**Documentation Overview**

**Network Diagram**

**A diagram of a network

Description automatically generated**

**Network Equipment**

1. **Router**
   * **Model**: Cisco ISR 4331
   * **Purpose**: Provides routing between VLANs, internet connectivity, and firewall capabilities.
2. **Multilayer Switch**
   * **Model**: Cisco 3560
   * **Purpose**: Handles inter-VLAN routing and connects to the router and other switches.
3. **Switches**
   * **Model**: Cisco 2960 (6 units)
   * **Purpose**: Provides Layer 2 connectivity for workstations and servers.
4. **Workstations**
   * **Total**: 10 computers
   * **Purpose**: User endpoints for various functions (Management, Study, Production, Support1, Support2).
5. **Servers**
   * **Total**: 3 servers
   * **Functions**:
     + **DNS Server**: Resolves domain names within the network.
     + **DHCP Server**: Dynamically assigns IP addresses to devices.
     + **iSCSI Storage Server**: Provides networked storage solutions.

**Estimated Costs for the Project**

**1. Router**

**Cisco ISR 4331 Router: €2,500**

**2. Switches**

**Multilayer Switch (Cisco 3560): €1,500**

**Access Switches (6 x Cisco 2960): €1,500 each**

**Total for Access Switches: €9000**

**3. Servers**

**DNS Server: €2,000**

**DHCP Server: €2,000**

**iSCSI Storage Server: €2,000**

**4. Workstations**

**Workstations (10 x €800): €8000 (10x €800)**

**Step 1: Define Network Structure**

* **Core Layer**: ISR 4331 Router
* **Distribution Layer**: Multilayer Switch (Cisco 3560)
* **Access Layer**: 6 x Cisco 2960 switches

**Step 2: VLAN Segmentation**

* **VLANs**:
  + VLAN 10: Management/Secretariat
  + VLAN 20: Study
  + VLAN 30: Production
  + VLAN 40: Support 1
  + VLAN 41: Support 2
  + VLAN 1: Servers

**Step 3: IP Addressing Scheme**

* **Subnetting**:
  + Each VLAN should have its own subnet.
  + Example:
    - VLAN 10: 192.168.10.10
    - VLAN 20: 192.168.20.10
    - VLAN 30: 192.168.30.10
    - VLAN 40: 192.168.40.10
    - VLAN 41: 192.168.41.10
    - VLAN 1: 192.168.1.1

**Step 4: Check the Connectivity**

* + - Ethernet cables are plugged in securely on all the computer and the router/switch.
    - Ipconfig(for windows) and ifconfig or ip addr show (for mac OS and Linux),These command displays IP address, subnet mask, and default gateway.
    - ping command to test connectivity to your router (ping router IP)
    - Accessing the ftp server
    - Getting the Ips from DHCP

**Step 5: Command and steps implemented in this process**

**Verify VLAN Configuration:**

Check VLANs with

Switch# show vlan brief

**X is number for Vlan 1,10,20,30,40,41**

**Abc – name of the Vlan**

**For each single layer access switch**

Switch>

Switch>enable

Switch#config terminal

Switch(config)#vlan x

Switch(config-vlan)#name Abc

Switch(config-vlan)#interface range FastEthernet0/1-FastEthernet0/8

Switch(config-if-range)#switchport access vlan x

**On access layer switch( On the interface from access switch to multilayer)**

Switch(config-if-range)#interface fastEthernet0/0

Switch(config-if)#switchport mode trunk

**On mutilayer switch (on the interface from multilayer to access switch)**

Switch>enable

Switch#Config terminal

Switch(config)#Interface f0/0

Switch(config-if)#Switchport trunk encapsulation dot1Q

Switch(config-if)#Switchport mode trunk

Switch(config-if)#Exit

Switch#Config terminal

Switch(config)#Vlan x

Switch(config-vlan)#Name abc

Switch(config-vlan)#Int vlan x

Switch(config-vlan)#Ip address 192.168.x.1 255.255.255.0

Switch(config-vlan)#No shut

Exit

#Ip routing

#Interface vlan 30

#Ip helper-address 192.168.1.2

**On router with connected interface**

#interface fa0/0 (the interface name)

#switchport mode trunk

#switchport trunk allowed vlan x

**Questions:**

**. Why did you choose to use VLANs instead of a physical DMZ setup?**

• **Answer**: VLANs allow us to logically separate network segments within the same physical infrastructure, which reduces costs while still providing effective isolation. By using ACLs, we can restrict access between VLANs, creating a “virtual” DMZ that prevents unauthorized access to sensitive internal resources without needing additional physical firewall hardware.

**2. How does RADIUS improve security on the network?**

• **Answer**: RADIUS centralizes user authentication, ensuring that access to critical devices is only granted after verification through a secure, centralized server. This reduces the chance of unauthorized access by enforcing strong password policies and simplifying account management. If a device is compromised, credentials aren’t stored locally, further protecting the network.

**3. How does the network handle IP addressing, and why did you choose to use a DHCP server?**

• **Answer**: We implemented a centralized DHCP server to automatically assign IP addresses within each VLAN, simplifying network management. This reduces the chance of IP conflicts and eases maintenance, as the server can handle address distribution dynamically, especially useful as the network scales or devices are added.

**4. Why is it important to segment different departments into separate VLANs?**

• **Answer**: Segmentation improves security by isolating traffic between departments, reducing the risk of sensitive data exposure across sectors. For example, the Management/Secretariat sector handles potentially confidential information that shouldn’t be accessible from Study or Production. VLANs also optimize network performance, as each sector’s traffic is managed separately.

**5. What measures are in place to protect the iSCSI storage server?**

• **Answer**: The iSCSI server is protected by VLAN segmentation and ACLs, allowing only authorized devices to access it. Additionally, RADIUS authentication ensures that only verified users can access network resources, which adds a layer of security to the storage server. In practice, data between the iSCSI and end devices could also be encrypted to prevent unauthorized data interception.

**6. How will the network scale if the client adds more workstations or new departments?**

• **Answer**: The VLAN structure allows us to scale easily by adding new workstations within existing IP ranges or creating additional VLANs if new departments are added. Since we’re using a DHCP server, we don’t need to manually assign IP addresses for new devices, making expansion straightforward and efficient.

**7. Why did you choose Cisco Packet Tracer for the simulation?**

• **Answer**: Cisco Packet Tracer is widely used in network design for its ease of use and ability to simulate network components like switches, routers, and ACLs effectively. Although some advanced features are limited, it supports core functions like VLANs, ACLs, DHCP, and RADIUS, which are essential to our design.

**8. What specific security threats does this network design address?**

• **Answer**: Our design addresses several threats, including unauthorized access, data breaches, and traffic interception. VLANs and ACLs limit access between departments, reducing the risk of insider threats. RADIUS protects against unauthorized access to network devices, and centralized DHCP and DNS services reduce the chances of IP spoofing or DNS poisoning within the network.

**9. How do ACLs help secure the DMZ?**

• **Answer**: ACLs control which types of traffic are allowed into and out of the DMZ, preventing unauthorized users from accessing sensitive resources within the internal network. For instance, only necessary services such as web and email servers are accessible externally, while all other services are restricted. This minimizes the attack surface available to external threats.

**10. Why is documentation so important for this network design?**

• **Answer**: Clear documentation ensures future maintainability, as it provides a detailed record of configurations, IP addressing, and security protocols. This is especially valuable if new IT staff are introduced or if changes are needed. Good documentation also helps troubleshoot issues more effectively and maintain consistent security practices.

**11. What cost-saving measures did you implement without compromising security?**

• **Answer**: We optimized costs by using VLANs instead of physical separation for the DMZ and by centralizing services like DHCP and DNS, reducing the need for multiple servers. Cisco Packet Tracer also allowed us to simulate the network design without investing in physical devices during the planning phase, ensuring cost-effective decision-making before any purchase.

**12. How does this network design ensure compliance with future growth?**

• **Answer**: The VLAN and DHCP configuration enables easy scaling by adding more IP address ranges or VLANs as needed. With centralized RADIUS authentication, adding new users and devices can be managed centrally, making the network highly adaptable without major reconfiguration. This flexibility ensures that future growth won’t require a complete redesign.

**13. How would this design handle remote access, if required?**

• **Answer**: Although remote access wasn’t a specified requirement, we could expand the design by integrating a VPN for secure remote access. RADIUS would further secure this setup, verifying remote user credentials. VPN access would allow external connections to specific VLANs without compromising internal network security.

**14. Why did you opt for centralized services rather than distributed ones?**

• **Answer**: Centralized services for DHCP, DNS, and RADIUS simplify management and ensure consistent configurations across the network. This approach reduces redundancy and simplifies updates, making it easier to enforce security policies and monitor the network from a single point, which is especially beneficial for smaller networks like this one.

**15. How are backup and disaster recovery addressed in this design?**

• **Answer**: Although specific backup requirements weren’t mentioned, our design recommends regular configuration backups for all network devices, especially for routers and switches. The iSCSI storage server can also be backed up periodically. In a production environment, we could include an offsite or cloud-based backup solution to ensure data recoverability in case of disaster.

These questions will help you be well-prepared to address different aspects of your network design, from technical details to justifications for security and scalability decisions. Let me know if you’d like more on any specific area!