Cyber Security - KamKar

Project : Network Plan

\

Mohamed - Sinan - Sami

BeCode 2024

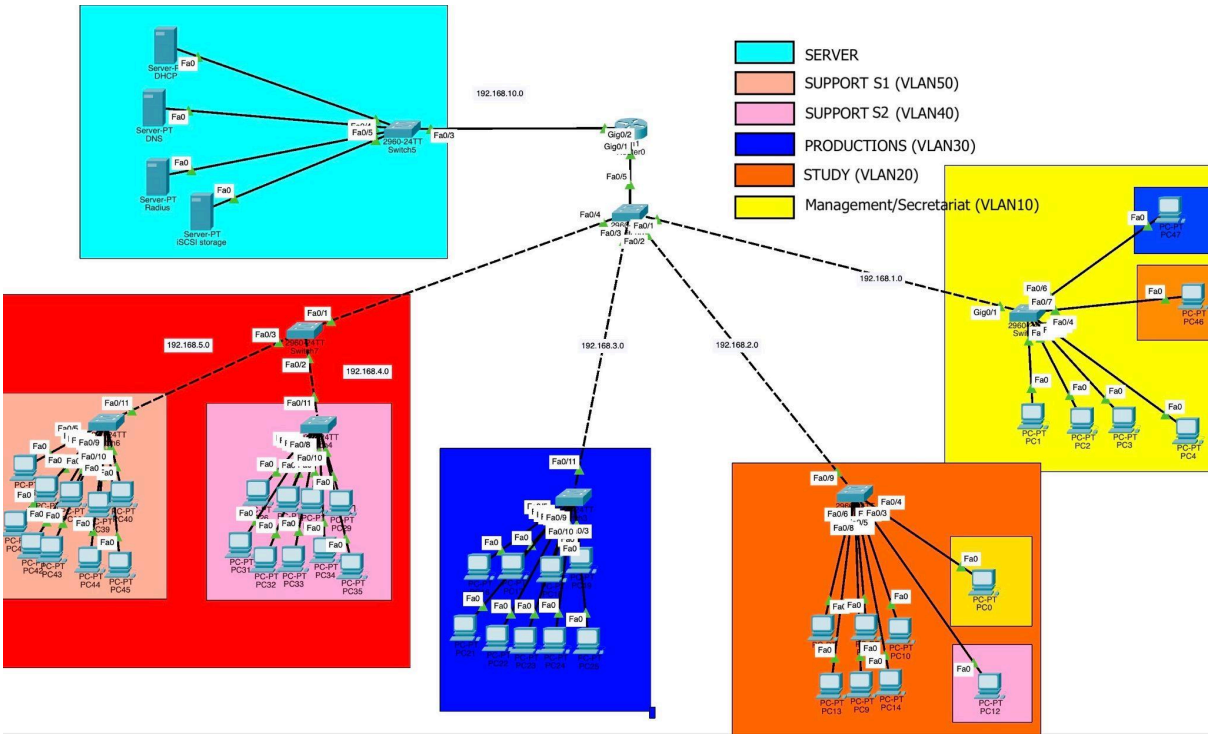
Table of contents

Network diagram with annotations

Our network is organized into distinct sectors for efficiency and security.
The server sector consists of 4 servers connected to a switch, which is then linked to a router.
This router also connects to another switch that serves four other sectors. Each sector is designed for specific functions and is equipped with its own switch and workstations:

Management/Secretariat has 5 workstations on VLAN10,
Study has 8 workstations on VLAN20,
Production has 10 workstations on VLAN30,
and Support is divided into two sectors, each with 10 workstations on VLAN40 and VLAN50, respectively.

This structure ensures a clear, organized network setup, facilitating both management and security.



IP addressing table per sector and VLAN (if used).

Sector	VLAN	Device Type	IP Address	Subnet Mask	Default Gateway
Management	10	Workstation	192.168.10.X	255.255.255.0	192.168.1.1
Study	20	Workstation	192.168.20.X	255.255.255.0	192.168.2.1
Production	30	Workstation	192.168.30.X	255.255.255.0	192.168.3.1
Support	40	Workstation	192.168.40.X	255.255.255.0	192.168.4.1
Support	50	Workstation	192.168.50.X	255.255.255.0	192.168.5.1
Servers	-	DNS	192.168.10.5	255.255.255.0	192.168.10.1
Servers	-	DHCP	192.168.10.10	255.255.255.0	192.168.10.1
Servers	-	Radius	192.168.10.15	255.255.255.0	192.168.10.1
Servers	-	iSCSI	-	-	-
-	10	Router	G0/1	192.168.10.1	255.255.255.0
-	20	Router	G0/2	192.168.20.1	255.255.255.0
-	30	Router	G0/3	192.168.30.1	255.255.255.0
-	40	Router	G0/4	192.168.40.1	255.255.255.0
-	50	Router	G0/5	192.168.50.1	255.255.255.0

Configuration details for key devices.

Routers

Routers connect different networks together, routing packets from one network to another based on their IP addresses.

- Interfaces: Configure IP addresses and subnet masks for each interface that connects to different segments of the network. This might include LAN, WAN, and management interfaces.
- Routing Protocols: Set up routing protocols (e.g.,DHCP) to dynamically learn and share routing information with other routers, or configure static routes to specify fixed paths for traffic between networks.
- ACLs (Access Control Lists): Implement ACLs to control what traffic can enter or leave the network through the router, enhancing security.

Switches

Switches connect devices within the same network, using MAC addresses to forward data to the correct destination.

- Port Configuration: Assign ports to specific VLANs (Virtual Local Area Networks) to segment network traffic, configure port speeds, and set up duplex modes.
- VLANs: Define VLANs to segment the network into smaller, isolated groups to improve performance and security.
- Port Security: Configure port security features to limit the number of MAC addresses allowed on a port or to restrict port access to specific MAC addresses.

Explanation of security measures and their purpose.

Cable Management

Our network security is streamlined and effective. We use a single cable to connect our router to the network, with specific ports for different areas: G0/0 for external WAN access, G0/1 for internal LAN use, and G0/2 for our servers.

This setup simplifies security management by clearly separating network segments, making it easier to monitor and protect our data and resources.

Vlan

Used to simulate the segmentation of networks into isolated subnetworks within the same physical infrastructure.

This allows learners to understand how VLANs enhance network efficiency, security, and manageability by logically separating devices despite their physical connections.
Through VLAN configuration exercises, users can see firsthand how traffic is managed and isolated, how broadcast domains are limited to improve network performance, and how VLANs support the implementation of security policies by segregating sensitive data traffic from general network traffic.

This simulation experience is crucial for mastering network design and management principles in complex environments.

Access list

They allow users to define rules that permit or deny traffic based on IP addresses, protocols, and ports, offering a practical way to understand and implement network security measures, control traffic flow, and enforce policy compliance.

By integrating access lists into simulations, learners can explore the impact of various security configurations on network performance and security, gaining valuable insights into effective network management practices.

Cross-Departmental Redundancy

In a strategic approach to enhance network resilience and ensure departmental service availability, organizations implement a cross-departmental redundancy plan.

This involves placing one or more hosts from each department into the network segments of other departments.

Such a setup guarantees that, in the event of a network failure affecting one department, critical services and connectivity can still be maintained through these strategically placed hosts.

This method not only bolsters the network's overall reliability but also facilitates uninterrupted operations, as these inter-departmental hosts can take over the necessary functions temporarily.

This redundancy plan is a proactive measure to mitigate downtime and maintain seamless service across the organization.

Radius Authentication

Used to simulate the integration of network access control with a centralized authentication mechanism.

This allows for the demonstration of how networks can securely manage user access to devices and services through a single authentication source.

By configuring RADIUS in simulations, users can explore the principles of AAA (Authentication, Authorization, and Accounting), understand the benefits of centralized authentication, and see how it enhances network security by ensuring that only authorized users can access network resources.

This practical experience is invaluable for grasping the complexities of managing secure access in real-world networks.

Cost breakdown of network components.

Device Type	Model	Quantity	Unit Price	Total Price
Server	Server PT	4	2000	8000$
Switch	2960 IOS 15	9	1500	13500$
Router	2911	1	895	895$
PC	PC-PT	43	1000	43000$
				-10%
				58.855$

Thank you