



Capstone Group Project

Project brought to you by:

- ★ ***Sonal Patel***
- ★ ***Balkrishna Gurung***
- ★ ***Nathanael Aime***
- ★ ***Noble Ekechukwu***

Executive Summary:	2
PerScholas Software-Defined Networking (SDN), Zero Trust, and SASE Network Refresh	2
Key Objectives	2
Key Components	2
RF PREDICTIVE WIRELESS SITE SURVEY:	3
Implementation Strategy	3
Network Topology: HQ/REMOTE SITE/HOME OFFICE	4
Password / IP Addressing	4
Configuration	5
SSH Protocol: Secure remote management	9
Access Point (AP) Failover and High Availability (HA)	10
What Is AP Failover?	10
What Is High Availability (HA)?	10
Channel Segmentation IoT Devices in Wireless	10
Why Channel Segmentation Matters for IoT Devices	10
1. Minimize Interference:	10
Micro-Segmentation	11
VPN Connectivity: HOME EXECUTIVE	11
Testing DHCP in Real-Time Simulation Mode	12
Micro-Segmentation and Contextual IP Allocation	13
Disabling SSID Broadcast	14
What Happens When You Disable SSID Broadcasting?	14
Considerations and Limitations	14
MAC Address Filtering in Wi-Fi for Zero Trust Security	15
Role of MAC Address Filtering in Zero Trust Security	15
Device Identification:	15
Best Practices for Using MAC Address Filtering with Zero Trust Security	16
1. Use MAC Filtering as an Additional Layer	16
2. Combine with Network Access Control (NAC)	16
3. Apply MAC Filtering to Micro-Segmented Networks	16
4. Use Certificates for Device Authentication	16
5. Regularly Update and Audit MAC Address Lists	16
Extended Access Control List (ACL) ON OUR REMOTE ROUTER	17
When to Use Extended ACLs	17
Best Practices for Extended ACLs	18
Benefit of Software-Defined Networking (SDN), Zero Trust, and SASE Network	19
Conclusion	19

Executive Summary:

PerScholas Software-Defined Networking (SDN), Zero Trust, and SASE Network Refresh

The proposed network refresh integrates Software-Defined Networking (SDN), the Zero Trust security framework, and Secure Access Service Edge (SASE) to deliver a unified, scalable, and secure architecture. This transformation ensures the organization is equipped to handle modern challenges, including cloud adoption, remote work, and evolving cyber threats, while streamlining operations and enhancing performance.

Key Objectives

1. **Modernized Network Infrastructure:** Shift to a software-driven, automated, and dynamic network to support agility and innovation.
2. **Enhanced Security Posture:** Leverage Zero Trust and SASE principles to establish a robust, identity-centric, and cloud-ready security framework.
3. **Optimized User Experience:** Provide seamless, high-performance connectivity to users regardless of location or device.
4. **Operational Efficiency:** Simplify network and security management through centralized tools and automated processes.

Key Components

1. **Software-Defined Networking (SDN):**
 - Centralized Control: Decouple network management from hardware, enabling simplified configuration and real-time adjustments.
 - Policy-Driven Networking: Implement consistent access and traffic policies across environments (on-premises, cloud, and hybrid).
 - Scalability and Flexibility: Enable rapid deployment of new services and infrastructure to meet business needs.
2. **Zero Trust Security Framework:**
 - Verify Identity and Device: Authenticate every user and device, applying adaptive access based on behavior, location, and risk assessment.
 - Micro-Segmentation: Contain potential breaches by restricting lateral movement within the network.
 - Continuous Monitoring: Proactively identify and mitigate threats with real-time insights and analytics.
3. **Secure Access Service Edge (SASE):**
 - Cloud-Native Security: Integrate SD-WAN with advanced security services such as secure web gateways (SWG), cloud access security brokers (CASB), and data loss prevention (DLP).
 - Edge-Based Connectivity: Optimize performance by securely connecting users to resources via the nearest edge location.
 - Zero Trust Integration: Extend security policies to remote and mobile users through identity and context-aware access controls.

RF PREDICTIVE WIRELESS SITE SURVEY:

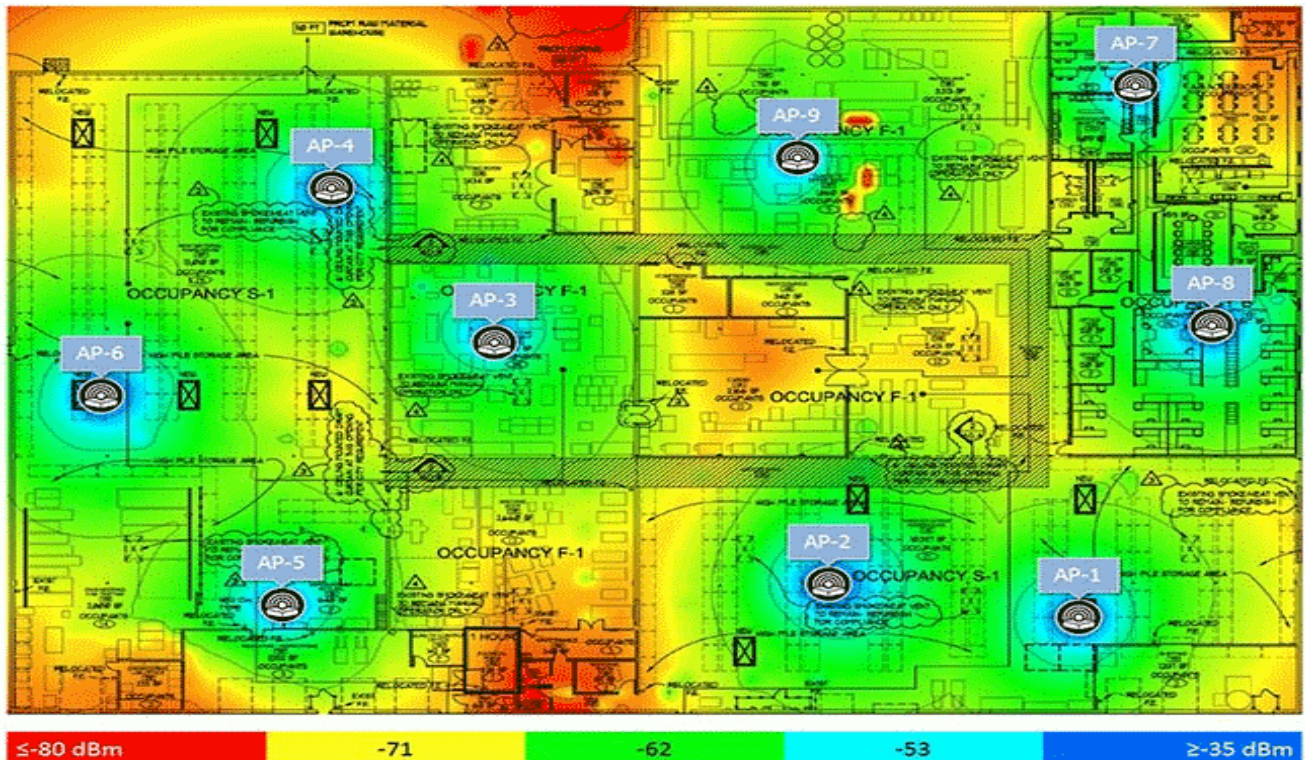
Detailed Report with Coverage Maps

Signal Strength (RSSI): Highlights areas with strong and weak signals across the site.

Coverage Gaps: Identifies dead zones or areas with inconsistent signal quality.

Interference Sources: Detects nearby networks, physical obstructions, or devices causing signal interference.

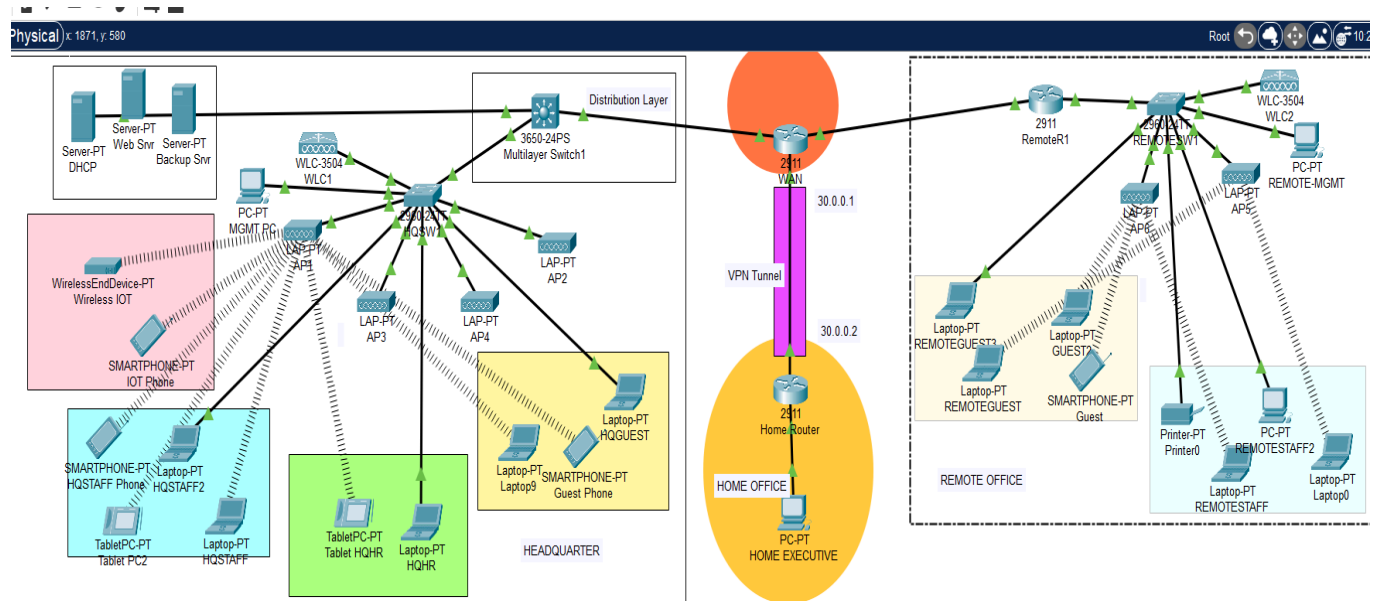
Usage Data: Analyzes client density and bandwidth utilization by location.



Implementation Strategy

1. **Assessment and Planning:** Evaluate current network and security posture to identify gaps and align with business objectives.
2. **Phased Deployment:** Roll out SDN, Zero Trust, and SASE components incrementally to minimize disruptions and ensure compatibility.
3. **Training and Support:** Equip IT teams and stakeholders with the knowledge and tools to manage the new architecture effectively.
4. **Continuous Improvement:** Monitor performance, gather feedback, and refine policies to ensure the network evolves with business needs.

Network Topology: HQ/REMOTE SITE/HOME OFFICE



Password / IP Addressing

HQ MGMT	192.168.1.0/24	VLAN 1	Pers2025
HQ Staff	192.168.11.0/24	VLAN2	Perstaff2025
HQ HR	192.168.12.0/24	VLAN3	Perhr2025
HQ Guest	192.168.13.0/24	VLAN4	Perguest2025
HQ IoT	192.168.14.0/24	VLAN5	Periot2025
WLC HQ	192.168.1.12/24	VLAN1	BOTH: Pers2025
Remote Office MGMT	192.168.2.0/24	VLAN1	
Remote Office Staff	192.168.21.0/24	VLAN7	Perstaff2025
Remote Office Guest	192.168.22.0/24	VLAN8	Perguest2025
WLC Remote	192.168.2.12/24	VLAN1	BOTH: Pers2025

Home router: HQ1

Console- home

Enable- class

Ip domain name- home.com

Ssh -l admin 192.168.6.1

Password

Remote router: RemoteR1
Console - remote
En- class
Ssh -l admin 192.168.22.1
Password- remote

WAN router: WAN
Console- wan
En- class
Ssh -l admin 192
Password- wan

Remote switch: RemoteS1
Console- switch
En- class
Ip domain name- remote switch.com
Ssh -l admin 192.168.
Password- switch

Headquarter Switch: HQS1
Console Password - hq
Enable password- class
Ssh -l admin 192.168.
Password hq

Headquarter Multilayer Switch
Con - switch
En- class
Ip domain name disswitch.com
Ssh -l admin 192.168.
Password- switch

Configuration

HQSW1#show run
Building configuration...
Current configuration : 1913 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname HQSW1
!
enable secret 5 \$1\$mERr\$9cTjUIEqNGurQiFU.ZeCi1
!
ip domain-name hq.com
!
username admin privilege 1 password 7 08295D

```
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
interface FastEthernet0/1  
switchport mode trunk  
!  
interface FastEthernet0/2  
switchport mode trunk  
!  
interface FastEthernet0/3  
switchport mode trunk  
!  
interface FastEthernet0/4  
switchport mode access  
!  
interface FastEthernet0/5  
switchport mode trunk  
!  
interface FastEthernet0/6  
switchport mode trunk  
!  
interface FastEthernet0/7  
switchport access vlan 2  
switchport mode access  
!  
interface FastEthernet0/8  
switchport access vlan 4  
switchport mode access  
!  
interface FastEthernet0/9  
switchport access vlan 3  
switchport mode access  
  
interface GigabitEthernet0/1  
switchport mode trunk  
interface GigabitEthernet0/2  
switchport mode trunk  
interface Vlan1  
ip address 192.168.1.2 255.255.255.0  
ip helper-address 192.168.1.11  
interface Vlan2  
ip address 192.168.11.2 255.255.255.0  
ip helper-address 192.168.1.11  
  
interface Vlan3  
ip address 192.168.12.2 255.255.255.0  
ip helper-address 192.168.1.11
```

```
ip default-gateway 192.168.1.1
banner motd ^CUnauthorized access is prohibited^C
line con 0
password 7 08295D
login
line vty 0 4
login local
transport input ssh
line vty 5 15
login local
transport input ssh
end
```

REMOTER1#show run

Building configuration...

Current configuration : 2127 bytes

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

hostname REMOTER1

enable secret 5 \$1\$mERr\$9cTjUIEqNGurQiFU.ZeCi1

ip dhcp excluded-address 192.168.2.1 192.168.2.20

ip dhcp excluded-address 192.168.2.49 192.168.2.255

ip dhcp excluded-address 192.168.21.1 192.168.21.49

ip dhcp excluded-address 192.168.21.101 192.168.21.255

ip dhcp excluded-address 192.168.22.1 192.168.22.49

ip dhcp excluded-address 192.168.22.101 192.168.22.255

ip dhcp pool REMOTEDHCP

network 192.168.2.0 255.255.255.0

default-router 192.168.2.1

domain-name perscholas

ip dhcp pool REMOTESTAFF

!

network 192.168.21.0 255.255.255.0

default-router 192.168.21.1

domain-name perscholas

ip dhcp pool REMOTEGUEST

network 192.168.22.0 255.255.255.0

default-router 192.168.22.1

domain-name perscholas

ip cef

no ipv6 cef

username admin password 7 08334943060D00

license udi pid CISCO2911/K9 sn FTX152478RV-


```
ip domain-name perscholas
spanning-tree mode pvst
interface GigabitEthernet0/0
ip address 192.168.3.253 255.255.255.0
duplex auto
speed auto
```

```
interface GigabitEthernet0/1
ip address 192.168.2.1 255.255.255.0
duplex auto
speed auto
```

```
interface GigabitEthernet0/1.7
encapsulation dot1Q 7
ip address 192.168.21.1 255.255.255.0
ip helper-address 192.168.2.1
ip helper-address 192.168.21.1
```

```
interface Vlan1
no ip address
shutdown
```

```
router rip
network 192.168.1.0
network 192.168.2.0
network 192.168.3.0
network 192.168.4.0
network 192.168.11.0
network 192.168.12.0
network 192.168.14.0
network 192.168.21.0
```

```
ip classless
```

```
ip flow-export version 9
access-list 101 deny icmp 192.168.21.0 0.0.0.255 192.168.2.0 0.0.0.255 echo
access-list 101 deny icmp 192.168.22.0 0.0.0.255 192.168.2.0 0.0.0.255 echo
access-list 101 permit ip any any
```

```
banner motd ^CUnauthorized access is prohibited^C
```

```
line con 0
password 7 08334943060D00
login
```

```
line aux 0
```

```
line vty 0 4
login local
transport input ssh
!
End
```

SSH Protocol: Secure remote management

SSH, or Secure Shell, is a powerful network protocol that allows you to securely access and manage remote computers over an unsecured network. It's like having a secure tunnel through the internet, protecting your sensitive information from prying eyes.

Enable SSH:

```
Router(config)# ip domain-name
Router(config)# crypto key generate rsa modulus 1024
Router(config)# line vty 0 4
Router(config-line)# transport input ssh
```

Configure SSH:

```
Router(config)# username <admin> password <password>
Router(config)# line vty 0 4
Router(config-line)# login local
```

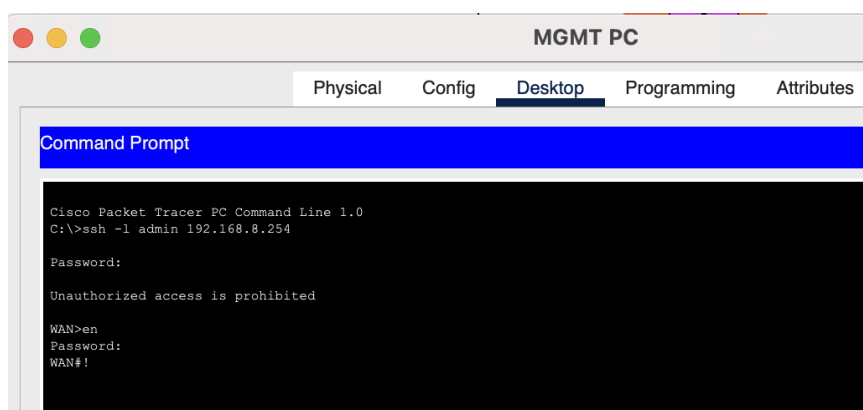
Why is SSH so important for secure network access?

Security

- **Encryption:** SSH encrypts all communication between your computer and the remote server. ¹ This means that even if someone intercepts your connection, they won't be able to understand the data being transmitted.
- **Authentication:** SSH uses strong authentication methods, such as public-key cryptography, to verify your identity before granting you access to the remote system. This prevents unauthorized users from logging in

Remote Access

- **Tunneling or Port Forwarding.:** SSH can create secure tunnels for other network protocols, allowing you to access services on the remote network as if you were connected directly. This is useful for securely accessing web servers, databases, and other resources.
- **Command-line access:** SSH allows you to log into a remote machine and execute commands as if you were sitting in front of it.



Access Point (AP) Failover and High Availability (HA)

AP failover and High Availability (HA) ensure uninterrupted wireless network connectivity by providing mechanisms for redundancy and seamless transitions when an access point (AP) or controller fails. These features are critical for businesses that rely on consistent and reliable Wi-Fi performance.

What Is AP Failover?

AP failover refers to the process where an access point switches to a backup controller or another AP when its primary controller or AP becomes unavailable. This minimizes service disruptions and ensures continuous connectivity for devices.

What Is High Availability (HA)?

High Availability is a broader concept focused on maintaining uptime by providing redundancy at the network architecture level, ensuring that failures in one component (e.g., APs, controllers, switches) don't disrupt overall network functionality.

Channel Segmentation IoT Devices in Wireless

Channel segmentation involves strategically allocating and managing wireless channels to minimize interference and optimize performance for IoT devices. Since IoT devices often operate on the 2.4 GHz band and are sensitive to interference and congestion, properly segmenting channels is critical to maintaining reliable connectivity.

*IoT VLAN / SSID Configured with focus on operating on **2.4 GHz***

Why Channel Segmentation Matters for IoT Devices

1. Minimize Interference:

- IoT devices typically operate on **2.4 GHz**, which is more prone to interference from other devices, including microwaves, cordless phones, and overlapping Wi-Fi networks.
- Proper channel segmentation avoids channel overlap, reducing interference.

2. Optimize Performance:

- Many IoT devices have low bandwidth needs but require stable connections for real-time data transfer (e.g., sensors, cameras).
- Assigning dedicated or less congested channels improves reliability.

3. Separate Traffic:

- Isolating IoT devices onto specific channels or bands ensures that critical IoT communications aren't disrupted by high-bandwidth consumer devices like laptops or phones.

Micro-Segmentation

- Divide IoT devices into smaller groups based on function (e.g., sensors, cameras, smart lighting) and assign each group to a specific channel.

Channel segmentation for IoT devices ensures reliable performance and minimizes interference in wireless networks. Combining proper channel allocation with techniques like band steering, micro-segmentation, and VLANs not only optimizes connectivity but also strengthens security.

VPN Connectivity: HOME EXECUTIVE

A VPN (Virtual Private Network) creates a secure, encrypted connection over a public network, often the internet. This secure connection, known as a tunnel, allows for private communication between two points.

How VPN tunneling works:

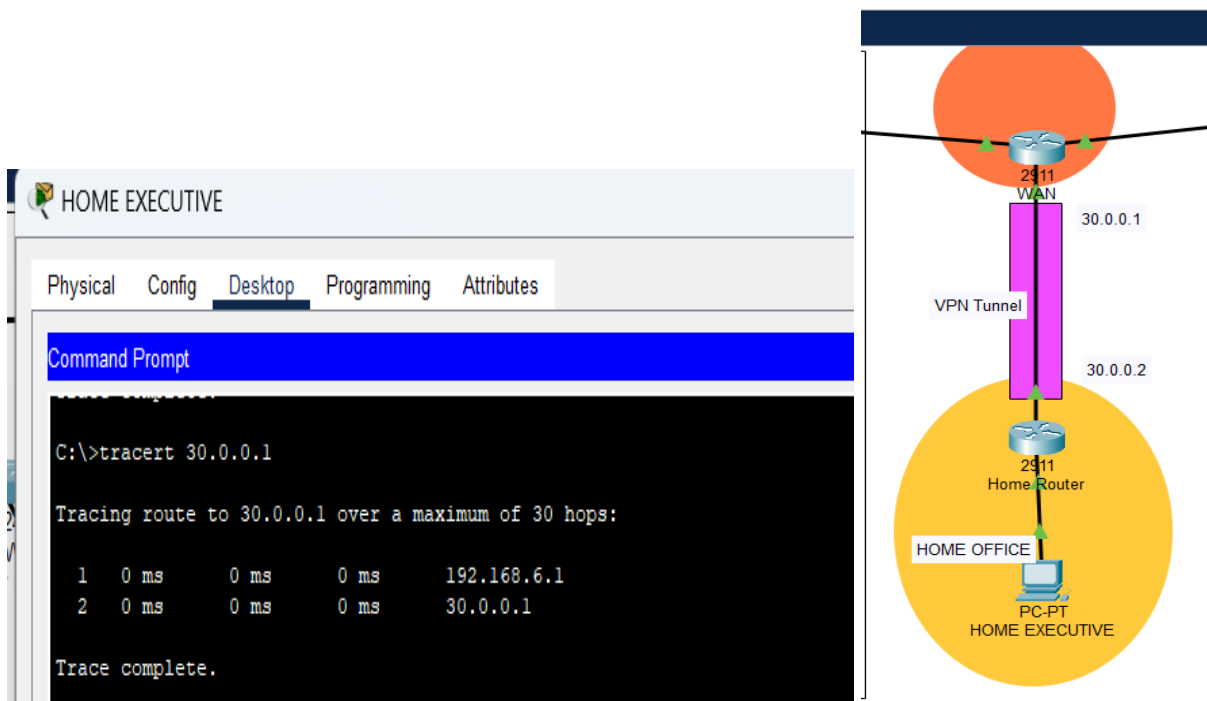
- **Initiation:**
 - A user device (e.g., computer, smartphone) initiates a connection to a VPN server.
 - The device encrypts the data it wants to send.
- **Encapsulation:**
 - The encrypted data is encapsulated within a VPN protocol packet. This packet includes information about the destination and source addresses, as well as encryption keys.
- **Transmission:**
 - The encapsulated packet is sent over the public internet to the VPN server.
 - The packet travels through various networks, but remains encrypted and protected.
- **Decryption:**
 - The VPN server receives the encrypted packet and decrypts it using the appropriate key.
 - The decrypted data is then forwarded to its intended destination within the private network.

Key Benefits of VPN Tunneling:

- **Security:** Encrypts data to protect it from interception and unauthorized access.
- **Privacy:** Hides the user's IP address, making it difficult to track online activities.
- **Remote Access:** Enables secure access to private networks from anywhere with an internet connection.

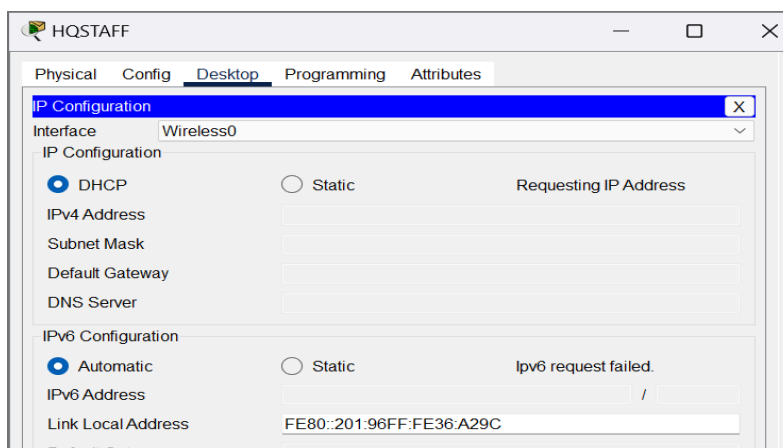
- **Bypass Censorship:** Can be used to circumvent internet censorship and access blocked content.

See testing results below for Tracert command using VPN tunnel in our topology for Home office connectivity.



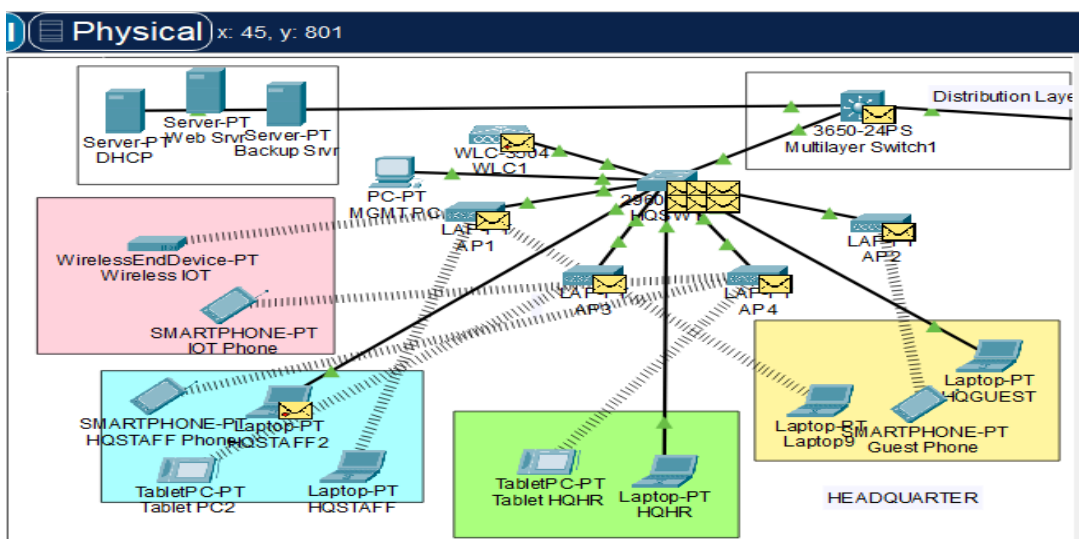
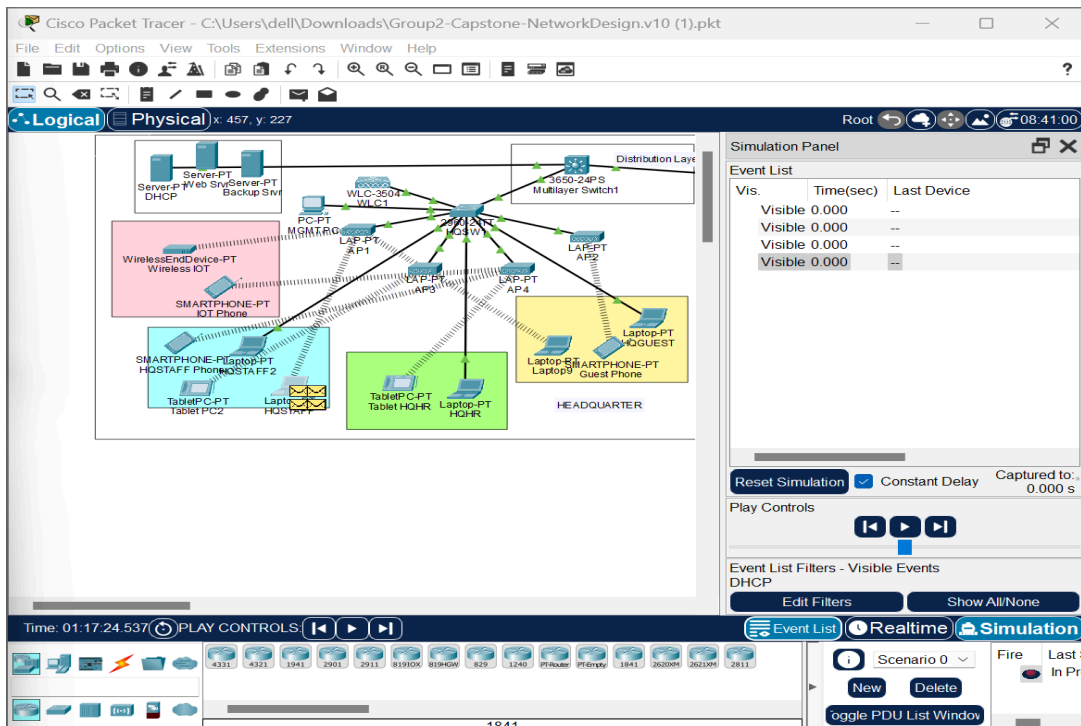
Testing DHCP in Real-Time Simulation Mode

1. Switch to **Real-Time Simulation** mode in Packet Tracer.
2. On the Client PC, click **Renew DHCP**.



3. Observe the DHCP process in real-time:
 - A **DHCP Discover** packet is sent from the client to R2.
 - R2 forwards the request (as a DHCP relay) to the DHCP server via R1.
 - The server responds with a **DHCP Offer**.

- The client receives an IP address (e.g., 192.168.3.x) from the server.



Dynamic Host Configuration Protocol (DHCP) is a critical network service that automates IP address assignment and configuration for devices on a network. While DHCP simplifies device connectivity, it can introduce vulnerabilities if not managed securely. Integrating DHCP into a **Zero Trust Security (ZTS)** model requires securing the protocol itself while continuously verifying device identity, health, and access permissions.

Micro-Segmentation and Contextual IP Allocation

- **Segment the Network:**

- Combine DHCP with **micro-segmentation** to restrict IP address ranges for different device types or roles.
- Example: IoT devices get IPs in a separate VLAN from corporate laptops
- **Logging and Monitoring**
 - Anomaly Detection–Use SIEM (Security Information and Event Management) tools to analyze DHCP logs for:
 - Repeated DHCP requests from the same MAC address (possible starvation attack).
 - Unusual IP assignments.

In a Zero Trust Security framework, DHCP must transition from a "trust-by-default" service to an **authenticated and monitored process**. By integrating DHCP with tools like NAC, micro-segmentation, and continuous monitoring, organizations can ensure that only verified devices receive IP addresses and access network resources.

Disabling SSID Broadcast

Disabling the broadcasting of your **SSID (Service Set Identifier)** is a security practice that can make your wireless network less visible to casual attackers. Disabling **SSID broadcasting** is a technique used to make your Wi-Fi network less visible by not advertising its presence to devices nearby. While it is a basic method for improving wireless security, it aligns with **Zero Trust Security (ZTS)** principles when combined with advanced security measures.

What Happens When You Disable SSID Broadcasting?

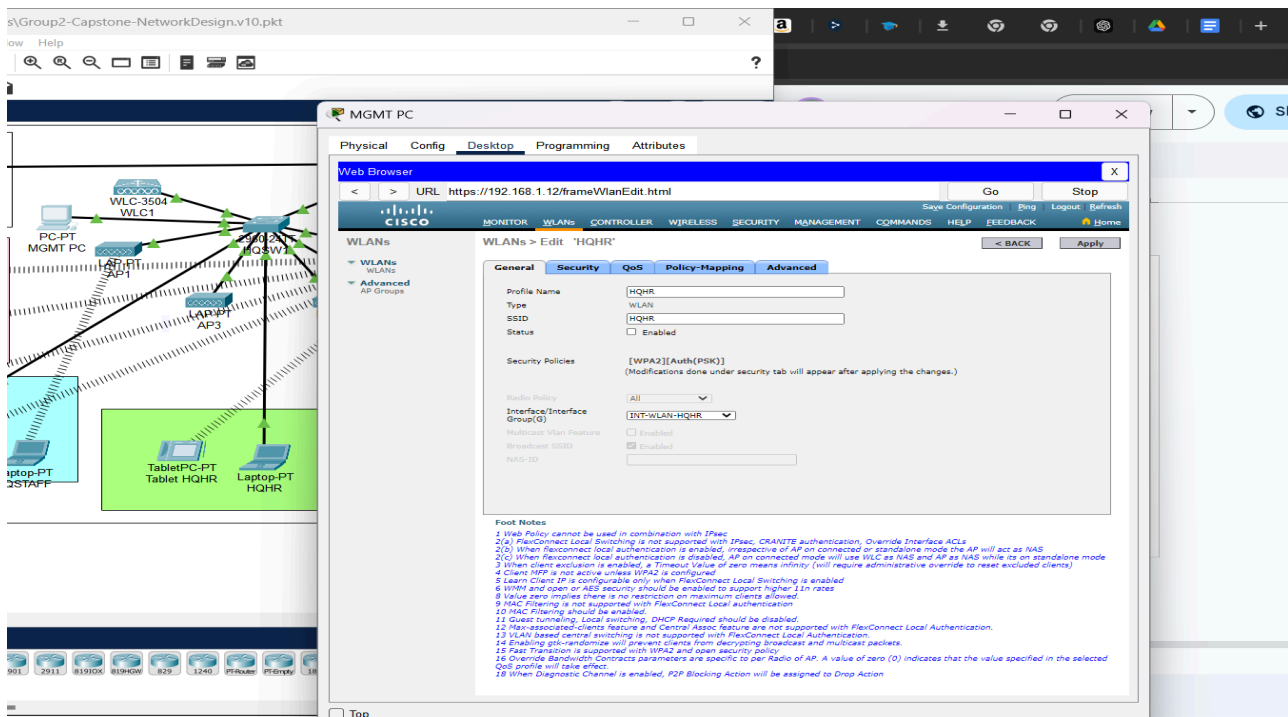
1. **The SSID becomes "hidden"**: Devices won't automatically see your network in the list of available Wi-Fi networks.
2. **Manual Connection Required**: Users must know the SSID name and enter it manually to connect.
3. **Added Security Layer**: While it doesn't prevent determined attackers (who can still sniff wireless traffic), it deters casual intruders.

Considerations and Limitations

- **Not Foolproof**: Tools like Wireshark or Kismet can still detect hidden SSIDs by sniffing network traffic, especially when devices try to connect.
- **User Convenience**: Disabling SSID broadcasting makes it harder for legitimate users to find and connect to your network.
- **Better Alternatives**:
 - Use **WPA3 or WPA2 encryption** for robust protection.
 - Enable **MAC address filtering** to limit which devices can connect.
 - Regularly change your network password.

Supports Network Segmentation:

- Hidden SSIDs can isolate sensitive segments of the network (e.g., IoT devices or guest access).
- Helps reinforce a **deny-by-default** posture, aligning with Zero Trust.



MAC Address Filtering in Wi-Fi for Zero Trust Security

While **MAC Address Filtering** is a traditional method to control which devices can connect to a network, integrating it into a **Zero Trust Security (ZTS)** framework involves enhancing and combining it with modern security practices. In a Zero Trust model, every access attempt—whether by users or devices—is continuously verified and never assumed to be trusted based solely on predefined criteria like MAC addresses.

Role of MAC Address Filtering in Zero Trust Security

Device Identification:

- MAC addresses provide a unique identifier for network devices, which can act as a basic layer of device recognition.
- Helps enforce **identity-based access control** for devices in addition to users.

First-Line Filtering:

- Acts as an initial checkpoint to block unknown or unregistered devices from even attempting to authenticate.
- Complements stronger verification processes, such as device health checks and certificate-based authentication.

Network Segmentation:

- By filtering MAC addresses, you can allow only specific devices into certain **micro-segmented areas** of the network.
- Works alongside Software-Defined Access (SDA) to isolate and limit access dynamically based on device trust levels.

Best Practices for Using MAC Address Filtering with Zero Trust Security

To integrate MAC filtering into a robust ZTS framework, consider the following enhancements:

1. Use MAC Filtering as an Additional Layer

- Combine MAC filtering with **Multi-Factor Authentication (MFA)** and **Identity and Access Management (IAM)**.
- Example:
 - A device with an allowed MAC address is still required to pass additional checks, such as user authentication and device compliance.

2. Combine with Network Access Control (NAC)

- Use **NAC solutions** to validate device compliance (e.g., OS version, antivirus status) in real-time.
- Only allow devices with approved MAC addresses *and* compliant configurations to access the network.
- Example:
 - Cisco ISE (Identity Services Engine) integrates MAC filtering with Zero Trust principles by continuously verifying device health and context.

3. Apply MAC Filtering to Micro-Segmented Networks

- Pair MAC filtering with **micro-segmentation** to limit device access to specific parts of the network.
- Allow only known MAC addresses in sensitive segments, such as databases or payment systems.
- Example:
 - IoT devices like cameras can be restricted to a dedicated VLAN with MAC filtering and no access to critical systems.

4. Use Certificates for Device Authentication

- Instead of relying solely on MAC addresses, issue **digital certificates** to approved devices.
- Certificates ensure a higher level of trust and are harder to spoof compared to MAC addresses.

5. Regularly Update and Audit MAC Address Lists

- Automate updates to the MAC filter list using centralized tools.
- Periodically audit and remove unused or deprecated MAC addresses to reduce attack surfaces.

MAC Address Filtering alone is not sufficient for implementing Zero Trust Security but can act as a foundational control when combined with dynamic and context-aware security measures like NAC, 802.1X authentication, and device certificates. By incorporating these practices, you ensure that your Zero Trust environment remains flexible, scalable, and resistant to modern threats.

Summary of MAC Filtering in Zero Trust Security

Aspect	Traditional MAC Filtering	Zero Trust Enhanced MAC Filtering
Device Identification	Static MAC-based whitelist/blacklist	Continuous validation with certificates, NAC, and context
Access Scope	Allows/denies devices to entire network	Restricts devices to segmented network zones
Protection	Vulnerable to MAC spoofing	Combines with MFA, encryption, and device health checks
Management	Manual and error-prone	Automated updates and audits via centralized tools

Extended Access Control List (ACL) ON OUR REMOTE ROUTER

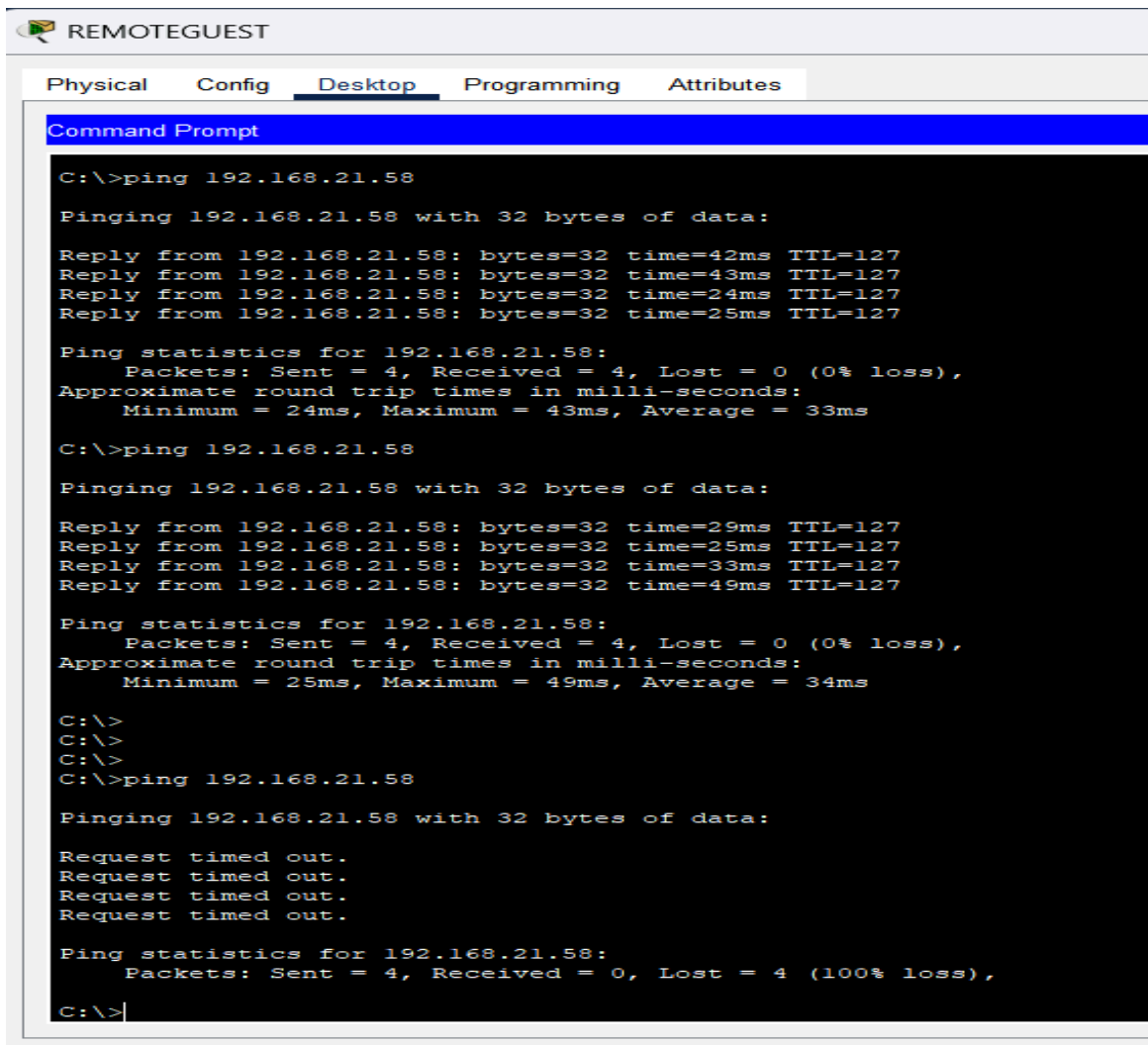
An Extended Access Control List (ACL) is a powerful feature on a router that allows filtering of traffic based on a wide range of criteria, such as:

- Source IP address
- Destination IP address
- Protocol type (e.g., TCP, UDP, ICMP)
- Port numbers (e.g., HTTP, SSH)

When to Use Extended ACLs

Extended ACLs are ideal for implementing fine-grained traffic filtering, for example:

- Allowing specific applications like HTTP or FTP.
- Restricting traffic between subnets.
- Enhancing security by blocking unwanted protocols or ports.



```
C:\>ping 192.168.21.58

Pinging 192.168.21.58 with 32 bytes of data:

Reply from 192.168.21.58: bytes=32 time=42ms TTL=127
Reply from 192.168.21.58: bytes=32 time=43ms TTL=127
Reply from 192.168.21.58: bytes=32 time=24ms TTL=127
Reply from 192.168.21.58: bytes=32 time=25ms TTL=127

Ping statistics for 192.168.21.58:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 24ms, Maximum = 43ms, Average = 33ms

C:\>ping 192.168.21.58

Pinging 192.168.21.58 with 32 bytes of data:

Reply from 192.168.21.58: bytes=32 time=29ms TTL=127
Reply from 192.168.21.58: bytes=32 time=25ms TTL=127
Reply from 192.168.21.58: bytes=32 time=33ms TTL=127
Reply from 192.168.21.58: bytes=32 time=49ms TTL=127

Ping statistics for 192.168.21.58:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 25ms, Maximum = 49ms, Average = 34ms

C:\>
C:\>
C:\>
C:\>ping 192.168.21.58

Pinging 192.168.21.58 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.21.58:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Applied to RemoteR1 router to Prevent the Guest from reaching the internal network.

REMOTER1#sh ip access-lists

Extended IP access list 101

10 deny icmp 192.168.21.0 0.0.0.255 192.168.2.0 0.0.0.255 echo

20 deny icmp 192.168.22.0 0.0.0.255 192.168.2.0 0.0.0.255 echo

30 permit ip any any

Ping not working after ACL was applied.

Best Practices for Extended ACLs

1. Place extended ACLs close to the source to filter unwanted traffic early and save bandwidth.
2. Use descriptive names when possible for easier management.
3. Add logging to critical deny rules for monitoring and auditing.
4. Organize rules from specific to general for efficient processing.
5. Regularly review and optimize ACLs to prevent rule bloat.

Benefit of Software-Defined Networking (SDN), Zero Trust, and SASE Network

1. Strengthened Security:

- Proactively address threats through Zero Trust and SASE's identity-driven, end-to-end protection.
- Improve incident detection and response with AI-powered monitoring and analytics.

2. Enhanced Performance:

- Reduce latency and boost application performance through SASE's edge architecture.
- Automate network configuration and fault resolution for uninterrupted operations.

3. Cost Efficiency:

- Consolidate network and security solutions, reducing complexity and operational costs.
- Optimize resource utilization with on-demand scaling.

4. Future-Ready Framework:

- Support emerging technologies such as IoT, AI, and multi-cloud environments.
- Ensure compliance with evolving regulatory standards.

Conclusion

By integrating SDN, Zero Trust, and SASE, this network refresh provides a holistic solution that enhances security, performance, and scalability. The organization will benefit from a future-proof, cloud-ready infrastructure capable of supporting innovation, remote work, and digital transformation.