Robust Enterprise Network Infrastructure: Design and Configuration

11 / 2025

This presentation details the design and configuration of a multi-department network infrastructure focused on efficiency, security, and redundancy. I utilize VLAN segmentation, dynamic routing (OSPF), and centralized AAA/TACACS+ authentication.

Network Topology Overview

R3 Router
Forms triangle mesh; attaches to switch bank

R1 Router
Connects to R2 and R3 via serial links

R2 Router
Peers with R1 and R3; local VLAN switch

Key Router Identifiers

Router Name	Interface to Switch	Interface Serial to router	Loop
R1	172.16.1.1/30	10.10.1.1 & 10.10.1.10	10.255.255.1/32
R2	172.16.2.1/30	10.10.1.2 & 10.10.1.5	10.255.255.2/32
R3	172.16.3.1/30	10.10.1.6 & 10.10.1.9	10.255.255.3/32

The core network design utilizes a triangular topology connecting R1, R2, and R3 via serial links to ensure redundancy and efficient routing. From R1, the network extends to local area networks via GigabitEthernet, incorporating VLAN subinterfaces for logical segmentation.

VLAN Configuration & Inter-VLAN Routing

Router-on-a-Stick VLAN Routing

Router Trunk Link
Single physical Ethernet link with 802.1Q trunking

Subinterfaces
Logical subinterfaces per VLAN for inter-VLAN routing

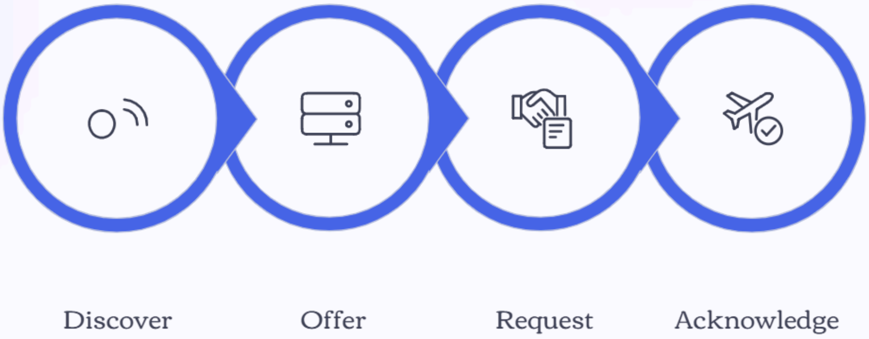
Access Switch
Switch ports assigned to VLANs forwarding tagged frames

Client Devices
Hosts connected to switch on VLAN 10, 20, 30

802.1Q encapsulation is crucial for enabling multiple VLANs to share a single physical link between a router and a switch. This process tags Ethernet frames with a VLAN ID, allowing the switch to direct traffic to the correct VLAN and the router to distinguish traffic belonging to different VLANs.

VLAN ID	Department	Network	Gateway
10	Receptionist	192.168.1.0/24	192.168.1.1
20	Logistics	192.168.2.0/24	192.168.2.1
30	Sales	192.168.3.0/24	192.168.3.1
40	HR	192.168.4.0/24	192.168.4.1
50	Finance	192.168.5.0/24	192.168.5.1
60	Store	192.168.6.0/24	192.168.6.1
70	Admin/Server	192.168.7.0/24	192.168.7.1
80	IT	192.168.8.0/24	192.168.8.1

DHCP Configuration & Address Management



Discover

Offer

Request

Acknowledge

Dynamic Host Configuration Protocol (DHCP) plays a critical role in automatically assigning IP addresses and other network configuration parameters to devices. In our segmented network, DHCP works seamlessly with subinterfaces and inter-VLAN routing to ensure that each VLAN receives the correct IP settings. The 'Router-on-a-Stick' configuration, where a single physical interface on the router handles multiple VLANs via subinterfaces, allows the router to act as the DHCP server for each VLAN, responding to requests that are forwarded across the trunk link from the switch. This process ensures that devices in each VLAN automatically obtain an IP address, default gateway, and DNS server information, streamlining network management and device onboarding.

Below are the DHCP pool configurations for R1, demonstrating the settings for receptionist, logistics, and sales VLANs:

Pool Name	Network	Default Router	DNS Server	Excluded Range
VLAN_10_Receptionist	192.168.1.0/24	192.168.1.1	8.8.8.8	192.168.1.1-192.168.1.10
VLAN_20_Logistics	192.168.2.0/24	192.168.2.1	8.8.8.8	192.168.2.1-192.168.2.10
VLAN_30_Sales	192.168.3.0/24	192.168.3.1	8.8.8.8	192.168.3.1-192.168.3.10

Key Configuration Snippets on R1

These snippets illustrate the command-line interface (CLI) commands used to configure DHCP exclusions and pools on R1.

DHCP IP Address Exclusions (Example)

```
ip dhcp excluded-address 192.168.1.1
192.168.1.10
ip dhcp excluded-address 192.168.2.1
192.168.2.10
! ... (similar exclusions for other VLANs)
```

DHCP Pool Configuration (Example for VLAN 10)

```
ip dhcp pool VLAN_10_Receptionist
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 8.8.8.8
```

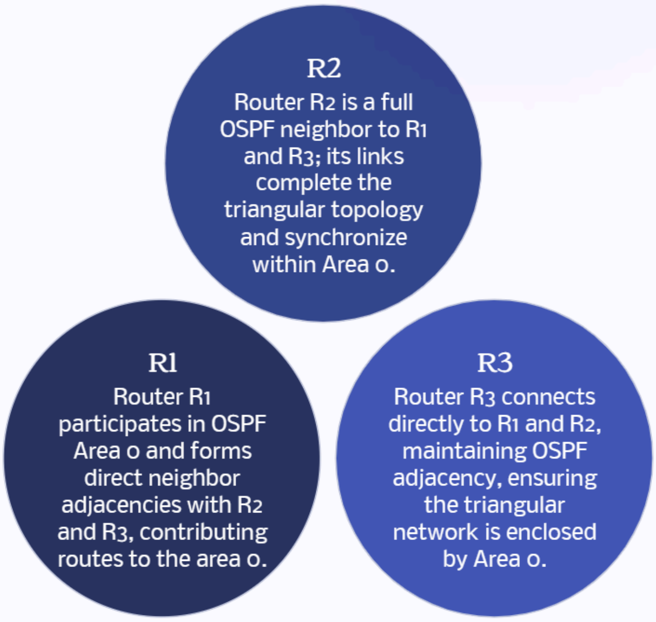
DHCP Pool Configuration (Example for VLAN 20)

```
ip dhcp pool VLAN_20_Logistics
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
 dns-server 8.8.8.8
```

DHCP Pool Configuration (Example for VLAN 30)

```
ip dhcp pool VLAN_30_Sales
 network 192.168.3.0 255.255.255.0
 default-router 192.168.3.1
 dns-server 8.8.8.8
```

OSPF Dynamic Routing Configuration



R2

Router R2 is a full OSPF neighbor to R1 and R3; its links complete the triangular topology and synchronize within Area 0.

R1

Router R1 participates in OSPF Area 0 and forms direct neighbor adjacencies with R2 and R3, contributing routes to the area 0.

R3

Router R3 connects directly to R1 and R2, maintaining OSPF adjacency, ensuring the triangular network is enclosed by Area 0.

Open Shortest Path First (OSPF) is an interior gateway protocol (IGP) used for routing within an autonomous system. It establishes neighbor relationships and exchanges routing information to build a complete topology map of the network. This section details the OSPF configuration for Router 1 (R1), focusing on network advertisements and the importance of loopback interfaces.

Below is a detailed table outlining the OSPF network advertisements for R1, specifying the network addresses, wildcard masks, and their association with Area 0:

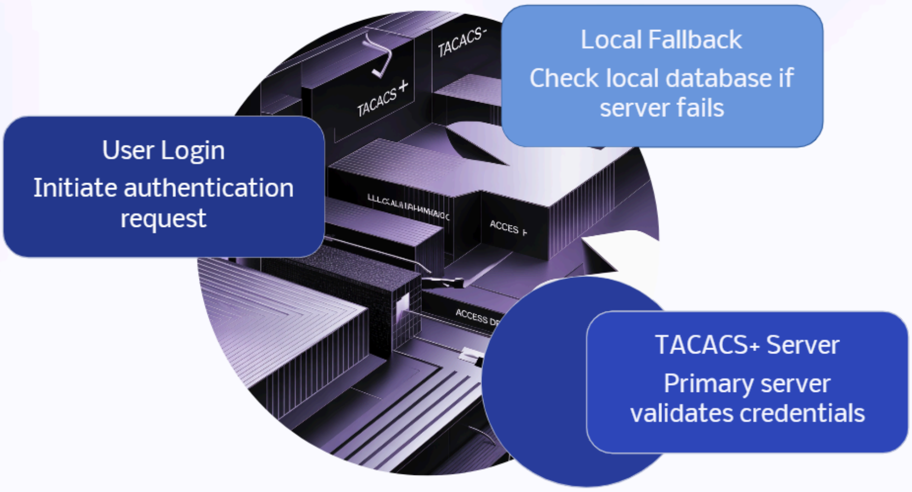
Description	*Network*	*Wildcard Mask*	*Area*
VLAN 10 Receptionist	*192.168.1.0*	*0.0.0.255*	*0*
VLAN 20 Logistics	*192.168.2.0*	*0.0.0.255*	*0*
VLAN 30 Sales	*192.168.3.0*	*0.0.0.255*	*0*
Serial link network	*10.10.0.0*	*0.0.0.3*	*0*
Serial link network	*10.10.0.8*	*0.0.0.3*	*0*
Serial link network	*10.10.1.0*	*0.0.0.3*	*0*
Serial link network	*10.10.1.8*	*0.0.0.3*	*0*
Loopback network	*10.255.255.0*	*0.0.0.255*	*0*

The following OSPF configuration is implemented on R1 to establish dynamic routing capabilities across the network:

```
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.3.0 0.0.0.255 area 0
 network 10.10.0.0 0.0.0.3 area 0
 network 10.10.0.8 0.0.0.3 area 0
 network 10.10.1.0 0.0.0.3 area 0
 network 10.10.1.8 0.0.0.3 area 0
 network 10.255.255.0 0.0.0.255 area 0
```

Loopback interfaces are crucial for OSPF as they provide a stable and always-up interface for the OSPF router-ID. Since loopback interfaces are logical and not tied to physical hardware, they remain active even if physical interfaces go down, ensuring the OSPF process maintains a consistent router-ID and does not destabilize neighbor relationships or routing table calculations. This enhances the overall stability and reliability of the OSPF routing domain.

AAA & TACACS+ Security Implementation



User Login
Initiate authentication request

Local Fallback
Check local database if server fails

TACACS+ Server
Primary server validates credentials

Authentication, Authorization, and Accounting (AAA) is a security framework that controls who can access the network, what they can do, and tracks their actions. TACACS+ (Terminal Access Controller Access Control System Plus) is a Cisco proprietary protocol that provides centralized authentication, authorization, and accounting services, offering more flexibility and reliability than RADIUS for device administration. This implementation focuses on configuring AAA on Router(R1, R2 and R3) to leverage TACACS+ for primary authentication with a local fallback mechanism for emergency access.

Below is a detailed table outlining the R1 AAA configuration, including commands and descriptions for each element:

Command	Description
`aaa new-model`	Enables the new AAA model on the device.
`aaa authentication enable default group tacacs+ enable`	Configures TACACS+ for privileged EXEC mode authentication, with local enable password as fallback.
`aaa authentication login myauth1 group tacacs+ local`	Defines a login authentication method list named 'myauth1', prioritizing TACACS+, then local users.
`tacacs-server host 192.168.7.10 key MyKey3`	Specifies the IP address of the TACACS+ server and the shared secret key for communication.
`username r1admin privilege 15 secret cisco123`	Creates a local user account for emergency access with full administrative privileges.

`line con 0`
`login authentication myauth1`
	Applies the 'myauth1' authentication list to the console line for local access.

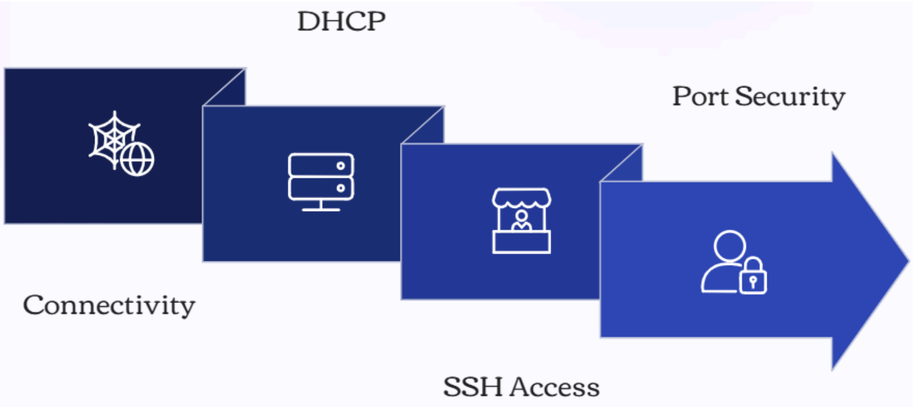
`line vty 0 4`
`login authentication myauth1`
	Applies the 'myauth1' authentication list to virtual terminal lines for remote access (Telnet/SSH).

The following configuration commands are implemented on R1 to establish the AAA and TACACS+ security:

```
R1(config)# aaa new-model
R1(config)# ! --- TACACS Server Host Configuration ---
R1(config)# tacacs-server host 192.168.7.10 key MyKey3
R1(config)#
R1(config)# ! --- Local Fallback Credentials ---
R1(config)# enable secret cisco123
R1(config)# username r1admin privilege 15 secret cisco123
R1(config)# ! --- VTY/SSH Login Authentication (TACACS+ then Local) ---
R1(config)# aaa authentication login myauth1 group tacacs+ local
R1(config)# ! --- Enable Mode Authentication (TACACS+ then Enable Secret) ---
R1(config)# aaa authentication enable default group tacacs+ enable
R1(config)# line vty 0 4
R1(config-line)# login authentication myauth1
R1(config-line)# authorization exec default
R1(config-line)# exit
R1(config)# line con 0
R1(config-line)# login local
R1(config-line)# exit
```

The fallback mechanism for emergency access is critical for maintaining network manageability if the TACACS+ server becomes unreachable. By configuring `aaa authentication login myauth1 group tacacs+ local`, the router first attempts to authenticate users against the TACACS+ server. If the TACACS+ server is unavailable or authentication fails, the router then attempts to authenticate against its local user database. The `r1admin` user account, created with a privilege level of 15, serves as a local emergency access account, ensuring that administrators can still log in and manage the router directly via console or VTY lines, even in the event of a TACACS+ server outage.

Testing & Verification Results



Comprehensive testing and verification were conducted to ensure the network infrastructure is functioning correctly and securely, adhering to the configured specifications. The following table summarizes the key test categories, methods, results, and their status:

Outcome / Result	Status
Ping tests confirmed all VLANs can communicate through the router, and all VLANs can reach their respective default gateways.	✅ Success
Devices configured for DHCP received the correct IP, default gateway, and DNS server information.	✅ Success
Successfully established SSH connections from the IT Test-PC to all three routers.	✅ Success
Privilege escalation test validated TACACS+ primary and local fallback authorization.	✅ Success
Sticky MAC configuration on the IT switch (Fa0/1) successfully learned and secured the MAC address.	✅ Success
Connecting an unauthorized device resulted in the port shutting down, as expected.	✅ Success

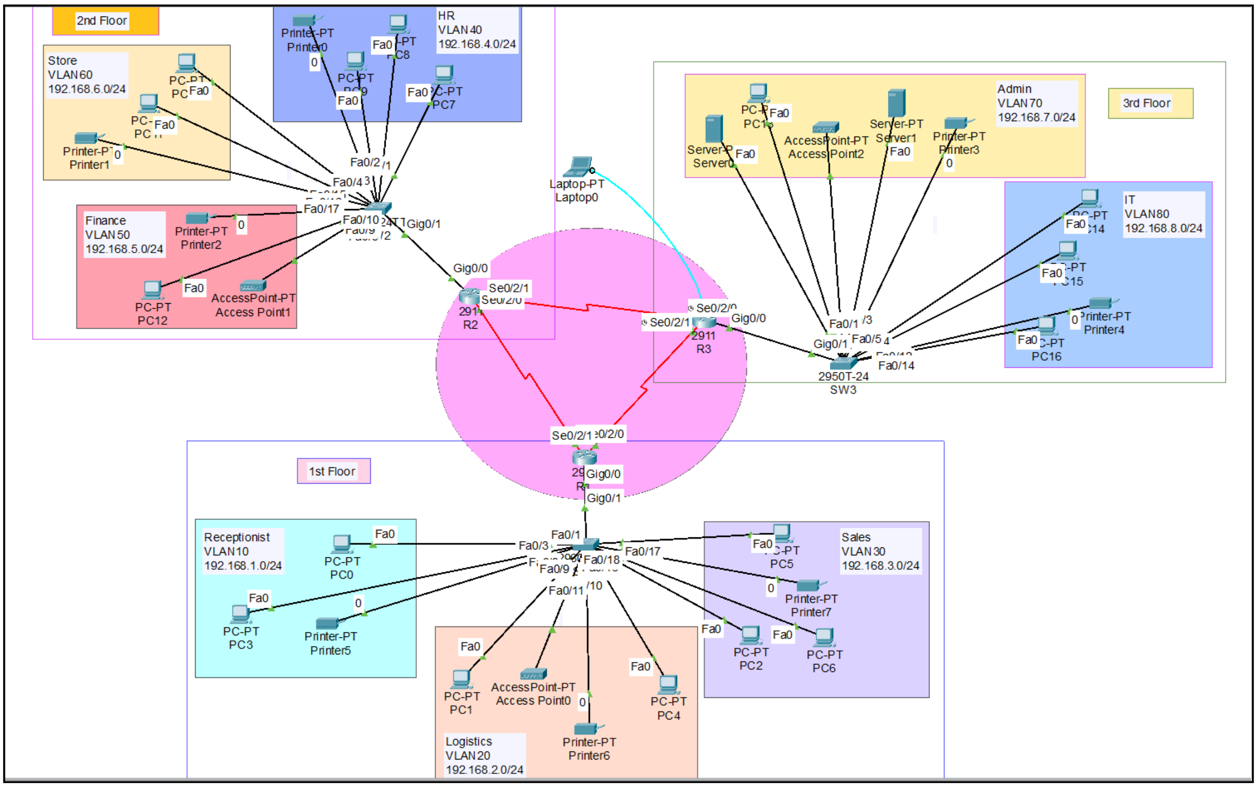
Specific test commands and their results demonstrate the network is functioning correctly as per the design specifications:

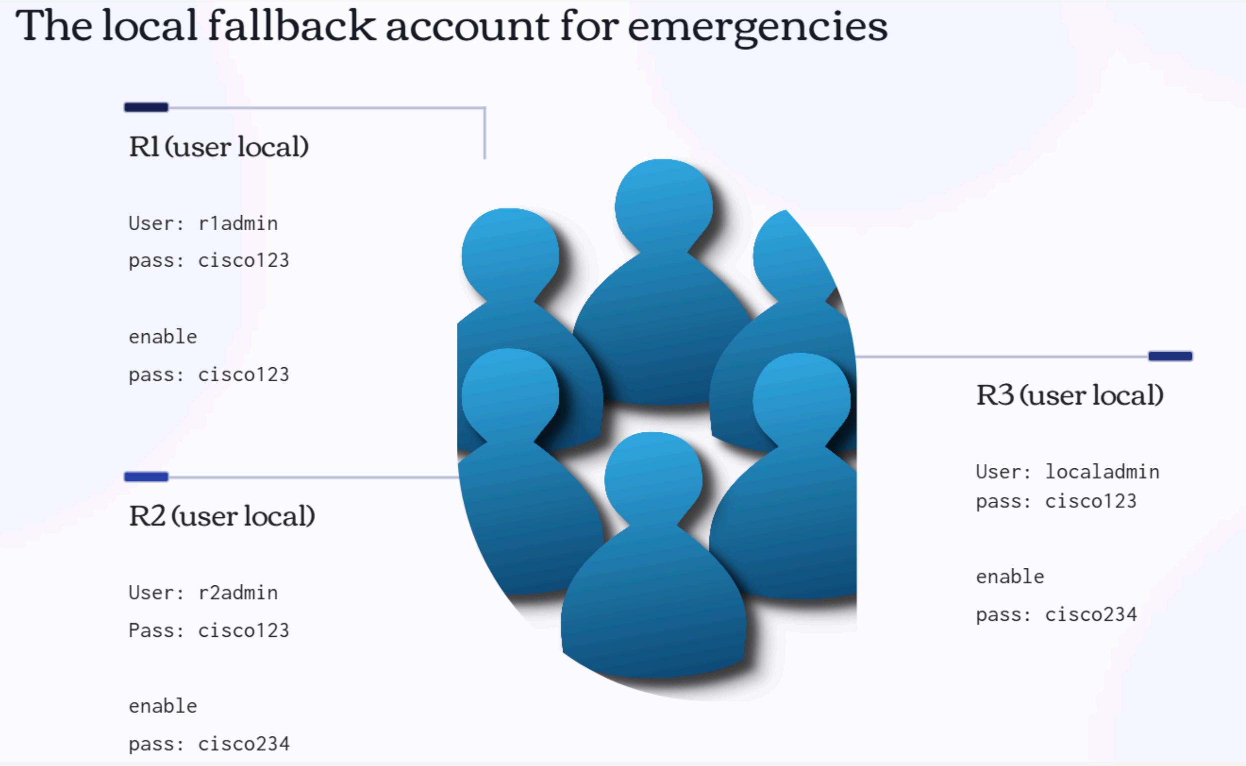
Specific test commands and their results demonstrate the network is functioning correctly as per the design specifications:

```
R1#show ip route ospf
     10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
O       10.10.1.4 [110/128] via 10.10.1.9, 00:00:49, Serial0/2/1
                  [110/128] via 10.10.1.2, 00:00:49, Serial0/2/0
O       10.255.255.2 [110/65] via 10.10.1.2, 00:00:49, Serial0/2/0
O       10.255.255.3 [110/65] via 10.10.1.9, 00:00:59, Serial0/2/1
O    192.168.4.0 [110/65] via 10.10.1.2, 00:00:49, Serial0/2/0
O    192.168.5.0 [110/65] via 10.10.1.2, 00:00:49, Serial0/2/0
O    192.168.6.0 [110/65] via 10.10.1.2, 00:00:49, Serial0/2/0
O    192.168.7.0 [110/65] via 10.10.1.9, 00:00:59, Serial0/2/1
O    192.168.8.0 [110/65] via 10.10.1.9, 00:00:59, Serial0/2/1

R1#ping 192.3168.2.1 (From R1 to a host in VLAN 20, R2)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.13, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

```
R1#show ip dhcp binding
IP address        Client-ID/              Lease expiration        Type
                  Hardware address
192.168.1.11      0005.5E9B.5CED           --                     Automatic
192.168.1.12      000C.CF36.D758           --                     Automatic
<ouput ommited>

R1#show running-config | section aaa
aaa new-model
aaa authentication enable default group tacacs+ enable
aaa authentication login myauth1 group tacacs+ local
```

Network Topology





The local fallback account for emergencies

R1 (user local)

```
User: r1admin
pass: cisco123

enable
pass: cisco123
```

R2 (user local)

```
User: r2admin
Pass: cisco123

enable
pass: cisco234
```

R3 (user local)

```
User: localadmin
pass: cisco123

enable
pass: cisco234
```