Technical Report: Network Design and Configuration for a Military Company

Table of Contents

Introduction

This report gives a detailed description of how the design and configuration of a decentralized network for a military company based in five different geographical locations in different countries can be done. There are, in fact, less than 15 employees at each site – analyzers, network administrators – and at most three temporary guest accounts.

Security, performance, and scalability are the main concerns of the design; each site is autonomous, and inter-site communication is secure but fast and efficient. The remaining network structure decision reflects the desire for a more reliable and fault tolerant design while still permitting autonomy and localized control of resources at various levels.

This report also contains recommendations to improve security posture by analysis of current design and assessment of performance reliability and security understanding. To exhibit the network topology and configuration validations implemented here are screenshots.

Network Overview

Decentralized Design: Why It Was Selected

A **decentralized network structure** was chosen for the following reasons:

1. **Independent Operation of Sites**
   Purpose: This means that each of the sites is fully equipped to stand alone with a Layer 3 router to go with the site's Layer 2 switch. This ensures that:

   Inter-site connectivity problems do not affect local station traffic.

   An RTC-SS can include analyzers' workstations or local file servers as these remain available during WAN link failures.

   Benefit: Reduces reliance on a singular network, and thereby causes minor disturbances when WAN links occur.

2. **Reliability and Fault Tolerance**
   Purpose: The key that decentralization provides, and contrast to the centralized game design, is that it does not rely on one central server, or router. If one site experiences a shut down, the rest of the sites operate in an isolated manner.

   Implementation: OSPF used as routing protocol provides dynamic routing, means it automatically adjusts to a network change, such as the failure of a WAN link.

   Benefit: Preserves the integrity of communication across the network while enhancing the general dependability.

3. **Improved Security**
   Purpose: The use of VLANs and especially Access Control Lists (ACLs) that isolate traffic at different sites ensures that a breach of security only affects the site in question.

Benefit:

Reduces exposure of the network's vulnerabilities.

It helps to prevent breaches in one site from affecting other sites; protects essential data and resources.

4. **Scalability**
   Purpose: Dispersed architecture makes adding a new site easier to accomplish. Each new site can be independently integrated with:

   A router and switch.

   Stet up VLANs and OSPF connections properly.

   Benefit: This does not cause any problem with existing configuration; thus, it can grow with the organization.

5. **Cost-Effectiveness**

   Purpose: The simplest Cisco routers and switches are used to build the network, so there is no need for expensive centralized equipment like a vast data center.

   Benefit: The design offers the optimal combination of speed, stability and growability for the military company but also credible and affordable.

Applicability of Design

The decentralized design is highly applicable for a military company due to the following reasons:

1. **Localized Control**
   All sites are completely independent, but make sure that some important resources such as for example the file servers, analyzers are always available in spite of the interruption of inter site communication.
2. **Enhanced Security**
   Information security at any of these sites is maintained through restricted access, thus limiting threats and effects of vulnerability incidents.
3. **Distributed Resources**
   This results in better performance of the systems as local resources have significantly less latency than does network resources. For example, the services are contained without requiring a go-to site where analyzers and network admins avail VLAN-specific resources.

4. **Flexible Management**
   Independent sites are easy to maintain through troubleshooting since their management can be decentralized thus lessen the workload of IT specialists.

Current Network Design

Network Topology

1. Five Geographically Distributed Sites

It has five centers that are ethnographically diverse although all five sites are structurally separate nodes of the same network. This design makes each of the site to be able to work independently, but at the same time be able to have connectivity to the other sites in different organizations through WAN links.

2. One Layer 3 Router per Site

- **Purpose:** Every site has a Layer 3 router to manage:
  - **Inter-VLAN Routing**: Connecting different VLANs of the same site for easy sharing of communication.
  - **WAN Connectivity**: Feature that involves linking up of the site to other sites in the different Wide Area Network (WAN) locations.
- **Benefit:** Allows for traffic on one VLAN within the site to pass through other VLANs and routing to other sites to be carried out dynamically.

3. One Layer 2 Switch per Site

- **Purpose:** A Layer 2 switch at each site is used for connectivity of attached equipment such as analyzers, workstations of the network administrators, and guest networking equipment.
- **Benefit:** Facilities VLAN segmentation to divide traffic and to ensure that the network is secure.

4. VLAN Segmentation

- **Implementation:** There are three VLANs configured in each site for traffic partition based on users:
  - **VLAN 10 (Analyzers)**: As specific for all devices that manage highly sensitive information, employs the subnet 192.168.10.0/24.
  - **VLAN 20 (Network Admins)**: Administrative servers classified with the subnet 192.168.20.0/24.

  - **VLAN 30 (Guests)**: Temporary user access aka part-time access, assigned to the subnet 192.168.30.0/24.
- **Benefit:** VLAN segmentation helps protect the traffic, reduce the chance of unauthorized access, and enhance the network's throughput, all by minimizing the number of broadcast domains.

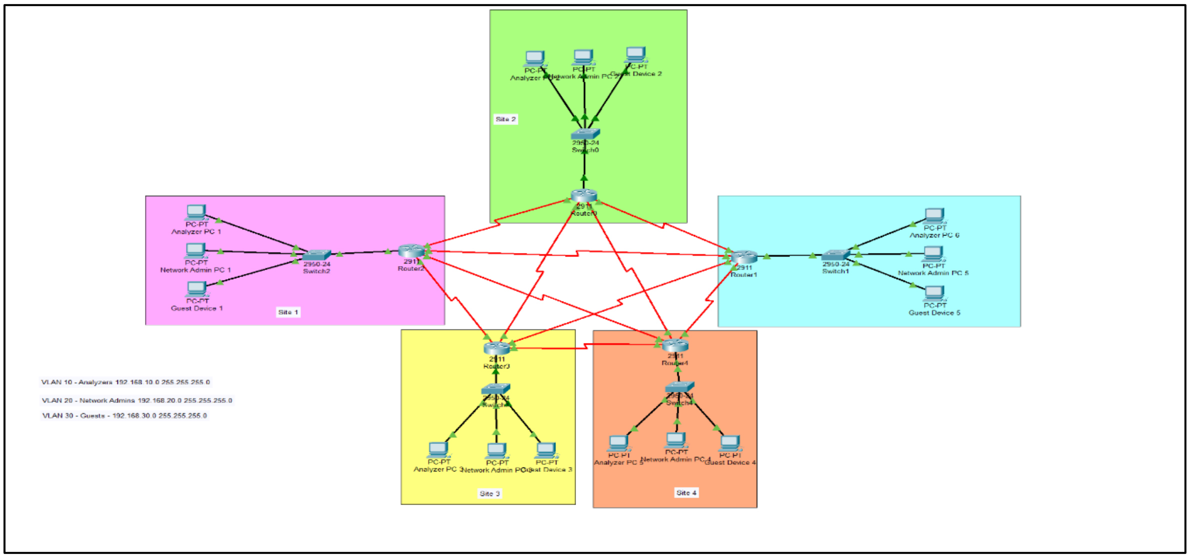
5. OSPF Dynamic Routing

- **Purpose:** Open Shortest Path First (OSPF) is configured on the routers to enable dynamic routing between sites.
- **Functionality:**
  - OSPF automatically updates routing tables when network changes occur (e.g., link failures).
  - Ensures efficient traffic routing and reduces manual configuration efforts.
- **Benefit:** Ensures that inter-site communication is always reliable and increases with growth of the network.

6. Serial Links for WAN Connectivity

- **Purpose: Serial interfaces are used to establish WAN links between routers at different sites.**
- **Configuration:**
  - Links are configured with /30 subnets, which allocate two usable IP addresses per link, optimizing IP address utilization.
- **Benefit:** Safeguards the availability of means of communication for linking the sites in a manner that offers reliability and effectiveness since the system is based on a decentralization of services.

Screenshot of Topology



Packet Tracer topology

Performance, Reliability, and Security Problems

Performance Issues

Lack of QoS Prioritization: There are certain constraints that are as follows: - Without QoS, critical analyzer traffic can be just delayed when the network saturates.

WAN Bandwidth: WAN links required bandwidth may not be sufficient, and then congestion occurs if all sites establish a connection simultaneously.

Reliability Issues

Single Points of Failure: The lack of multiple WAN links creates that possibility of network breakdown if one WAN link is unavailable.

Routing Dependencies: False OSPF configurations can lead to suboptimal path section or a slow convergence of the network routes.

Security Issues

Unrestricted Guest Access:
With the absence of ACLs, traffic of guest VLAN then can be mapped to sensitive VLANs in the agency, making internal resources a target for scans and attacks.

Lack of Port Security:
Some resources illustrate that unauthorized devices can freely join switches and launch malware attacks or initiate unauthorized access.

Rogue DHCP Servers:
Lack of DHCP Snooping implies that the network can in fact be compromised by other DHCP servers giving out the wrong IP settings.

Proposed Network Design

VLAN Configuration

Purpose: VLANs separate traffic by functional areas to provide additional security and to create much tighter traffic compartments.

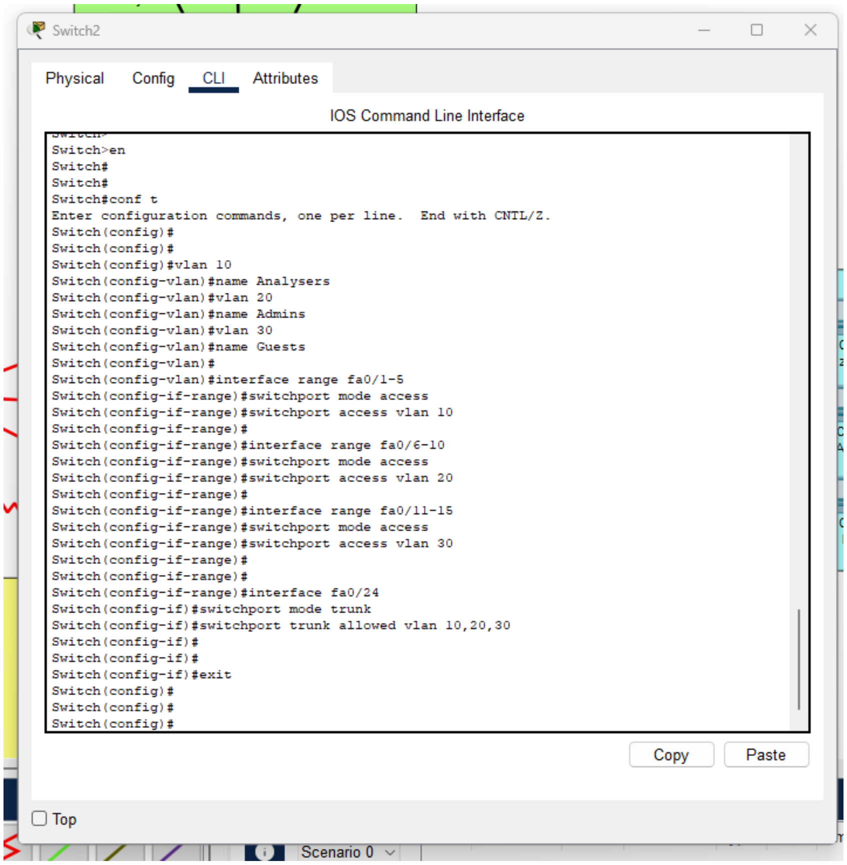
Setup:

- VLAN 10 (Analyzers): 192.168.10.0/24.
- VLAN 20 (Admins): 192.168.20.0/24.

- VLAN 30 (Guests): 192.168.30.0/24.

Access Ports: The switch ports are configured to be in particular VLANs to ensure that the longarm arrangement of devices is followed.

```
vlan 10
name Analyzers
vlan 20
name Admins
vlan 30
name Guests

interface range fa0/1-5
switchport mode access
switchport access vlan 10

interface range fa0/6-10
switchport mode access
switchport access vlan 20

interface range fa0/11-15
switchport mode access
switchport access vlan 30
```



```
Switch>
Switch>en
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#vlan 10
Switch(config-vlan)#name Analysers
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name Admins
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name Guests
Switch(config-vlan)#
Switch(config-vlan)#interface range fa0/1-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#
Switch(config-if-range)#interface range fa0/6-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#
Switch(config-if-range)#interface range fa0/11-15
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#interface fa0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20,30
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#
Switch(config)#
Switch(config)#
```

Router Configuration

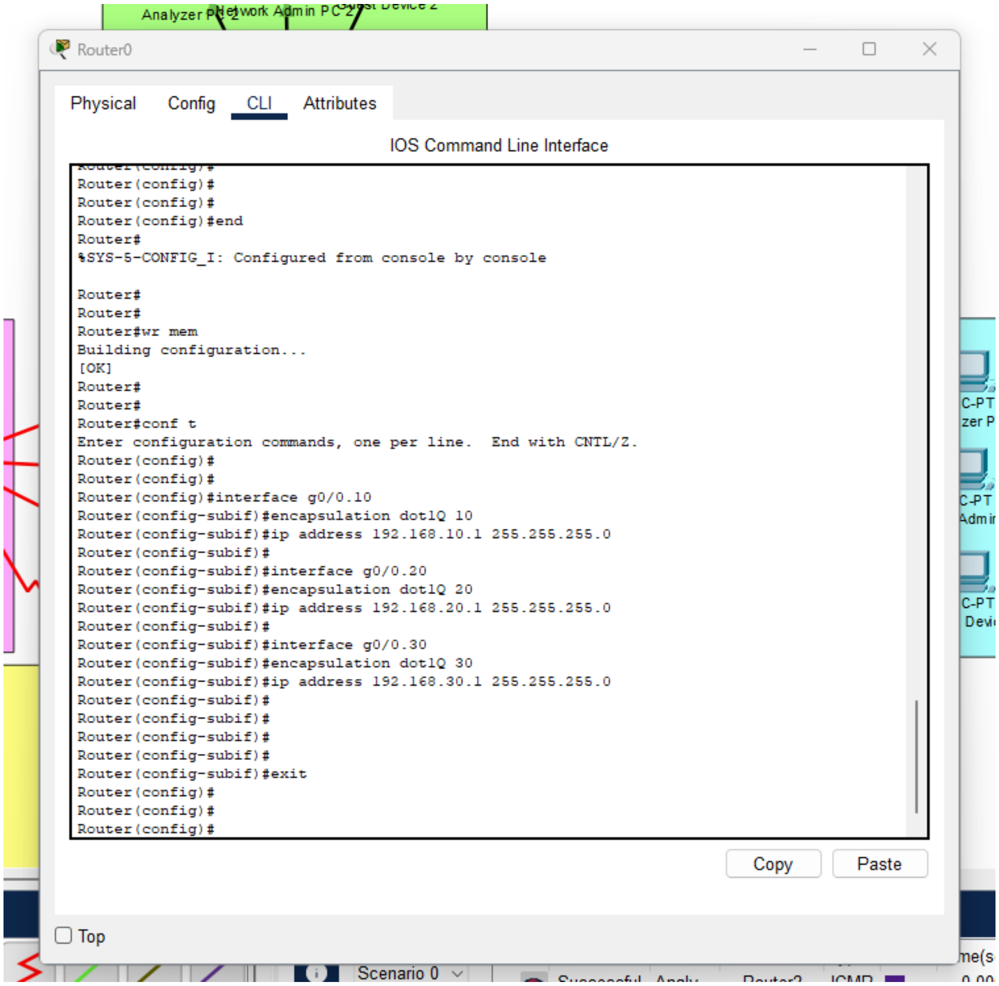
Sub-Interfaces for Inter-VLAN Routing

Purpose: Every sub-interface on the router has its own VLAN for VLAN communication.

Setup: VLAN ID is assigned to each sub-interface in 802.1Q encapsulation manner and the sub-interface is configured to act as the VLAN default gateway that is 192.168.10.1 for VLAN 10.

```
interface g0/0.10

encapsulation dot1Q 10

ip address 192.168.10.1 255.255.255.0
```

```
interface g0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0

interface g0/0.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
```



```
Router(config)#
Router(config)#
Router(config)#
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#
Router#wr mem
Building configuration...
[OK]
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#interface g0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#interface g0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#interface g0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#exit
Router(config)#
Router(config)#
Router(config)#
```

WAN Links

Purpose: In the case of inter-site communication, communication between routers happens through serial links.

Setup: To be configured with /30 subnets for optimization in the allocation of the IPs as well as for its activation, which does not need a shutdown command.

```
interface s0/2/1

ip address 10.1.7.2 255.255.255.252

no shutdown
```

Dynamic Routing with OSPF

Purpose: OSPF should be used because it is an effective routing protocol that provides for site redundancy.

Setup: While VLAN subnets and WAN links are established, OSPF encompasses them in Area 0 to allow the dynamic management of routing.

.

```
router ospf 1

network 192.168.10.0 0.0.0.255 area 0

network 192.168.20.0 0.0.0.255 area 0

network 10.0.0.0 0.0. 0.3 area 0
```

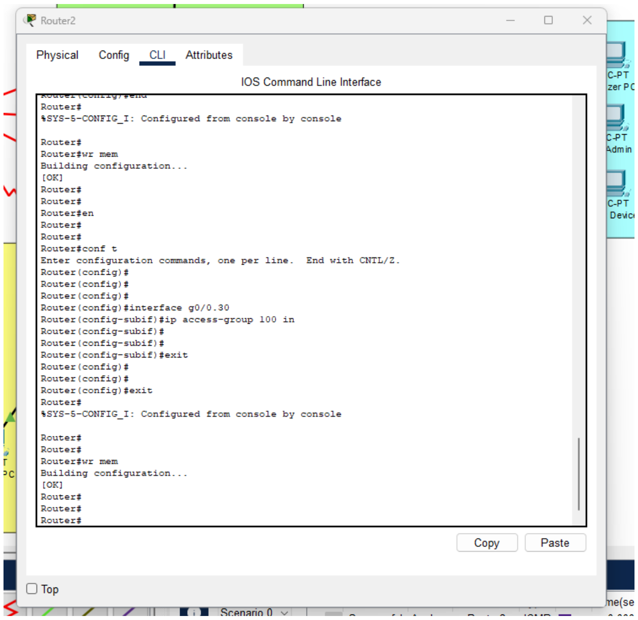
Security Enhancements

Access Control Lists (ACLs)

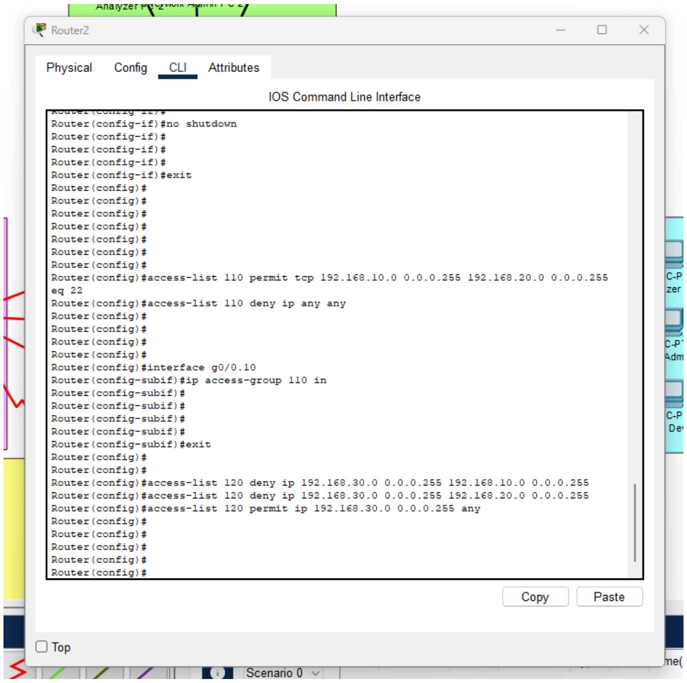
Disable guest VLAN (VLAN 30) to have no access to restricted VLANs (VLAN 10 and VLAN 20).

Allow concrete network traffic (for example SSH) only between the analyzers and admins.

```
access-list 120 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255

access-list 120 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255

access-list 120 permit ip 192.168.30.0 0.0.0.255 any
```



```
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#wr mem
Building configuration...
[OK]
Router#
Router#
Router#en
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#
Router(config)#interface g0/0.30
Router(config-subif)#ip access-group 100 in
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#exit
Router(config)#
Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#
Router#wr mem
Building configuration...
[OK]
Router#
Router#
Router#
```



```
Router(config-if)#
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#access-list 110 permit tcp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
eq 22
Router(config)#access-list 110 deny ip any any
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#interface g0/0.10
Router(config-subif)#ip access-group 110 in
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#exit
Router(config)#
Router(config)#
Router(config)#access-list 120 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
Router(config)#access-list 120 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
Router(config)#access-list 120 permit ip 192.168.30.0 0.0.0.255 any
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
```

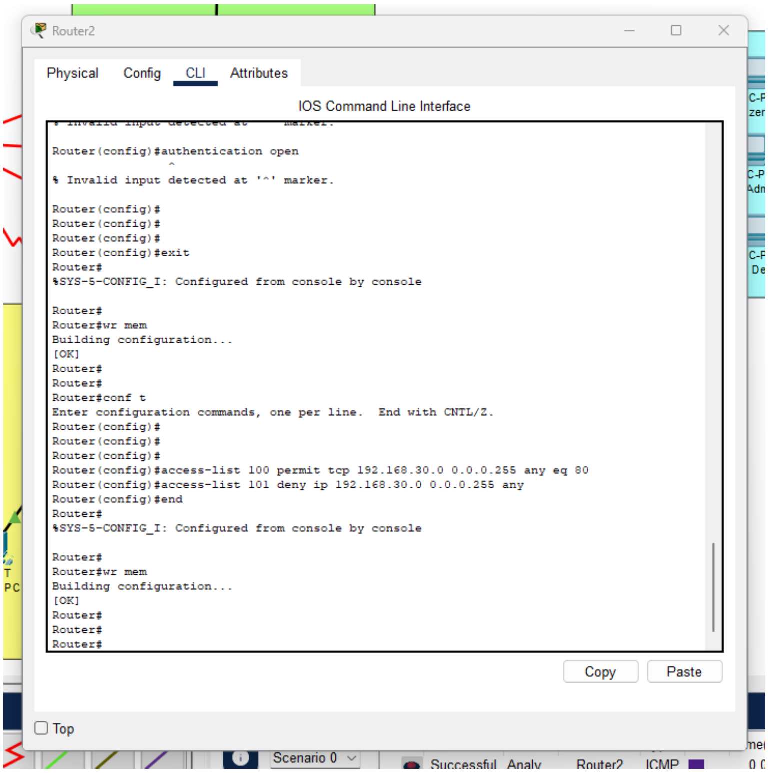
Allow analyzer-to-admin communication (e.g., SSH):

```
access-list 110 permit tcp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 eq 22
access-list 110 deny ip any any
```

Port Security

Port security prevents unauthorized devices from accessing the network:

```
interface range fa0/1-15
switchport port-security
switchport port-security maximum 1
switchport port-security violation shutdown
```

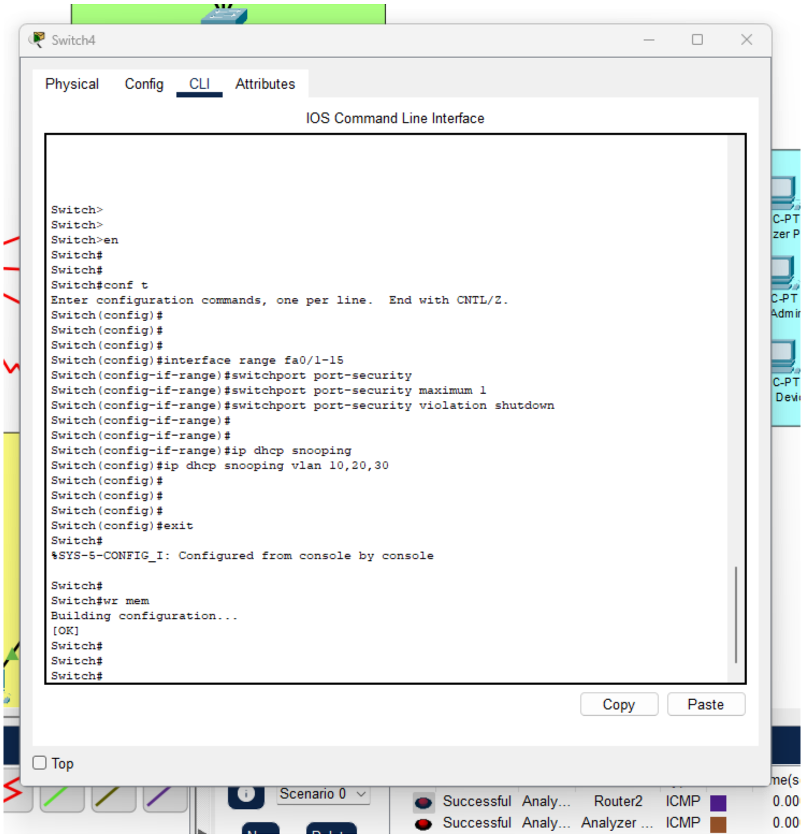


```
% Invalid input detected at '^' marker.

Router(config)#authentication open
                ^
% Invalid input detected at '^' marker.

Router(config)#
Router(config)#
Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#wr mem
Building configuration...
[OK]
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#
Router(config)#access-list 100 permit tcp 192.168.30.0 0.0.0.255 any eq 80
Router(config)#access-list 101 deny ip 192.168.30.0 0.0.0.255 any
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#wr mem
Building configuration...
[OK]
Router#
Router#
Router#
```

DHCP Snooping

DHCP snooping ensures only trusted DHCP servers can assign IP addresses:

```
ip dhcp snooping

ip dhcp snooping vlan 10,20,30
```



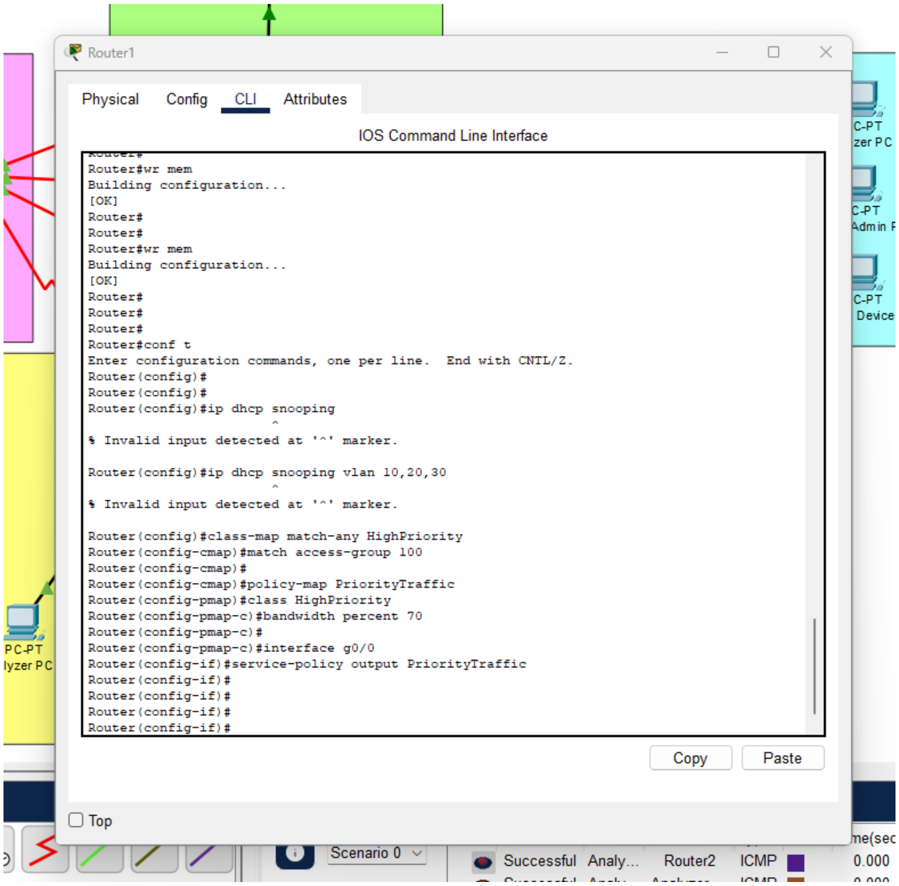
Switch4
Physical
Config
CLI
Attributes
IOS Command Line Interface
Copy
Paste
□ Top
Scenario 0
Successful Analy... Router2 ICMP 0.00
Successful Analy... Analyzer ... ICMP 0.00

```
Switch>
Switch>
Switch>en
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#interface range fa0/1-15
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 1
Switch(config-if-range)#switchport port-security violation shutdown
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 10,20,30
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
Switch#wr mem
Building configuration...
[OK]
Switch#
Switch#
Switch#
```

Quality of Service (QoS)

QoS prioritizes traffic for analyzers, ensuring critical data receives priority during congestion:

```
class-map match-any HighPriority
match access-group 110

policy-map QoSPolicy
class HighPriority
bandwidth percent 60

interface g0/0
service-policy output QoSPolicy
```



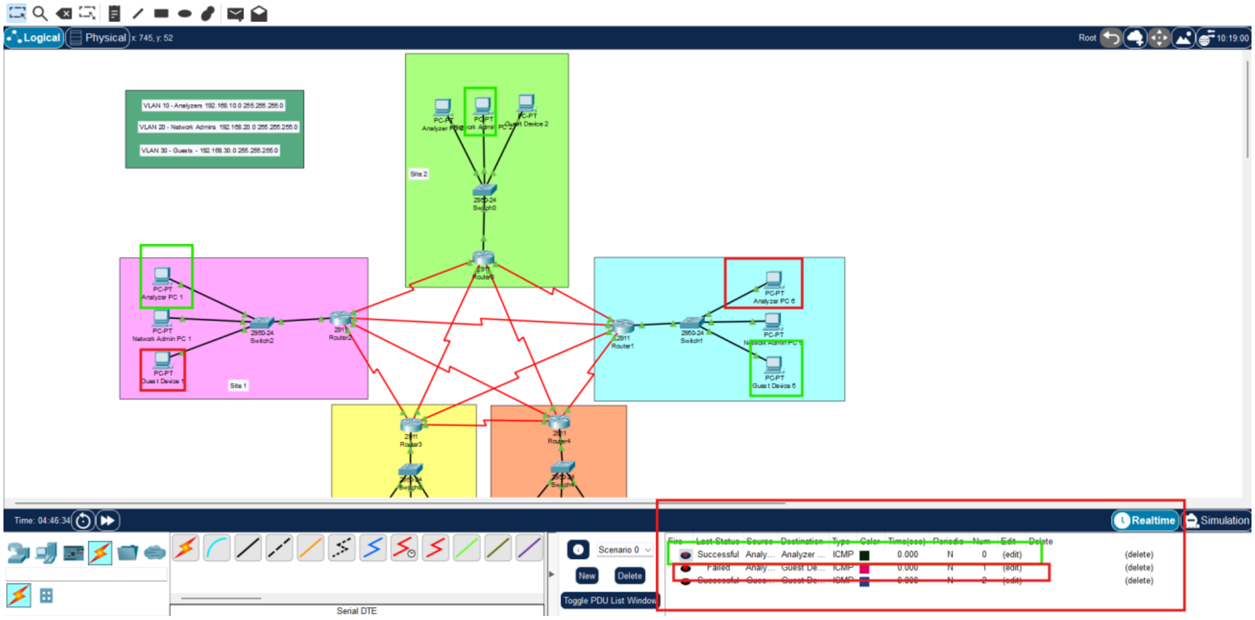
```
Router#
Router#wr mem
Building configuration...
[OK]
Router#
Router#
Router#wr mem
Building configuration...
[OK]
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#ip dhcp snooping
                       ^
% Invalid input detected at '^' marker.

Router(config)#ip dhcp snooping vlan 10,20,30
                       ^
% Invalid input detected at '^' marker.

Router(config)#class-map match-any HighPriority
Router(config-cmap)#match access-group 100
Router(config-cmap)#
Router(config-cmap)#policy-map PriorityTraffic
Router(config-pmap)#class HighPriority
Router(config-pmap-c)#bandwidth percent 70
Router(config-pmap-c)#
Router(config-pmap-c)#interface g0/0
Router(config-if)#service-policy output PriorityTraffic
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
```

Testing and Validation

Connectivity Tests

Validate inter-VLAN routing by pinging between VLANs at each site.

Test WAN links by pinging devices across sites.

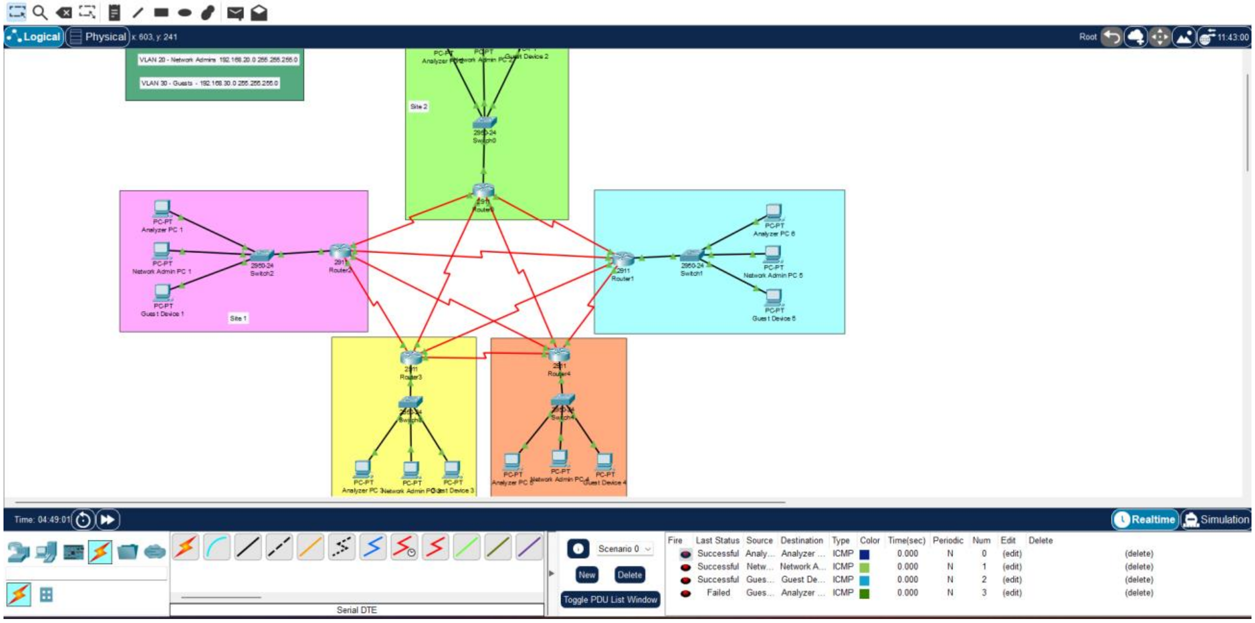


Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	Analy...	Analyzer ...	ICMP	■	0.000	N	0	(edit)	(delete)
●	Failed	Analy...	Guest De...	ICMP	■	0.000	N	1	(edit)	(delete)
●	Successful	Gues...	Guest De...	ICMP	■	0.000	N	2	(edit)	(delete)

Security Tests

Simulate unauthorized access attempts to validate ACLs and port security.

Introduce a rogue DHCP server to ensure DHCP snooping blocks it.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	Analy...	Analyzer ...	ICMP	■	0.000	N	0	(edit)	(delete)
●	Successful	Netw...	Network A...	ICMP	■	0.000	N	1	(edit)	(delete)
●	Successful	Gues...	Guest De...	ICMP	■	0.000	N	2	(edit)	(delete)
●	Failed	Gues...	Analyzer ...	ICMP	■	0.000	N	3	(edit)	(delete)

Performance Validation

Simulate high traffic loads to ensure QoS settings prioritize analyzer traffic.

Evaluation of Controls

Why These Controls Were Chosen

All the controls were selected based on the issues that the network is likely to face to improve its security, efficacy, and capacity. Here's a detailed explanation:

1. **VLANs and ACLs**
    - **Purpose:** VLANs were selected to provide ways of sorting traffic in the network into meaningful groups (for example analyzers, network admin, and guests). This leads to the isolation of traffic that flows in every VLAN thus minimizing chances of free access to vital resources. ACLs add to this in that they allow or deny traffic flow between VLANs as per set protocols. For instance, standard ACLs prevent traffic on guest VLAN (VLAN 30) to transit to sensitive VLANs such as VLAN 10 and VLAN 20.
    - **How It Works:** VLANs logically divide traffic at the Layer 2 level, while ACLs act at Layer 3 to filter traffic based on IP addresses, ports, and protocols. For instance:
        - VLAN segmentation ensures that analyzers' sensitive data is not accessible to guests.
        - ACLs control inter-VLAN communication by explicitly permitting or denying specific traffic types (e.g., SSH between analyzers and network admins).
2. **Port Security**
    - Purpose: Port security was selected to avoid other devices to have connection authorization such as computers which are unsafe to the rest of the network. This control helps in authorizing connections from only the right devices to particular switch ports.
    - How It Works: In port security, you cannot allow a port to have more than some MAC addresses. If the port is accessed by an unauthorized device, the port immediately closes to help protect the network against intruders.
3. **DHCP Snooping**
    - Purpose: DHCP Snooping was developed to prevent unauthorized DHCP servers that try to assign wrong IP settings or even intercept traffic.

- How It Works: DHCP Snooping checks DHCP messages and relays them by only permitting DHCP servers that have been authorized to reply to the DHCP messages. Whereas unauthorized DHCP responses are not forwarded to devices, so there and then they are ignored as the devices receive genuine IP addresses.

4. **Quality of Service (QoS)**
    - Purpose: QoS guarantees priority of important traffic during congestion, for Example traffic related to analyzers data. This is especially relevant in cases where the product has a short-life cycle, adapted most suitably for the purpose.
    - How It Works: By using ACLs or any other values, QoS effectively sets traffic priority levels or class. Sensitive traffic is identified to receive more bandwidth or to undergo lower latency to avoid its accumulation.

Benefits

Enhanced Security Posture Through Layered Controls

- VLAN segmentation protects some traffic while leaving others to roam the network; thus, isolating the breach.
- ACLs enforce strict access rules, reducing the likelihood of unauthorized access.
- Port security ensures only approved devices are connected, limiting attack vectors.
- DHCP Snooping prevents unauthorized devices from tampering with network configurations.

Improved Performance with Traffic Prioritization

- QoS guarantees that the data packets of an essential application (for instance, analyzer workflow) will be allowed to run efficiently during high traffic.

Scalability and Reliability for Future Expansion

- VLANs and ACLs make it possible for the administration and configuration of growth into the network in a new direction without redesigning.
- OSPF dynamic routing and layered security controls guarantee the network is always reliable and scalable, especially when more resources or users are incorporated.

Potential Risks

- Port security that is too stringent maybe harmful to the authorized user.

- Overly restrictive port security could disrupt authorized users.

Conclusion

These aspects of network decentralization make communication for the military company secure, reliable and scalable. Current configurations comprising VLAN segmentation, OSPF routing, ACLs, port security, and QoS contribute to satisfying the performance and security objectives of the network. The design also allows for inflexion of future new additions, keeping the military company's IT in good stead.

****