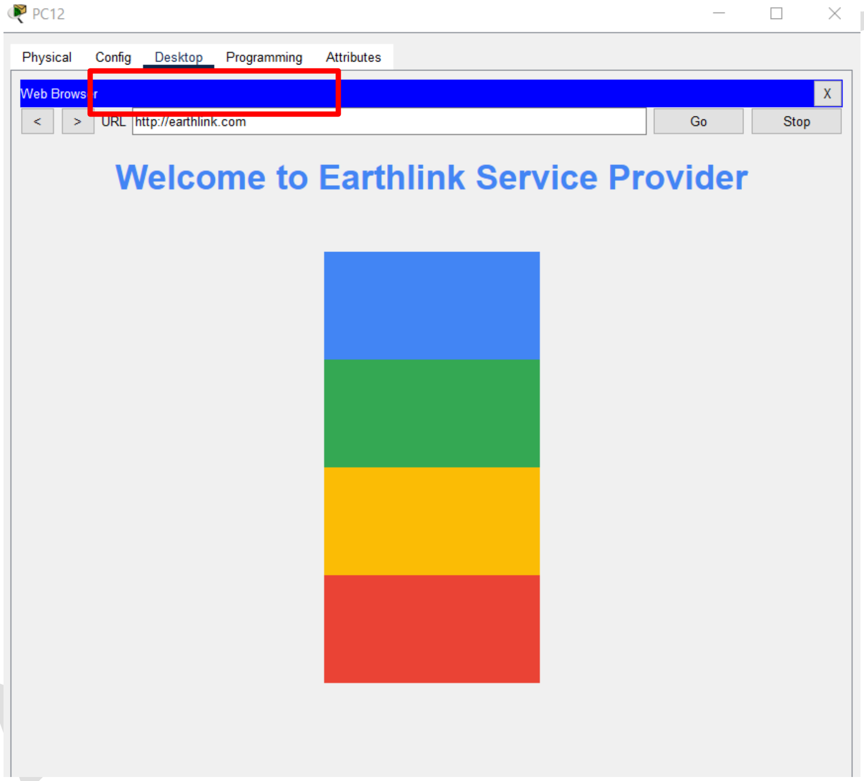
FT 802.1X □ Enable

Figure 44 WLAN Security

Validation

We will test our network in this chapter to make sure the system is error-free. This chapter will demonstrate the product's quality and demonstrate to the clients that it satisfies all of their requests. If we discover any issues with this section, we can fix them right away and finish the project on schedule. In this chapter, we will ping the computers, routers, and servers in all departments to make sure they are always up and fully functional. Port security, SSH, AAA, Firewall, and ACL will all be put to the test.

1. HTTP



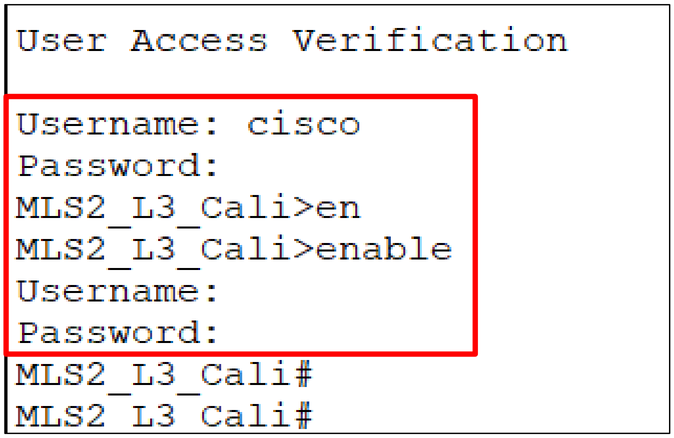
URL http://earthlink.com

Welcome to Earthlink Service Provider

Figure 45 HTTP

I have successfully implemented HTTP at our head office in California. The HTTP (Hypertext Transfer Protocol) is being implemented in order to facilitate data transfer and communication over the web easier. Any data exchange on the Web depends on HTTP, which enables browsers to send and receive requests for information from web servers.

2. AAA

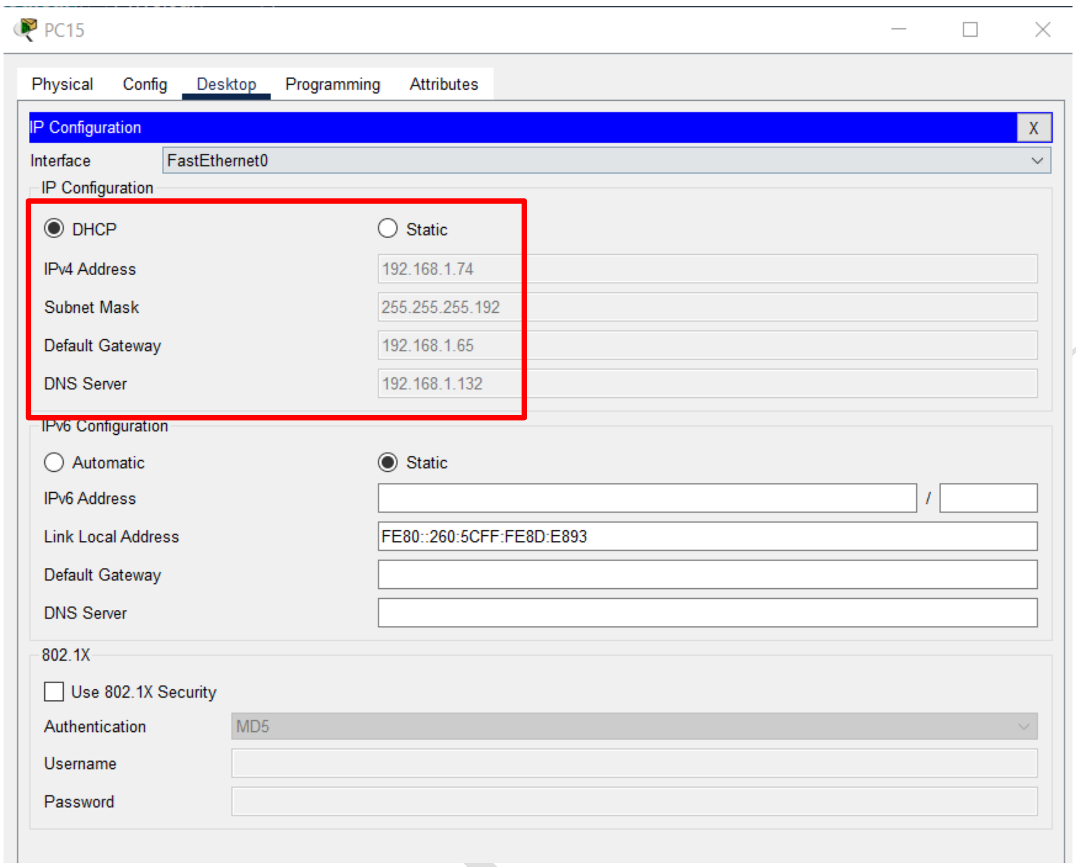


```
User Access Verification

Username: cisco
Password:
MLS2_L3_Cali>en
MLS2_L3_Cali>enable
Username:
Password:
MLS2_L3_Cali#
MLS2_L3_Cali#
```

Figure 46 Authenthication Authorization Accounting (AAA)

In order to ensure secure and controlled access to network resources, the AAA framework is essential. It is frequently used in network devices like switches, routers, and authentication servers. Organizations may limit access to critical information, enforce security regulations, and keep an audit trail of network activity by utilizing AAA.

3. DHCP



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.1.74

Subnet Mask: 255.255.255.192

Default Gateway: 192.168.1.65

DNS Server: 192.168.1.132

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::260:5CFF:FE8D:E893

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

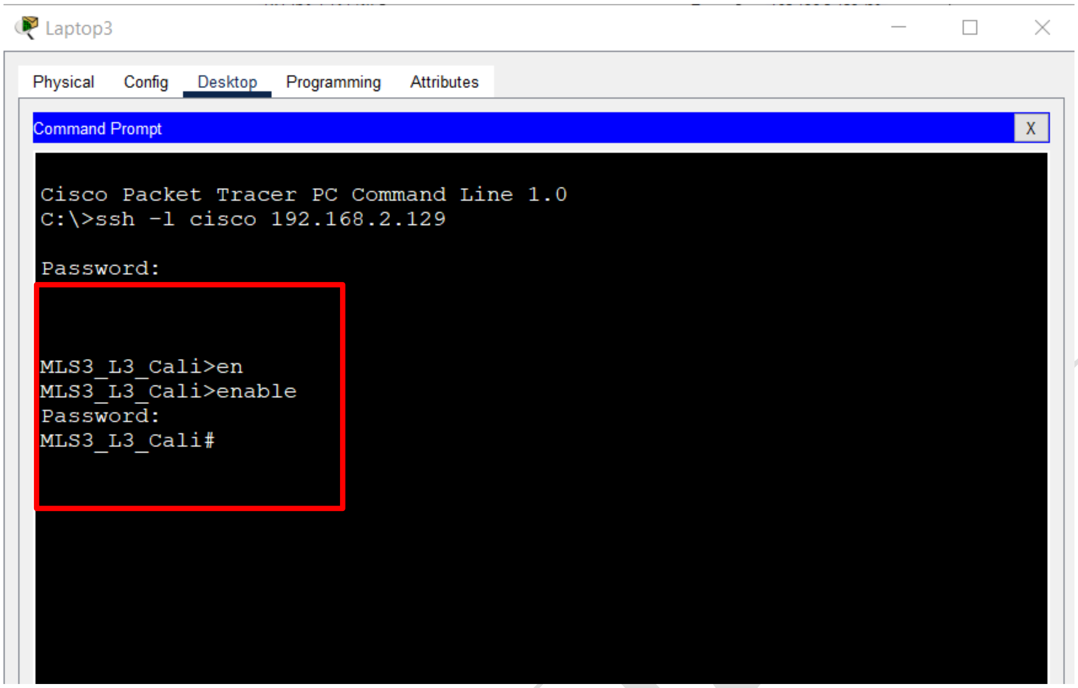
Username:

Password:

Figure 47 DHCP

We configure the IP address using DHCP. The DHCP server assigns the IP address, and the testing confirms that the configuration is accurate.

4. SSH



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l cisco 192.168.2.129

Password:



MLS3_L3_Cali>en
MLS3_L3_Cali>enable
Password:
MLS3_L3_Cali#
```

Figure 48 SSH

SSH stands for Secure Shell, and it is a cryptographic network protocol used for secure communication over an unsecured network. The primary purpose of SSH is to provide a secure way to access and manage network devices, servers, and systems remotely. It establishes a secure, encrypted connection between a client and a server, allowing for secure data transmission and remote command execution. Through this test, I verified that SSH functions as expected**.**

5. Telephone Service

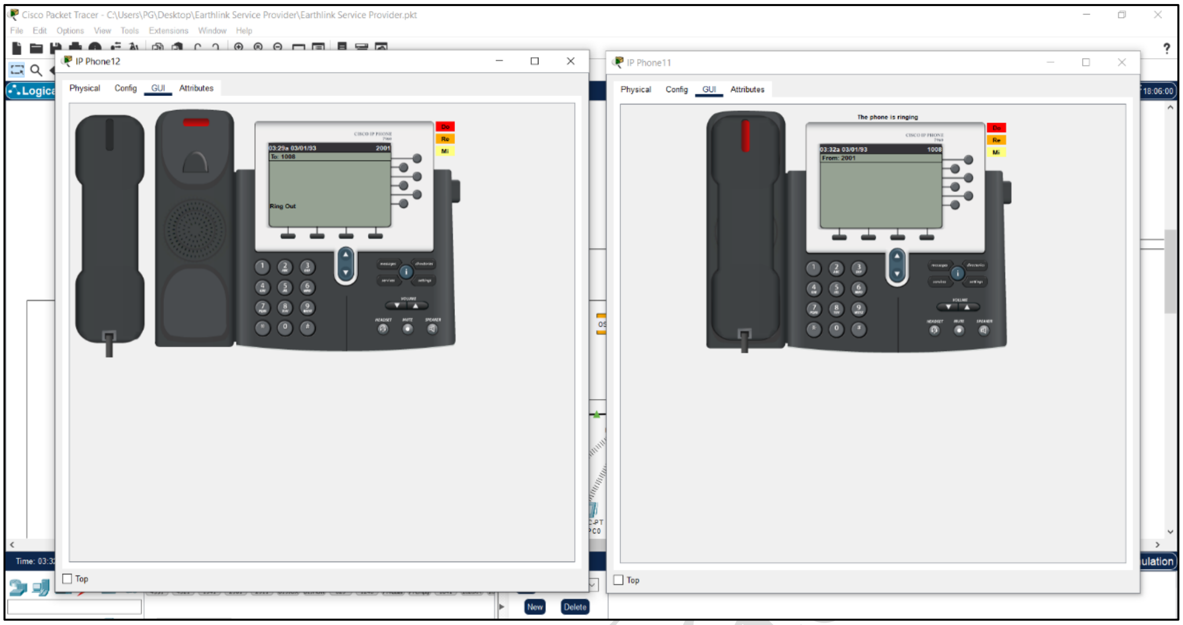
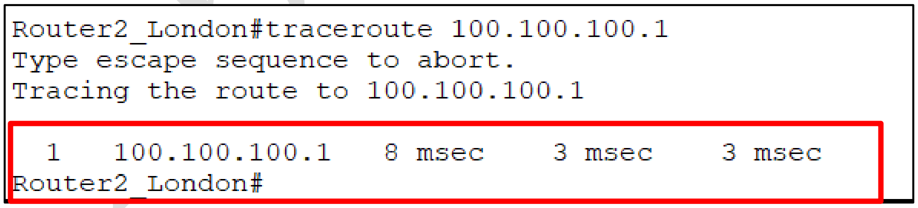

Cisco Packet Tracer - C:\Users\PG\Desktop\Earthlink Service Provider\Earthlink Service Provider.pkt
File Edit Options View Tools Extensions Window Help
IP Phone12
Physical Config GUI Attributes
Ring Out
IP Phone11
Physical Config GUI Attributes
The phone is ringing
From: 2001
Top
New
Delete

Figure 49 Telephone Service

I have successfully implemented the telephone service at the California branch. The importance of implemented the telephone service:

- Improved communication
- Customer service
- Operational efficiency
- Accessibility

6. VPN

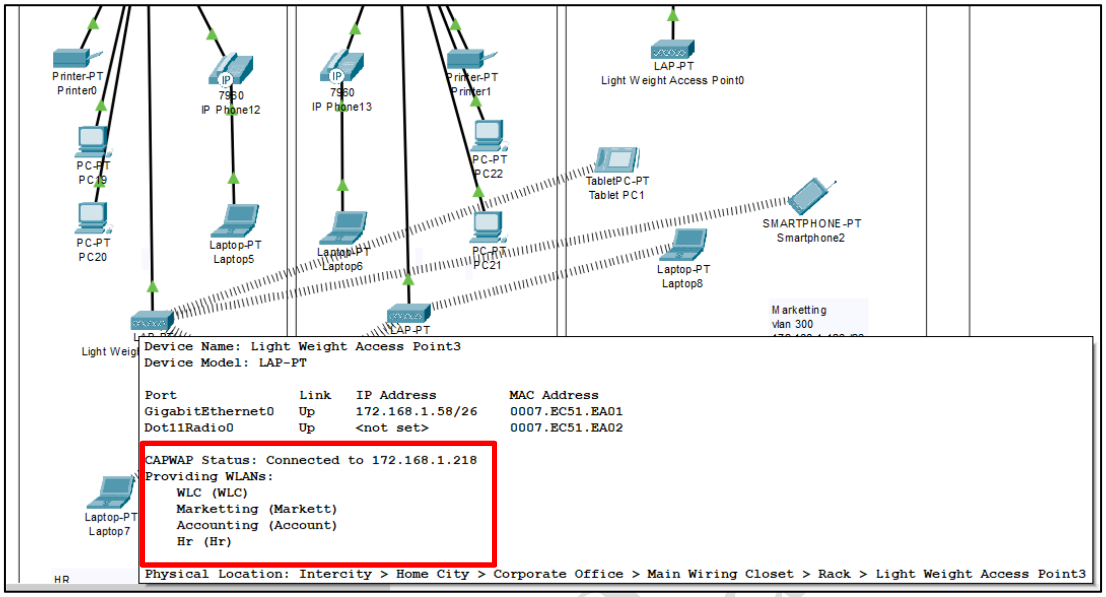


```
Router2_London#traceroute 100.100.100.1
Type escape sequence to abort.
Tracing the route to 100.100.100.1

  1   100.100.100.1   8 msec     3 msec     3 msec
Router2_London#
```

Figure 50 VPN

VPN testing is an essential step in the installation process that improves the network's overall security and functionality. It helps in identifying and mitigating possible hazards, ensuring a strong and reliable VPN solution for confidential communication.

7. WLC



```
Device Name: Light Weight Access Point3
Device Model: LAP-PT

Port             Link   IP Address         MAC Address
GigabitEthernet0  Up    172.168.1.58/26    0007.EC51.EA01
Dot11Radio0       Up    <not set>          0007.EC51.EA02

CAPWAP Status: Connected to 172.168.1.218
Providing WLANs:
    WLC (WLC)
    Marketting (Markett)
    Accounting (Account)
    Hr (Hr)
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Light Weight Access Point3
```

Figure 51 WLC

WLC stands for Wireless LAN Controller, a device used in wireless networking that controls access points (APs) and makes it easier for wireless clients and wired networks to communicate. The importance of implementing a WLC:

- Network performance
- Load Balancing
- Redundancy and failover
- Security
- Device compatibility

Conclusion

In conclusion, the project "Simulating Cyber Threats and Resilience: An Analysis of Network Security in EarthLink Service Provider" has provided valuable insights into the vulnerabilities and challenges within EarthLink's network infrastructure. Through the systematic simulation of cyber threats, critical weaknesses were identified, including a weak network design, compromised firewall health, and other vulnerabilities that contributed to the recent cyberattack and data loss. The analysis further revealed the importance of incorporating advanced cybersecurity technologies, such as intrusion detection systems and encryption protocols, to fortify the network and mitigate potential threats.

The project underscores the significance of addressing these issues, not only in terms of securing sensitive information but also in rebuilding client trust, which has been adversely affected by the recent cyber incident. By aligning EarthLink's network security with industry best practices and designing a framework that prioritizes both security and ease of management, the project aims to contribute to the overall resilience and operational efficiency of EarthLink Service Provider.

As the project concludes, the proposed recommendations and enhancements seek to empower EarthLink to optimize its network performance, enhance cybersecurity posture, and navigate the evolving landscape of cyber threats successfully. The insights gained from this research provide a foundation for ongoing efforts to strengthen network security, fostering a secure and resilient environment for EarthLink's operations in the telecommunications industry.

References

Bhat, A., June 22, 2022. [Online]
Available at: https://www.questionpro.com/blog/secondary-research/

Bouchrika, I., Jan 2, 2023. [Online]
Available at: https://research.com/research/how-to-write-research-methodology

franklin, D., 2 Aug, 2022. [Online]
Available at: https://www.geeksforgeeks.org/three-layer-hierarchical-model-in-cisco/

Malal, A., June 2021. [Online]
Available at: https://www.researchgate.net/figure/The-research-onion-according-to-Saunders-et-Al-2016-as-cited-in-Saunders-et-Al_fig6_343480486

Marklin, 2022. [Online]
Available at: https://www.open.edu/openlearn/money-business/using-data-aid-organisational-change/content-section-4.1

Mathews, Jan 20, 2024. [Online]
Available at: https://www.computernetworkingnotes.com/ccna-study-guide/access-distribution-and-core-layers-explained.html

Peter, 2022. [Online]
Available at: https://www.twingate.com/blog/ipsec

Stiward, L., 2022. [Online]
Available at: https://atlasti.com/research-hub/primary-secondary-data

Streefkerk., R., June 22, 2023. [Online]
Available at: https://www.scribbr.com/methodology/qualitative-quantitative-research/