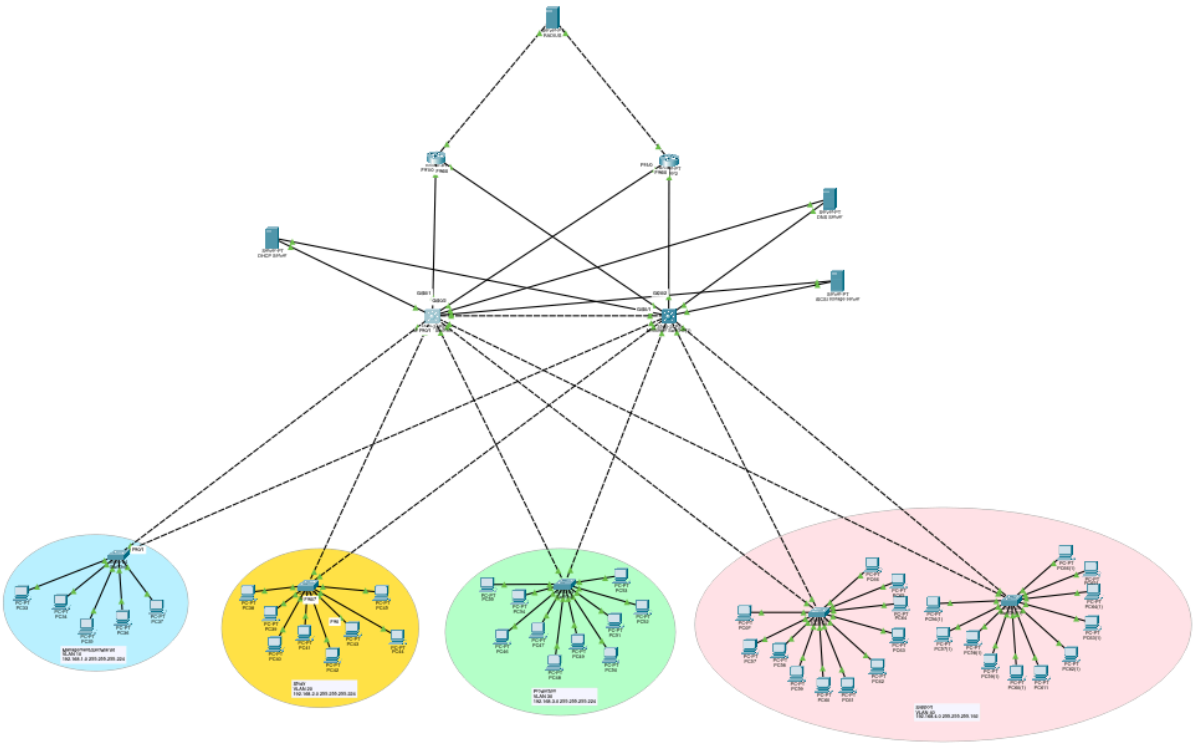


Why 2 Tier Architecture:

Simplicity: A 2-tier architecture is generally simpler to design, deploy, and manage compared to more complex architectures. This can reduce the workload for network administrators.

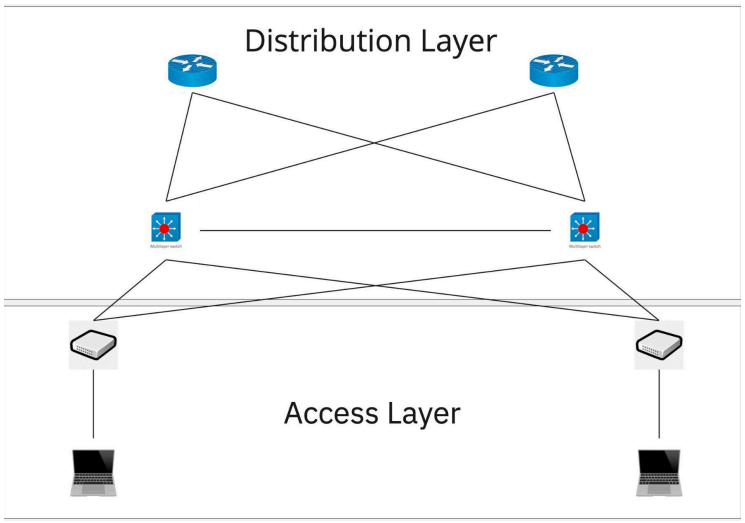
Improved Performance: With fewer intermediate levels, communications between different network elements can be faster and more efficient, enhancing overall network performance.

Scalability: This architecture is often easier to scale as it is less complex. Adding new nodes or devices may be simpler and require fewer modifications.

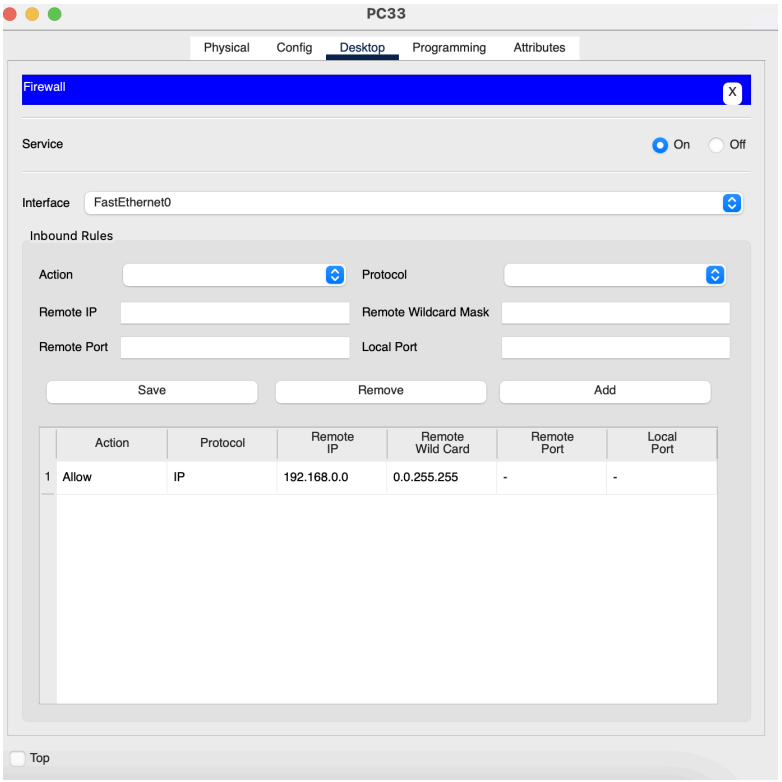
Reduced Cost: Less network hardware and software are required in a 2-tier architecture compared to more complex architectures, which can lower purchasing, maintenance, and upgrade costs.

Ease of Troubleshooting: Fewer tiers often make troubleshooting simpler because there are fewer potential points of failure and data paths are more direct.

Better Security: With fewer intermediate layers, it can be easier to establish and manage consistent security policies across the entire network.



Firewall on the PCs:



IPv4 firewalls on PCs in a two-tier architecture enhances network security by providing host-level protection, controlling traffic flows, preventing internal malware propagation, and enforcing customized security policies. This helps strengthen the overall network security posture and reduces the risks of attacks and security incidents.

Switch L2 security configuration:

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#hostname SwitchM/S
SwitchM/S(config)#line console 0
SwitchM/S(config-line)#password Group
SwitchM/S(config-line)#login
SwitchM/S(config-line)#exit
SwitchM/S(config)#
SwitchM/S(config)#enable password Group
SwitchM/S(config)#no ip domain-lookup
SwitchM/S(config)#service password-encryption
SwitchM/S(config)#exit
SwitchM/S#
%SYS-5-CONFIG_I: Configured from console by console

SwitchM/S#
```

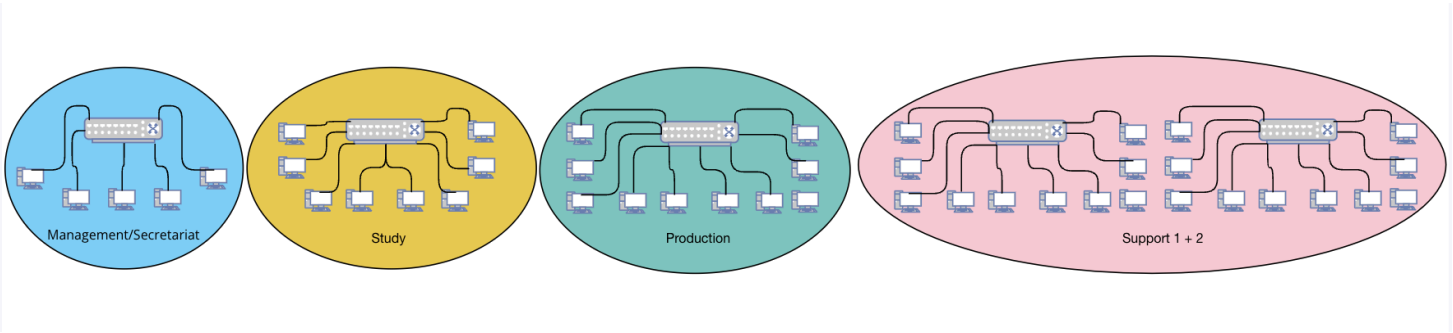
- `enable`: This command moves from user mode (EXEC mode) to privileged mode (privileged EXEC mode), which provides full access to all configuration and diagnostic commands of the switch.
- `conf t`: This command moves from privileged EXEC mode to global configuration mode, where you can configure the switch's global settings.
- `hostname SwitchM/S`: This command sets the hostname of the switch to "SwitchM/S".
- `line console 0`: This command selects console line 0, which is the physical console connection on the switch.
- `password Group`: This command configures a password "Group" for logging into the console line.
- `login`: This command enables the password requirement for logging into the console line.
- `exit`: This command exits the console line configuration mode and returns to global configuration mode.
- `enable password Group`: This command configures a password "Group" for accessing privileged EXEC mode.
- `no ip domain-lookup`: This command disables IP domain name lookup. This prevents the switch from looking up domain names when entering invalid commands.
- `service password-encryption`: This command enables automatic encryption of passwords stored in the switch configuration. This secures passwords by encrypting them in the configuration, making them unreadable in plaintext.

VLANs:

VLANs provide a layer of security by isolating traffic between different VLANs. Access control lists (ACLs) and other security measures can be implemented to control traffic flow between VLANs, allowing control over network access and minimizing the risk of unauthorized access.

Implementing VLANs in a two-tier architecture helps enhance network security, optimize resource utilization, improve network performance, and simplify network management.

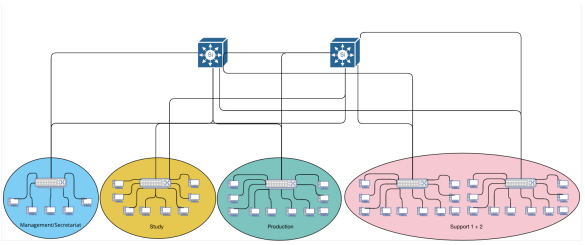
VLAN Name	VLAN	IP range
Vlan10-Management/Secretariat	10	192.168.1.0/27
Vlan20-Study	20	192.168.2.0/27
Vlan30-Production	30	192.168.3.0/27
Vlan40-Support	40	192.168.4.0/26



Switch L3 security configuration:

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#Ip domain-name groupproject.com
Switch(config)#Username admin secret Group-Project
Switch(config)#Crypto key generate rsa
% Please define a hostname other than Switch.
Switch(config)#1024
               ^
% Invalid input detected at '^' marker.

Switch(config)#Ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
Switch(config)#Line vty 0 15
Switch(config-line)#Transport input ssh
Switch(config-line)#
Switch(config-line)#
```



Advantages of SSH:

Enhanced Security: SSH provides data encryption during communication between the administrator and the switch, significantly reducing the risks of security breaches and tampering with sensitive data.

Secure Remote Access: By using SSH, administrators can securely access the L3 switch remotely. This enables efficient network management even from remote locations without compromising security.

Centralized Management: By using SSH to access multiple L3 switches from a centralized console, administrators can streamline and centralize network management, facilitating monitoring, configuration, and maintenance.

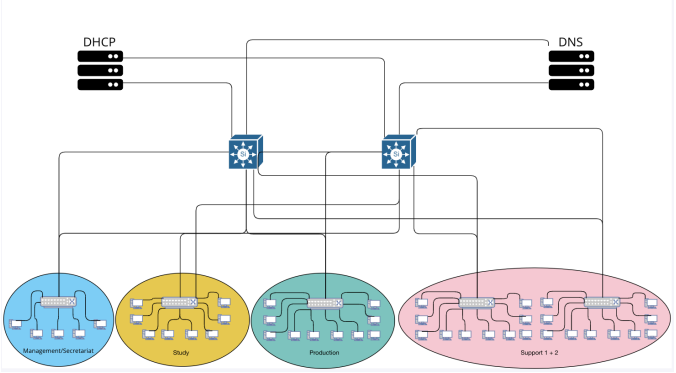
Audit and Traceability: Utilizing SSH allows tracking and auditing of administrative activities on the L3 switch, which is crucial for regulatory compliance and security best practices.

Protection against Network Eavesdropping Attacks: With SSH, authentication and management information are encrypted, guarding against network eavesdropping attacks where data can be intercepted and compromised.

Integration with Existing Security Policies: SSH can be integrated with other existing network security policies.

Using SSH on a Layer 3 switch in a two-tier network architecture is a recommended practice to enhance security, enable secure remote access, and facilitate centralized network management.

DHCP and DNS server:



Advantages of DHCP server:

Simplified Management: A centralized DHCP server streamlines IP address management on the network. Instead of manually configuring each device with a static IP address, the DHCP server can dynamically assign IP addresses to devices connecting to the network.

Scalability: A DHCP server can easily scale to accommodate a growing number of devices on the network. It typically involves adjusting the available IP address range and configuration settings on the DHCP server.

Elimination of IP Address Conflicts: By automatically assigning IP addresses to devices on the network, the DHCP server reduces the risk of IP address conflicts, which can occur when a manually assigned IP address overlaps with another device.

Centralized Management of Network Settings: In addition to assigning IP addresses, a DHCP server can also provide other essential network settings such as default gateway addresses, DNS servers, and WINS servers, facilitating centralized management of network configuration.

Reduction of Configuration Errors: By automating the IP address assignment process, a DHCP server reduces the risk of human configuration errors that may occur when manually configuring IP addresses on each device.

Management of Temporary IP Addresses: A DHCP server can be configured to assign temporary IP addresses with a defined lease duration. This allows for efficient management of IP addresses in environments where devices frequently connect and disconnect from the network.

Deploying a DHCP server in a two-tier architecture simplifies IP address management, enhances operational efficiency, and reduces the risk of configuration errors on the network.

Advantages of DNS server:

Name Resolution: A DNS server translates domain names into IP addresses, enabling devices on the network to communicate with each other using human-readable domain names instead of numeric IP addresses. This simplifies network administration and makes it easier for users to access resources by name.

Centralized Management: A DNS server allows for centralized management of domain name resolution within the network. Administrators can configure and maintain DNS records from a single location, ensuring consistency and accuracy across the network.

Redundancy and Fault Tolerance: By deploying multiple DNS servers in the network, redundancy and fault tolerance can be achieved. If one DNS server fails, other servers can continue to resolve domain names, ensuring uninterrupted network connectivity and access to resources.

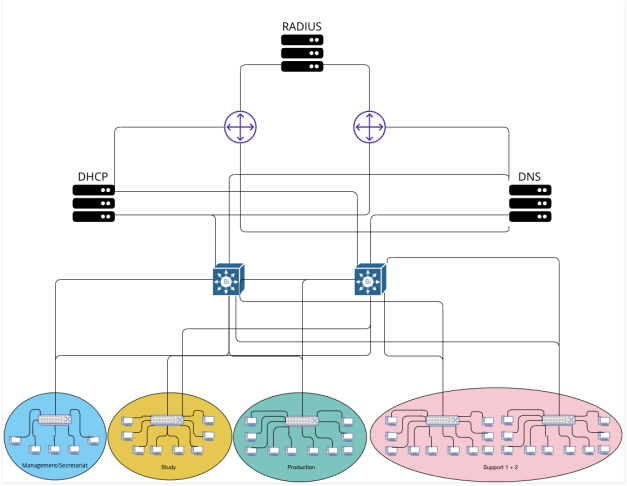
Improved Performance: DNS caching can help improve network performance by storing recently resolved domain name-to-IP address mappings. This reduces the need to query external DNS servers for frequently accessed resources, resulting in faster response times and reduced network latency.

Security: DNS servers can be configured to enforce security policies and filter out malicious or unauthorized DNS queries. Additionally, DNSSEC (DNS Security Extensions) can be implemented to provide cryptographic authentication and integrity verification of DNS data, mitigating the risk of DNS spoofing and other attacks.

Private DNS Zones: In a two-tier architecture, organizations may have internal resources or services that are not publicly accessible. A DNS server allows for the creation of private DNS zones, enabling internal users to access these resources using domain names while keeping them hidden from the public Internet.

Overall, integrating a DNS server into a two-tier architecture enhances name resolution, simplifies network management, improves performance, enhances security, and enables access to internal resources using domain names.

Routeur security configuration with RADIUS server:



Advantage of Radius Server:

Centralized Authentication and Authorization: A RADIUS server centralizes the authentication, authorization, and accounting (AAA) process. This means that users can be centrally authenticated regardless of their physical location when connecting to the network.

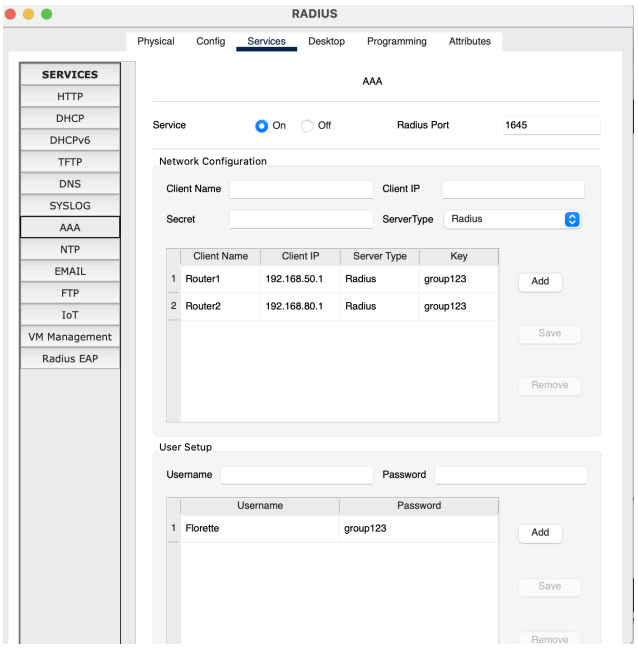
Enhanced Security: By using a RADIUS server for authentication, user credentials are encrypted when transmitted over the network. Additionally, RADIUS servers can support robust authentication protocols such as EAP-TLS, EAP-TTLS, or PEAP, thus enhancing the security of network connections.

Granular Access Control: A RADIUS server enables the implementation of granular access policies based on attributes such as user identity, group membership, connection time, etc. This allows for precise control over user access rights to network resources.

Centralized Account Management: With a RADIUS server, user account information (usernames, passwords, authorization attributes, etc.) can be centrally managed, simplifying user management and access permissions.

Integration with Other Network Services: RADIUS servers can be integrated with other network services such as VPN servers, Ethernet switches, wireless access points, etc., providing a consistent and centralized authentication and authorization solution for the entire network.

Traceability and Auditability: RADIUS servers provide detailed audit logs, allowing administrators to track and audit authentication and authorization activities on the network. This is crucial for regulatory compliance and network security.




```
Enable
Conf t
aaa new-model
aaa authentication login default group
radius local
radius-server host 192.168.80.2 auth-port
1645 key group123
Line vty 0 15
login authentication default
```

`enable`: This command puts the user in privileged EXEC mode, allowing access to all commands on the switch.
`conf t`: This command enters global configuration mode, where you can configure global parameters for the switch.
`aaa new-model`: This command enables the AAA (Authentication, Authorization, and Accounting) framework on the switch.
`aaa authentication login default group radius local`: This command configures authentication for login sessions. It specifies that the switch should first attempt RADIUS authentication (specified by the "radius" keyword), and if that fails, it should fall back to local authentication. The "default" keyword specifies that this is the default authentication method.
`radius-server host 192.168.80.2 auth-port 1645 key group123`: This command configures the RADIUS server with the IP address "192.168.80.2", the authentication port "1645", and the shared secret key "group123".
`line vty 0 15`: This command enters line configuration mode for the virtual terminal (vty) lines, which are used for remote management access.
`login authentication default`: This command specifies that the default authentication method configured earlier (RADIUS followed by local authentication) should be used for login authentication on the vty lines.

Costs:

Switch 2950-24 (x5):
new: from $100 to $500 USD. However, that price range might vary based on the vendor, any bundled services, and other factors.

Used or Refurbished: from $20 to $200 USD, depending on factors such as condition, age, and included accessories.

It's worth noting that Cisco offers several variants and series of switches, each with its own features and prices. The 2950-24 is an older model, so it may be cheaper than newer models.

Switch 3560-24PS (x2):

New: $500 to $1500 USD. Prices may vary based on the vendor, any bundled services, warranty coverage, and other factors.

Used or Refurbished: from $100 to $500 USD, depending on factors such as condition, age, and included accessories.