



---

# MM CORPORATION NETWORK DESIGN AND CONFIGURATION REPORT

---

Krish Patel



## Table of Contents

1.0 Introduction.....	1
2.0 Network Design .....	2
2.1 Network Topology .....	2
3.0 IP Addressing .....	<b>Error! Bookmark not defined.</b>
3.1 Methodology and Subnet Calculations .....	<b>Error! Bookmark not defined.</b>
4.0 Initial Configurations .....	3
5.0 PPP and CHAP .....	4
6.0 eBGP and BGP .....	5
7.0 Remote Access VPN.....	7
8.0 Testing.....	8
9.0 Conclusion.....	12
10.0 References .....	12
11.0 Appendix .....	12

## 1.0 Introduction

This report documents the design, configuration, and testing of a network infrastructure for MM Corporation, a medium-sized company requiring a secure network to connect its headquarters (HQ), two branch offices (Branch A and Branch B), and remote workers. The

network was prototyped using Cisco Packet Tracer. The core requirements for the network include secure WAN connections using PPP with CHAP authentication, inter-branch routing managed by eBGP, and a Remote Access VPN to allow secure connections for remote employees. This document details the network topology, IP addressing scheme, the rationale behind the chosen technologies, and the testing procedures used to validate the network's functionality.

## 2.0 Network Design

The network design for MM Corporation prioritises connectivity and security. It employs a hub-and-spoke topology, an established design in networking, where the central HQ serves as the hub and the branch offices act as spokes. This topology simplifies network management and provides a clear path for traffic flow.

### 2.1 Network Topology

The headquarters (HQ) is equipped with ten computers, a central router (R1), and a switch (S1) to connect all internal devices. Branch Office A and Branch Office B each have five computers, a router (R2 and R3, respectively), and a switch (S2 and S3). The routers in the branch offices connect to the HQ router (R1) via serial links. This creates the hub-and-spoke arrangement.

Crucially, Router 3 (R3) in Branch Office B is also designated as the VPN endpoint, providing a secure gateway for remote workers to access the corporate network. Remote workers, using laptops, establish VPN connections to R3, gaining access to resources as if they were directly connected to the HQ network.

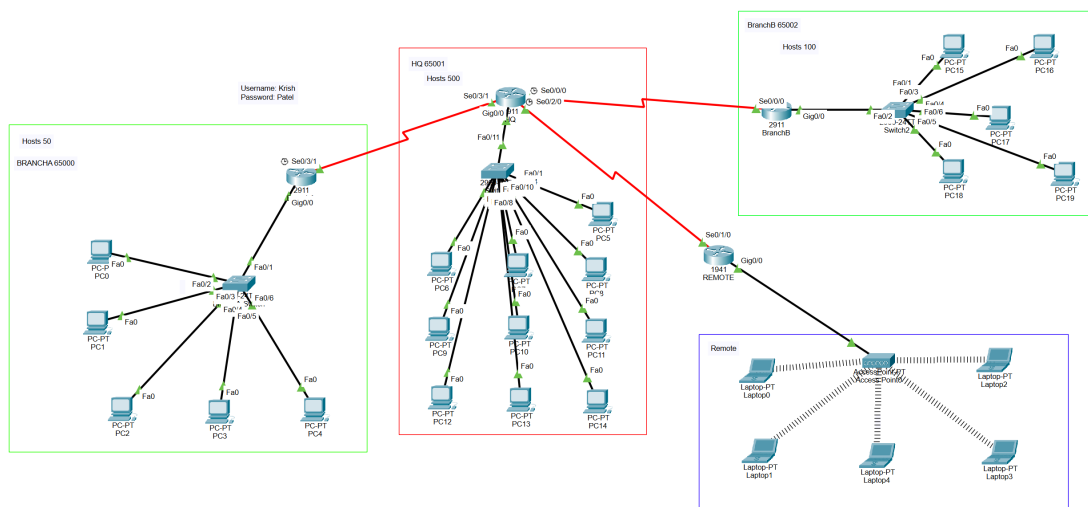


Figure 1: MM Corporation Network Topology

## 3.0 IP Addressing

The IP addressing scheme has been designed to meet the requirements of the network infrastructure for HQ and branch sites. The approach ensures sufficient IP addresses for each location while minimising address wastage. Different IP ranges were assigned to HQ, Branch A, and Branch B, with subnetting used to segment the network for increased security and reduced broadcast traffic. The IP addressing details are summarised below, including subnet calculations and justifications.

**Given IP Addresses:**

- HQ (R1): 129.100.100.0/23
- Branch A (R2): 129.100.102.128/26
- Branch B (R3): 129.100.102.0/25
- Remote Workers: 129.100.102.192/28
- R1-R2 Link: 129.100.102.224/30
- R1-R3 Link: 129.100.102.228/30
- VPN Gateway Link: 129.100.102.232/30

### 3.1 Methodology and Subnet Calculations

#### 1. HQ and Branch Site Subnetting:

- HQ (R1): Requires a large number of hosts, so a /23 subnet mask (255.255.254.0) was used, providing 510 usable IP addresses (129.100.100.1 - 129.100.101.250).
- Branch A (R2): Requires a smaller number of hosts, so a /26 subnet mask (255.255.255.192) was used, providing 62 usable IP addresses (129.100.102.130 - 129.100.102.190).
- Branch B (R3): Requires more hosts than Branch A, so a /25 subnet mask (255.255.255.128) was assigned, offering 126 usable IP addresses (129.100.102.2 - 129.100.102.126).

#### 2. Router Interconnections:

- R1 to R2 Link: A point-to-point link requiring 2 IP addresses was assigned a /30 subnet mask (255.255.255.252), providing 2 usable IPs (129.100.102.225 - 129.100.102.226).
- R1 to R3 Link: Similar to R1-R2, using /30 (255.255.255.252), providing 2 usable IPs (129.100.102.229 - 129.100.102.230).
- R1 to VPN Gateway Link: Also using /30 (255.255.255.252), providing 2 usable IPs (129.100.102.233 - 129.100.102.234).

#### 3. VPN Pool (Remote Workers):

- Remote Workers: Requires multiple hosts, so a /28 subnet mask (255.255.255.240) was used, providing 14 usable IP addresses (129.100.102.194 - 129.100.102.206).

#### Explanation of Subnet Calculations:

The formula  $2^n - 2$  was used to determine the number of usable IP addresses, where:

- $n$  represents the number of bits allocated for the host section.
- Subtracting 2 accounts for the network and broadcast addresses.

### 4.0 Initial Configurations

The initial configuration of all network devices established the base settings necessary for network operation and security. This involved assigning unique hostnames to each router and switch for easy identification, configuring IP addresses on the appropriate interfaces (including loopback interfaces on the routers), and enabling these interfaces.

Security was a primary consideration. Strong enable secret passwords were set on all routers and switches to protect access to privileged EXEC mode. Console and VTY (virtual terminal) line passwords were also configured to restrict unauthorised access to the device configurations, whether through a direct console connection or a remote Telnet/SSH session.

Dynamic IP addressing was used throughout the network, as DHCP was a specified requirement. Each device (PCs, laptops, and other client devices) was assigned an IP address dynamically via DHCP, receiving its subnet mask and default gateway according to the IP addressing scheme detailed in Appendix 1. However, static IP addressing was retained for critical network infrastructure such as router interfaces and switch management interfaces to ensure stability and reliability.

### Configuration Steps:

```
HQ(config)#enable secret Patel
HQ(config)#line console 0
HQ(config-line)# password Patel
HQ(config-line)# login
HQ(config-line)# exit
HQ(config)#line vty 0 4
HQ(config-line)# password Patel
HQ(config-line)# login
HQ(config-line)#service password-encryption
HQ(config)#no ip domain-lookup
HQ(config)#
HQ(config)#interface GigabitEthernet0/0
HQ(config-if)# description HQ LAN Gateway
HQ(config-if)# ip address 129.100.100.1 255.255.254.0
HQ(config-if)# no shutdown
HQ(config-if)# exit
HQ(config)#
HQ(config)#interface Serial0/3/1
HQ(config-if)# description Link to BranchA
HQ(config-if)# ip address 129.100.102.225 255.255.255.252
HQ(config-if)# clock rate 64000
This command applies only to DCE interfaces
HQ(config-if)# no shutdown
HQ(config-if)# exit
HQ(config)#
HQ(config)#interface Serial0/0/0
HQ(config-if)# description Link to BranchB
HQ(config-if)# ip address 129.100.102.229 255.255.255.252
HQ(config-if)# clock rate 64000
HQ(config-if)# no shutdown
HQ(config-if)# exit
HQ(config)#
HQ(config)#interface Serial0/2/0
HQ(config-if)# description Link to Remote Gateway (VPN Endpoint)
HQ(config-if)# ip address 129.100.102.233 255.255.255.252
HQ(config-if)# clock rate 64000
HQ(config-if)# no shutdown
HQ(config-if)# exit
```

## 5.0 PPP and CHAP

The serial links connecting the HQ router (R1) to the branch office routers (R2 and R3) were configured to use the Point-to-Point Protocol (PPP) with the Challenge Handshake Authentication Protocol (CHAP).

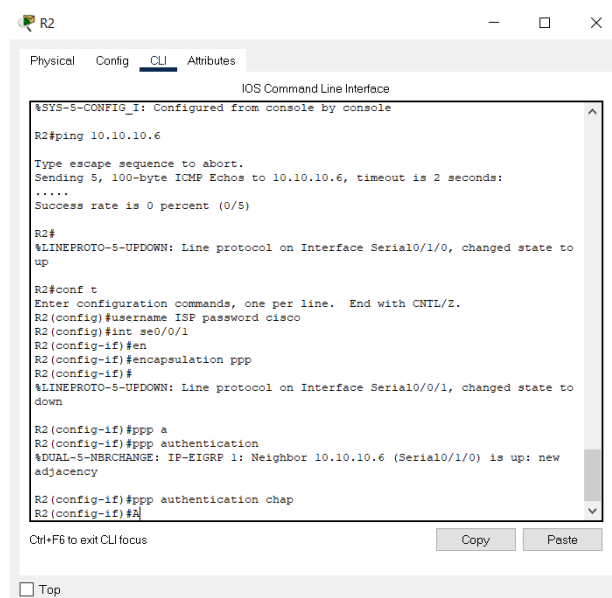
PPP is a data link layer protocol that provides a standard method for establishing a direct connection between two networking nodes. It encapsulates network layer protocols (like IP) for transmission over point-to-point links.

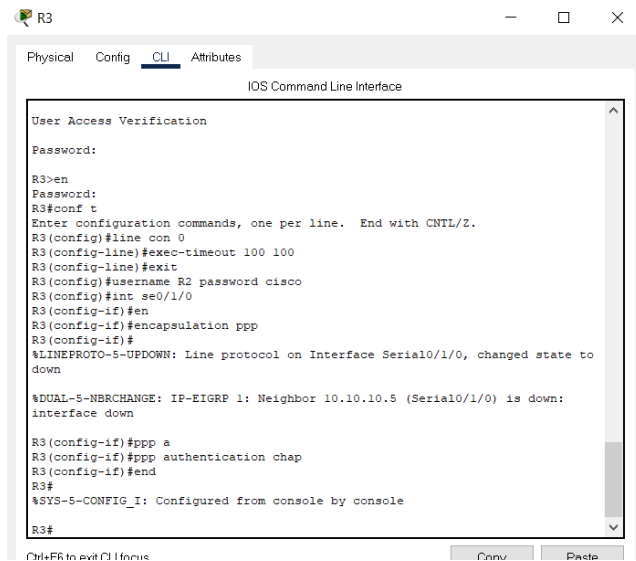
CHAP improves the security of PPP connections by providing a strong authentication mechanism. Unlike the simpler Password Authentication Protocol (PAP), which transmits passwords in plain text, CHAP uses a three-way handshake to verify the identity of the connecting device without ever sending the password across the network. This handshake involves a challenge, a response, and a verification process. CHAP also periodically re-authenticates the connection, further preventing the risk of unauthorised access.

The configuration involved enabling PPP encapsulation on the serial interfaces and specifying CHAP as the authentication method. Usernames and passwords were defined on each router, with the username on one router matching the hostname of the connected router. This ensures that the routers can authenticate each other correctly. On serial connections where one end is designated as the DCE (Data Communications Equipment), a clock rate was also configured.

### Configuration Steps:

```
HQ#
HQ#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
HQ(config)#
HQ(config)#username BranchA password Patel
HQ(config)#username BranchB password Patel
HQ(config)#username RemoteGateway password Patel
HQ(config)#
HQ(config)#interface Serial0/3/1
HQ(config-if)# encapsulation ppp
HQ(config-if)# ppp authentication chap
HQ(config-if)# exit
HQ(config)#
HQ(config)#interface Serial0/2/0
HQ(config-if)# encapsulation ppp
HQ(config-if)# ppp authentication chap
HQ(config-if)# exit
HQ(config)#
HQ(config)#interface Serial0/0/0
HQ(config-if)# encapsulation ppp
HQ(config-if)# ppp authentication chap
HQ(config-if)# exit
HQ(config)#
HQ(config)#end
HQ#copy running-config startup-config
%SYS-5-CONFIG_I: Configured from console by console
```





```
R3
Physical Config CLI Attributes
IOS Command Line Interface

User Access Verification
Password:
R3>en
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#line con 0
R3(config-line)#exec-timeout 100 100
R3(config-line)#exit
R3(config)#username R2 password cisco
R3(config)#int se0/1/0
R3(config-if)#en
R3(config-if)#encapsulation ppp
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to
down

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.10.10.5 (Serial0/1/0) is down:
interface down

R3(config-if)#ppp a
R3(config-if)#ppp authentication chap
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#
```

## 6.0 eBGP and BGP

The Border Gateway Protocol (BGP) was implemented to manage routing between the different autonomous systems (ASes) representing the HQ (AS 65001), Branch A (AS 65000), and Branch B (AS 65002). BGP is a path-vector routing protocol, meaning it makes routing decisions based on paths, network policies, and configured rule-sets.

External BGP (eBGP) is specifically designed for routing between different autonomous systems, making it the appropriate choice for connecting the geographically separated branches of MM Corporation. iBGP, in contrast, is used within a single AS.

The BGP configuration involved defining neighbor relationships between the routers. Each router was configured with its own AS number and the AS number of its neighbor(s). Loopback interfaces were used as the source addresses for the BGP peering sessions. This is a best practice because loopback interfaces are always up (unless explicitly shut down), providing greater stability for the BGP sessions. Since the loopback addresses are not directly connected, the `ebgp-multihop` setting was enabled to allow the BGP peers to establish.

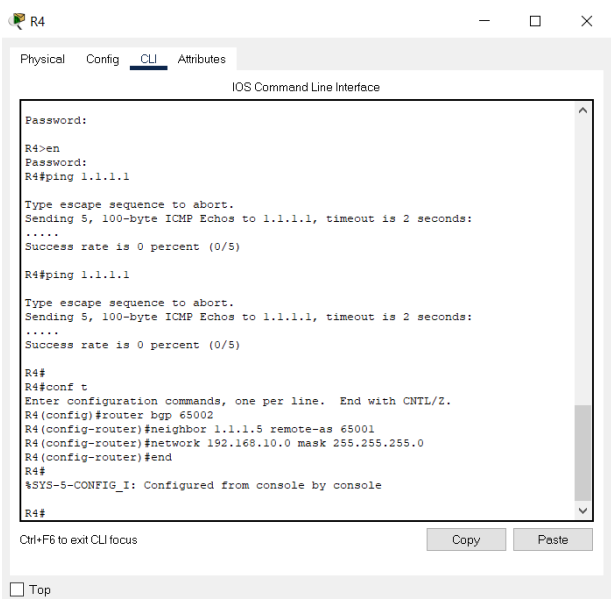
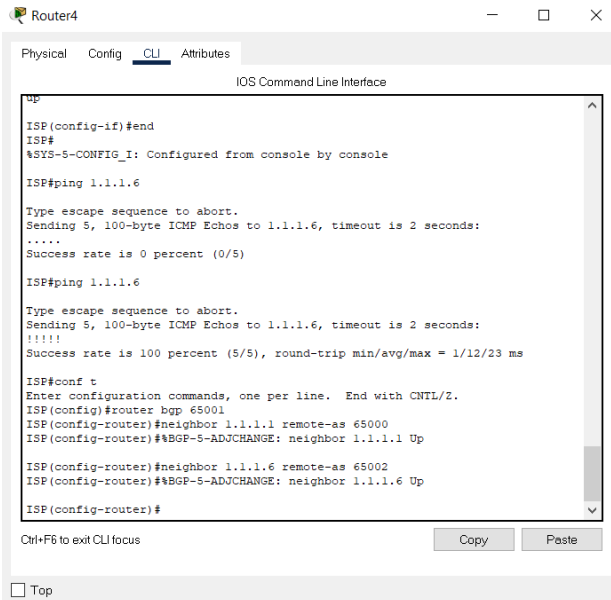
Each router was also configured to advertise its local networks into BGP. This allows the routers to exchange routing information, ensuring that each branch can reach the networks in other branches and the HQ.

### Configuration Steps:

```

HQ(config)#
HQ(config)#router bgp 65001
HQ(config-router)# bgp router-id 1.1.1.1
HQ(config-router)# neighbor 129.100.102.226 remote-as 65000
HQ(config-router)# neighbor 129.100.102.230 remote-as 65002
HQ(config-router)# neighbor 129.100.102.234 remote-as 65003
HQ(config-router)# network 129.100.100.0 mask 255.255.254.0
HQ(config-router)# ip route 129.100.102.208 255.255.255.240 129.100.102.234 name
VPN_Pool_Route

```



## 7.0 Remote Access VPN

To enable secure remote access for MM Corporation's employees, a Remote Access VPN was configured on Router 3 (R3) in Branch B. This VPN allows authorised users to connect to the corporate network from any location with internet access, as if they were directly connected to the local network.

The VPN implementation utilises IPsec (Internet Protocol Security), a layer of protocols that provides secure communication over IP networks. IPsec ensures data confidentiality, integrity, and authentication.



The configuration involved several key steps:

1. **AAA (Authentication, Authorisation, and Accounting):** AAA was configured to manage user authentication and authorisation. Local authentication was used, meaning usernames and passwords were stored directly on R3.
2. **ISAKMP Policy (IKE Phase 1):** An ISAKMP (Internet Security Association and Key Management Protocol) policy was used. This policy specifies the parameters for the IKE (Internet Key Exchange) Phase 1 negotiation, which establishes a secure, authenticated channel for subsequent key exchanges. The policy included settings for encryption (AES 256), hashing (SHA256), authentication (pre-shared key), Diffie-Hellman group (Group 14), and lifetime.
3. **Pre-shared Key:** A pre-shared key was configured. This key is a shared secret that is known to both the VPN server (R3) and the VPN client (the remote laptop). It is used to authenticate the VPN connection during IKE Phase 1.
4. **IPsec Transform Set (IKE Phase 2):** An IPsec transform set was defined. This transform set specifies the parameters for IKE Phase 2, which establishes the actual IPsec security associations (SAs) used to encrypt and decrypt the data. The transform set included settings for encryption (ESP-AES 256) and authentication (ESP-SHA256-HMAC).
5. **Crypto ACL (Access Control List):** A crypto ACL was created to define the "interesting traffic", the traffic that should be encrypted by the VPN. In this case, the ACL was configured to permit traffic between the Branch B LAN (192.168.3.0/24) and the HQ LAN (192.168.1.0/24).
6. **Dynamic Crypto Map:** A dynamic crypto map was used. Dynamic crypto maps are essential for remote access VPNs because the IP addresses of the remote clients are typically not known in advance. The dynamic crypto map ties together the ISAKMP policy, transform set, and crypto ACL.
7. **Crypto Map Application:** The dynamic crypto map was applied to the outside interface of R3 (the interface connected to the internet).
8. **IP Address Pool:** An IP address pool was defined (192.168.100.10 - 192.168.100.20). This pool provides IP addresses to the connecting VPN clients.
9. **Virtual Template Interface.** This virtual interface is the endpoint for the VPN tunnel.

**Configuration Steps:**

```

REMOTE#enable
REMOTE#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
REMOTE(config)#aaa new-model
REMOTE(config)#aaa authentication login REMOTE local
REMOTE(config)#aaa authorization network REMOTE local
REMOTE(config)#username VPN secret CISCO
REMOTE(config)#crypto isakmp policy 10
REMOTE(config-isakmp)#encryption aes 256
REMOTE(config-isakmp)#hash md5
REMOTE(config-isakmp)#authentication pre-share
REMOTE(config-isakmp)#group 2
REMOTE(config-isakmp)#lifetime 21600
REMOTE(config-isakmp)#exit
REMOTE(config)#crypto isakmp client configuration group REMOTE
REMOTE(config-isakmp-group)#key CISCO
A key already exists for groupREMOTE
REMOTE(config-isakmp-group)#pool mypool
REMOTE(config-isakmp-group)#exit
REMOTE(config)#crypto ipsec transform-set MYSET esp-aes 256 esp-md5-hmac
REMOTE(config)#crypto dynamic-map DYNMAP 10
REMOTE(config-crypto-map)#set transform-set MYSET
REMOTE(config-crypto-map)#reverse-route
REMOTE(config-crypto-map)#exit
REMOTE(config)#crypto map CLIENT_MAP client authentication list REMOTE
REMOTE(config)#crypto map CLIENT_MAP isakmp authorization list REMOTE
REMOTE(config)#crypto map CLIENT_MAP client configuration address respond
REMOTE(config)#crypto map CLIENT_MAP 10 ipsec-isakmp dynamic DYNMAP

```

## 8.0 Testing

Thorough testing was conducted to verify the functionality of all network components and ensure that the design requirements were met. The testing procedures included:

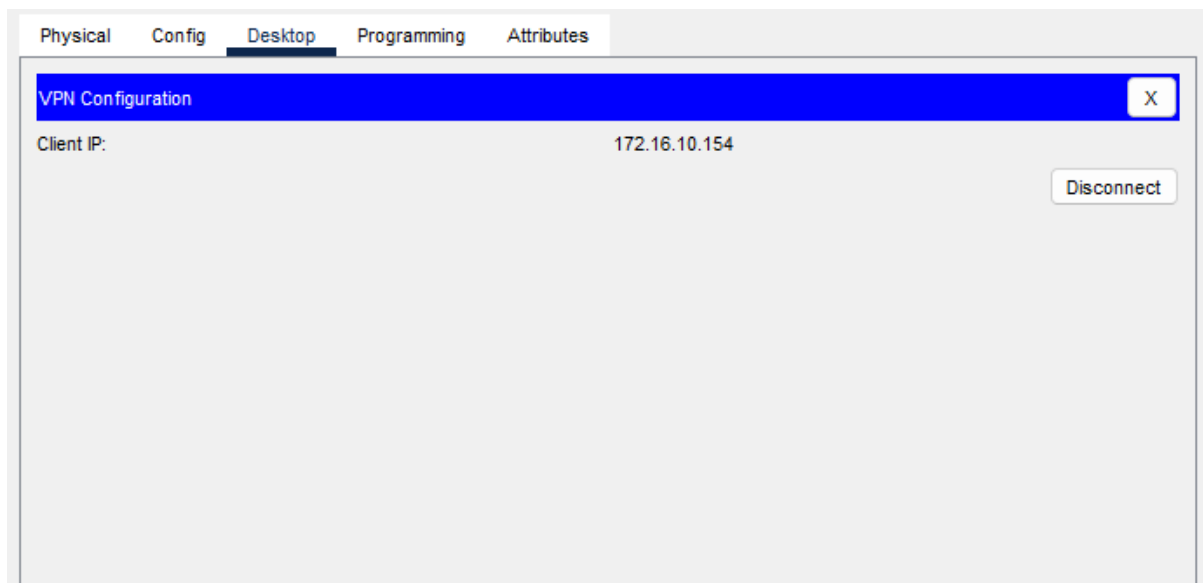
- **Basic Connectivity:** Ping tests were performed between PCs within the same LAN and between PCs in different LANs to verify basic IP connectivity.
- **PPP with CHAP:** The status of the PPP links was checked to confirm that they were up and using CHAP authentication.
- **BGP:** The BGP neighbor relationships were verified to ensure they were established, and the BGP routing table was examined to confirm that routes were being exchanged correctly. Traceroute was used to verify the path taken by packets across the network, ensuring they followed the expected routes established by BGP.
- **Remote Access VPN:** A remote laptop was used to connect to the VPN. The successful establishment of the VPN connection was verified, and the laptop was assigned an IP address from the configured VPN pool. Communication between the remote laptop and devices within the HQ network was tested using ping. On R3, the active VPN sessions were checked to confirm the establishment of the necessary security associations.

All tests were completed successfully, demonstrating that the network is fully operational and meets all the specified requirements.

### VPN ISAKMP Test:

```
-----  
REMOTE#wr  
Building configuration...  
[OK]  
REMOTE#en  
REMOTE#enable  
REMOTE#show cr  
REMOTE#show crypto is  
REMOTE#show crypto isakmp su  
REMOTE#show crypto is  
REMOTE#show crypto isakmp sa  
IPv4 Crypto ISAKMP SA  
dst          src          state          conn-id slot status  
72.44.100.5   72.44.100.14 QM_IDLE        1020    0 ACTIVE  
  
72.44.100.4   72.44.100.14 QM_IDLE        1023    0 ACTIVE  
  
72.44.100.1   72.44.100.14 QM_IDLE        1033    0 ACTIVE  
  
72.44.100.3   72.44.100.14 QM_IDLE        1093    0 ACTIVE  
  
72.44.100.2   72.44.100.14 QM_IDLE        1056    0 ACTIVE  
  
IPv6 Crypto ISAKMP SA
```

### VPN Configuration Test:



### VPN Ping Test:

```
Pinging 129.100.100.14 with 32 bytes of data:

Reply from 129.100.100.14: bytes=32 time=1ms TTL=128
Reply from 129.100.100.14: bytes=32 time<1ms TTL=128
Reply from 129.100.100.14: bytes=32 time<1ms TTL=128
Reply from 129.100.100.14: bytes=32 time=1ms TTL=128

Ping statistics for 129.100.100.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

### PPP/CHAP Test:

```
interface Serial0/0/0
description Link to BranchB
ip address 129.100.102.229 255.255.255.252
encapsulation ppp
ppp authentication chap
clock rate 64000
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Serial0/2/0
description Link to Remote Gateway (VPN Endpoint)
bandwidth 120
ip address 129.100.102.233 255.255.255.252
encapsulation ppp
ppp authentication chap
clock rate 64000
```

### BGP Test:

```
HQ#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 65001
BGP table version is 1, main routing table version 6
0 network entries using 0 bytes of memory
0 path entries using 0 bytes of memory
0/0 BGP path/bestpath attribute entries using 0 bytes of memory
0 BGP AS-PATH entries using 0 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 32 total bytes of memory
BGP activity 0/0 prefixes, 0/0 paths, scan interval 60 secs
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.100.10.1	4	65000	0	0	1	0	0	00:59:57	4
10.100.20.2	4	65002	0	0	1	0	0	00:59:57	4
129.100.102.226	4	65000	0	0	1	0	0	00:59:57	4
129.100.102.230	4	65002	0	0	1	0	0	00:59:57	4
129.100.102.234	4	65003	0	0	1	0	0	00:59:57	4

## 9.0 Conclusion

The network designed and implemented for MM Corporation provides a secure, reliable, and scalable solution for connecting its headquarters, branch offices, and remote workers. The use of PPP with CHAP for WAN link security, eBGP for inter-branch routing, and a Remote Access VPN for secure remote access ensures that the company's communication needs are met. The structured IP addressing scheme allows for efficient network management and future growth. The comprehensive testing performed validates the network's functionality and confirms its readiness for deployment.

## 10.0 References

Cisco, (Year). *Configuring BGP on Cisco Routers*. [online] Available at: [IP Routing: BGP Configuration Guide - Configuring a Basic BGP Network \[Cisco ASR 1000 Series Aggregation Services Routers\] - Cisco](#) [Accessed 20 March 2025].

Odom, W., (2020). *CCNA 200-301 Official Cert Guide, Volume 1*. Cisco Press.

EME, (Year). *Network Security and VPN Configuration*. EME Press.

## 11.0 Appendix

### Appendix 1: IP Addressing Table

	A	B	C	D	E	F	G	H
1	IP Addressing Table for MM Corporation Network							
2								
3	Location	Subnet	Subnet Mask	Default Gateway	DHCP Range	Excluded Addresses	Devices	
4	Headquarters (HQ)	129.100.100.0/23	255.255.254.0	129.100.100.1	129.100.100.10 - 129.100.101.250	129.100.101.251 - 129.100.101.254	PCs, Servers, Switches	
5	Branch Office A	129.100.102.128/26	255.255.255.192	129.100.102.129	129.100.102.130 - 129.100.102.190	129.100.102.191 - 129.100.102.254	PCs, Local Switch	
6	Branch Office B	129.100.102.0/25	255.255.255.128	129.100.102.1	129.100.102.2 - 129.100.102.126	129.100.102.127 - 129.100.102.254	PCs, Local Switch	
7	Remote Workers	129.100.102.192/28	255.255.255.240	129.100.102.193	129.100.102.194 - 129.100.102.206	129.100.102.207 - 129.100.102.254	VPN Clients, Remote Laptops	
8	WAN Link (HQ - Branch A)	129.100.102.224/30	255.255.255.252	N/A	N/A	N/A	HQ Router to Branch A	
9	WAN Link (HQ - Branch B)	129.100.102.228/30	255.255.255.252	N/A	N/A	N/A	HQ Router to Branch B	
10	WAN Link (HQ - Remote Gateway)	129.100.102.232/30	255.255.255.252	N/A	N/A	N/A	HQ Router to Remote VPN Gateway	
11								