University of Alberta

Department
Of
Electrical and Computer Engineering

Enterprise Based VPN

SUBMITTED BY:
VEER BAHADUR SINGH THIARA

Table of Contents

Abstract

VPN (Virtual Private Network) as the name suggests is a is a network that is virtual and is constructed over already established network like Internet and helps connecting internal network of a company at one site to internal network of company at another site. This method provides secure access from a company branch to there headquarters. It guarantees that the Data, which can be sensitive data for the company is being sent and received, encrypted and is safe from attacks. VPN provides confidentiality, authentication, and integrity. VPN can be set up using different protocols like IPSec, Transport Layer Security, Secure Socket Tunneling Protocol etc. Protocols like Transport Layer Security, Secure Socket Tunneling Protocol provides data security and privacy between two computer applications that are communicating. Models used to implement VPN are overlay and Peer to peer. Tunnels that being implemented in this project are based on Cisco IOS such as IP sec and DMVPN.

Acknowledgment

I wish to express my sincere gratitude to Dr. Mike MacGregor and MR. Shawnawaz Mir for providing me an opportunity to do my Masters in internetworking and project “Enterprise Based VPN”.

I sincerely thank Mr. Arsh Saini for his guidance and encouragement in carrying out this project work. I also wish to express my gratitude to my friends and staff of MINT who rendered their help during the period of my project work.

I also like to thank my family who supported me in my project work.

VPN

1.1 Introduction

A VPN is defined virtual private network. It's a virtual network deployed on Shared infrastructure such as Internet but has the same performance as well as same policies as a private network.

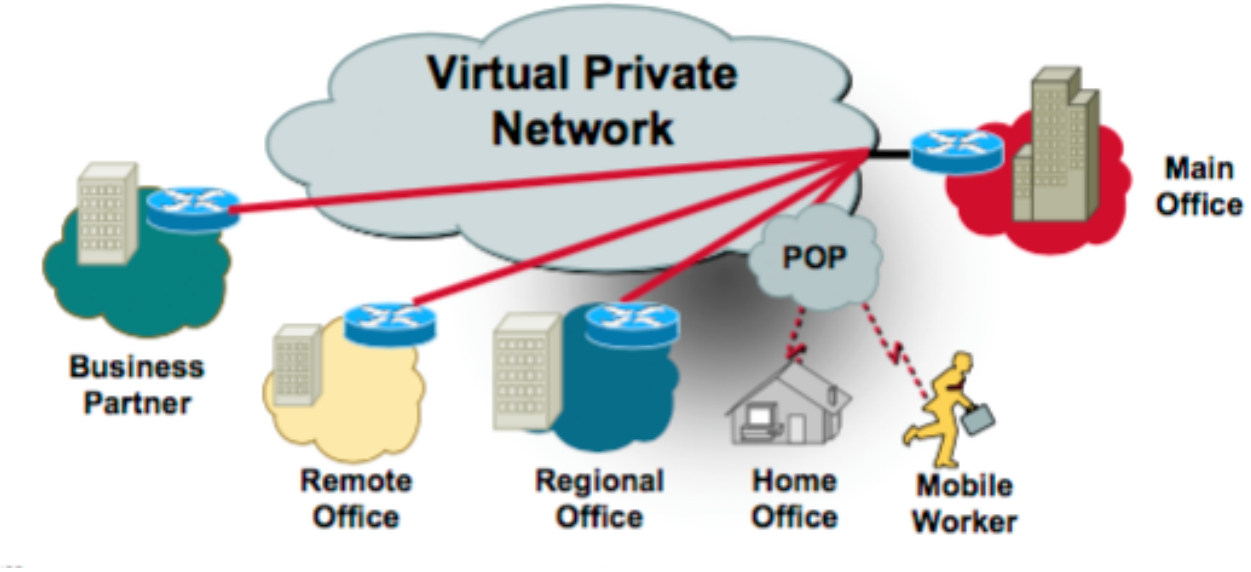

Figure 1. Virtual Private Network Usage [1] (Page 4)

Fig. 1 shows the VPN usage where a vpn is like a WAN that gives a private network for companies to connect with their remote sites. A classic WAN is a link from main office to remote offices. This approach of providing a dedicated link is not scalable as there are thousand of remote workers that need to connect to HQ of a company as well as other business partners. Fig. 2 shows VPN extending WAN VPN provides a way to extend the current network with the same policies as well as security for the organization.

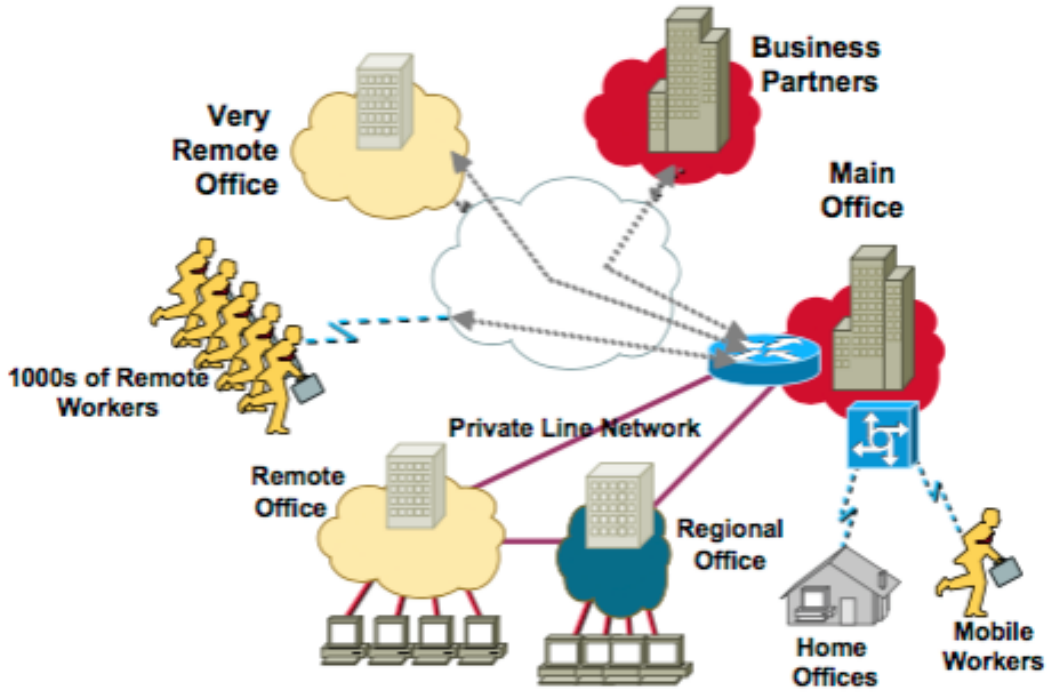

Figure 2. Virtual Private network with Dedicated WAN [1](page 6)

1.2 Categories of VPN

VPN can be divided into three categories:

1. Intranet VPN
2. Extranet VPN
3. Remote access VPN

Intranet VPN: Fig. 3 shows Intranet VPN where intranet VPN connects remote sites to there main office. VPN services such as IPSec, encryption and QOS are used to ensure reliable throughput. This also helps in cutting costs as costs associated with Frame Relay and leased lines is more as compared to VPN.

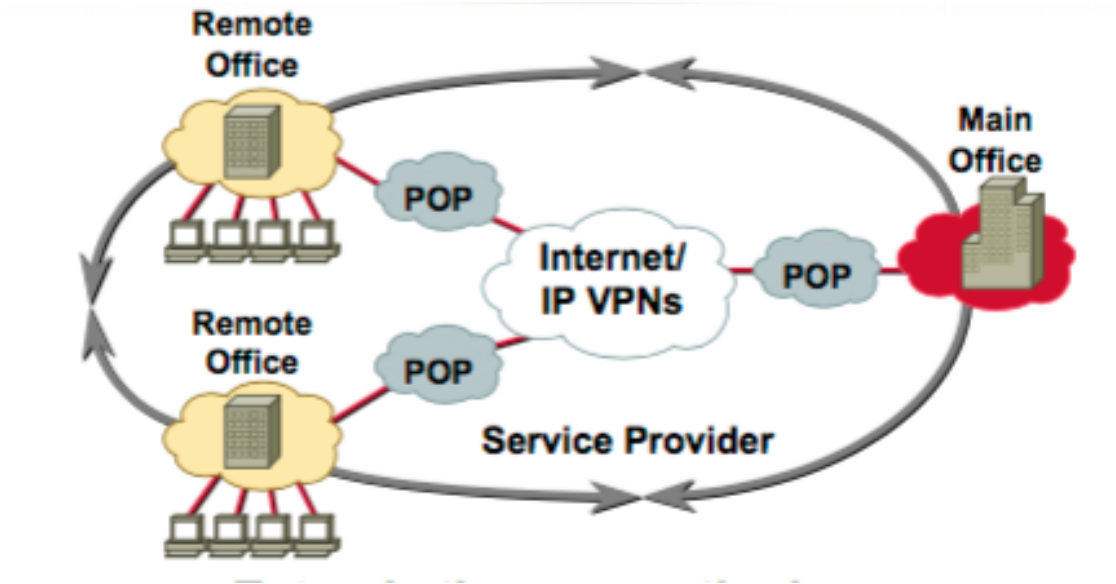

Figure 3. Intranet VPN [1] (page 13)

Extranet VPN: Fig. 4 shows extranet VPN where these VPN are extended WAN to business partners. These VPN extend connectivity to suppliers and customers. It is implemented over a shared infrastructure and using dedicated connections.

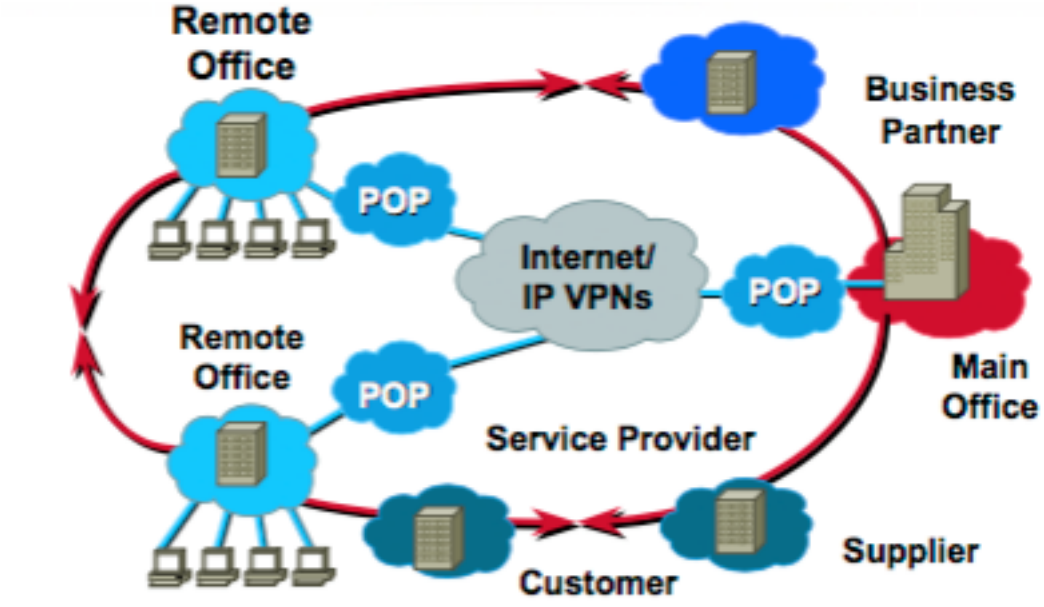

Figure 4. Extranet VPN [1] (page 14)

Remote Access VPN: These are scalable VPN tunnels as there can be thousands of remote workers. These VPN are established using client VPN software across a public network. IT provides cost saving over toll free numbers and other alternatives to connect to main office. Fig. 5 shows VPN usage for mobile client thus helping for scalability and mobility.

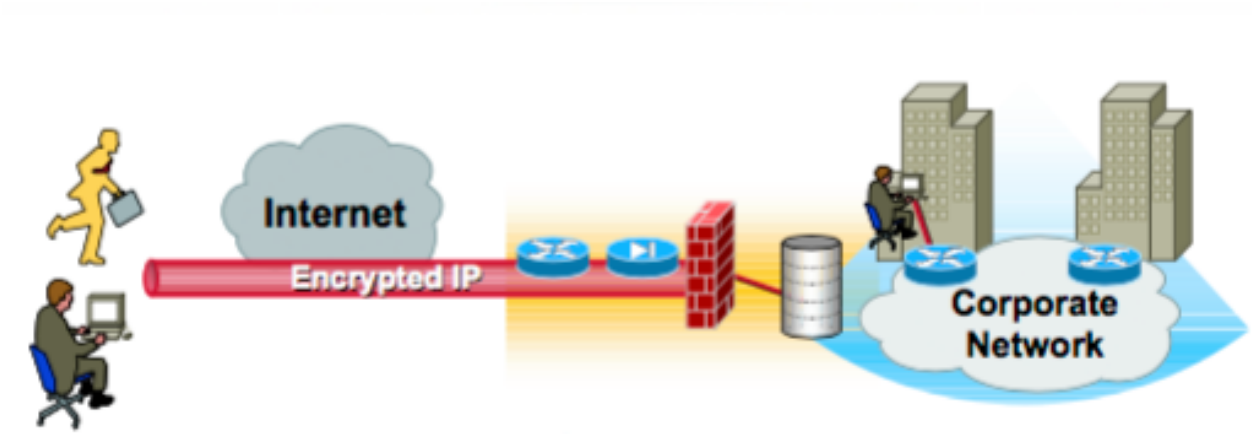

Figure 5. Mobile Client and VPN [1] (page 12)

VPN service can either be enterprise managed or service provider managed. Enterprise managed VPN the enterprise is responsible for QOS, security and configuration of VPN functions whereas service provider just provides basic VPN connectivity.

Service provider managed vpn, the enterprise controls security and also outsources design provisioning and management whereas service provider provides VPN.

VPN can be either between router and firewall, router to router, PC to server and PC to router etc. these IETF standard enables encrypted communication between these users and devices. Open standard enables multivendor interoperability. One such standard is IPSec.

DMVPN

2.1 Introduction

DMVPN stands for Dynamic multipoint VPN. DMVPN is a cisco IOS software solution for building IPSEC+GRE VPNs in an easy, dynamic and scalable manner. DMVPN works using two technologies.
1: NHRP (Next hop resolution protocol.): NHRP creates a distributed mapping database of all spokes with its real IP addresses.
2. Multipoint GRE tunnel Interface.

DMVPN also uses Technologies like, Routing Protocol, Dynamic IPSEC encryption and Cisco Express Forwarding. DMVPN has three phases Phase 1, Phase 2 and Phase 3. Phase 1 is Hub and Spoke, Phase 2 is Hub and Spoke with Spoke to Spoke. DMVPN provides full meshed connectivity with simple configuration of hub and spoke.

2.2 NHRP

NHRP works by mapping tunnel IP to there real IP. The packets used in NHRP are:

1. NHRP registration
2. NHRP resolutions and redirects.

NHRP registration: Spokes dynamically register with NHS (next hop server), which carries the database of mapping of NBMA addresses to real IP addresses.

NHP resolution and redirects: these messages help building dynamic spoke to spoke tunnel and also direct unicast data traffic thus reducing load on hub routers.

2.3 Multipoint GRE (mGRE)

Multipoint Gre is advanced version of Point to point GRE i.e. in mGRE there can be multiple sites connecting to a Hub. mGRE allows a tunnel to have multiple destinations. NHRP helps the end of the tunnel to map the tunnel IP addresses to actual IP addresses. NHRP is protocol that is needed by routers to help resolve the logical addresses to NBMA addresses. NHRP uses the idea that when NHRP is enabled on router every router in the topology act as a next hop client or a next hop server. Next Hop Server (NHS) is a database agent with whom all next hops clients register. When a router needs to send data to another router after checking the routing table it sends data to the tunnel ip of the destination. This request will be forwarded to NHS as it will have the entire mapping and thus data will reach the destination.

2.4 Working

DMVPN relies on two technologies which are NHRP (next hop resolution protocol) which is used for mapping database of spoke tunnels to real addresses and second is Multipoint GRE tunnel interface which is a single GRE interface to support multiple GRE tunnels. DMVPN uses concept of dynamic addressing where spokes that have dynamic IP addresses.

Destination router learns all route present at other end of the tunnel with next hop IP of tunnel. The router before forwarding any traffic to host on other end of router will check CEF entries, which are invalid in the beginning. Once a router tries to ping another spoke router it fails because it does not have the NBMA address of end router. Then router sends the packet to NHS. The resolution request that NHS receives has NBMA address and Logical IP of sending router but only Logical ip of destination router. When NHS receives resolution request it has mapping for NBMA and logical IP of Destination router since every router registers with NHS on tunnel formation. Thus NHS

sends the resolution reply to sending router. When the sender receives the resolution reply it completes its CEF entry for the destination network. Thus now it can send directly to that spoke router instead of trying to resolve first. Fig. 6 shows the header format for GRE packet that is used for formation of GRE tunnel.

Bits 0–3				4–12	13–15	16–31
C		K	S	Reserved0	Version	Protocol Type
Checksum *(optional)*						Reserved1 *(optional)*
Key *(optional)*						
Sequence Number *(optional)*						

Figure 6. Standard GRE packet header [2]

2.5 DMVPN design

DMVPN offers two network designs for building DMVPN tunnels:

1. Hub and Spoke
2. Spoke to Spoke

Hub and Spoke:
This design enables all spoke routers to connect to HUB. Fig. 7 shows the hub and spoke design where hub is the router at the bottom connecting to three spoke routers. Since spoke-to-spoke direct VPN tunnel is not supported in this design thus spoke-to-spoke traffic passes through HUB. This requires same number of tunnels as spokes since very spoke will connect to HUB using tunnel.

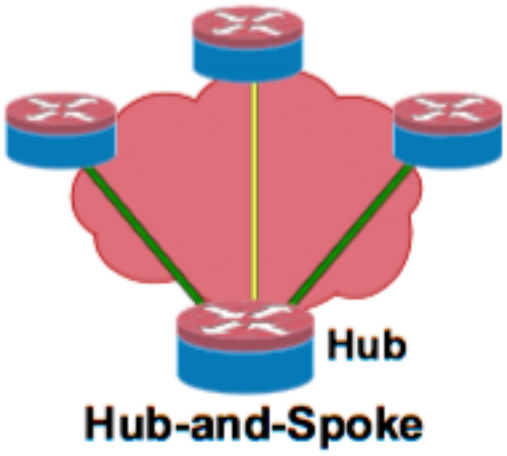

Figure 7. Hub and Spoke Design [4] (page 26)

To increase the CPU power a server load balancing approach can be used in hub and spoke topology where many identical hubs will be connected to a load balancer. Fig. 8 shows the design with a load balancer that also provides redundancy. In this design if one DMVPN hub fails the connectivity will not be lost since the topology has multiple hubs. This topology on other hand increases the cost for the company, as the DMVPN hubs are usually router at HQ. These routers are usually high-end router like 7200 series so that they can support large traffic from various sites.

The choice between these two topologies is based the deciding factor cost vs. redundancy. But there are many benefits and features associated with server load balancing.

1. Topologies can be scaled to very large DMVPN hub and spoke network that support thousands of spokes.
2. Load balancer server provides automatic load management over all available hubs.
3. IT increases the throughput, tunnel creation rate thus increments performance.
4. Configuration and maintenance is easy
5. Low-end routers can also participate in large IPSec VPN.

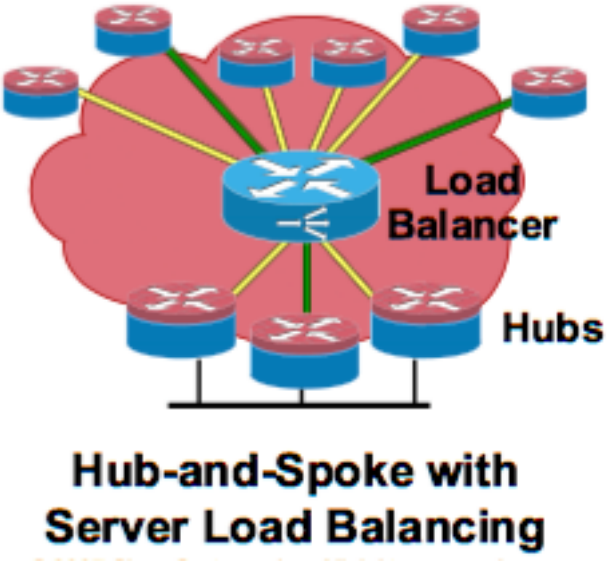

Figure 8. Hub and Spoke design with load balancing [4] (page 26)

There can be different server load balancing deployment models.

1. Distributes encryption with server load balancing.
   In this deployment model the encryption techniques such as IPSec is deployed on HUB routers. Fig. 9 shows distributed encryption with server load balancing

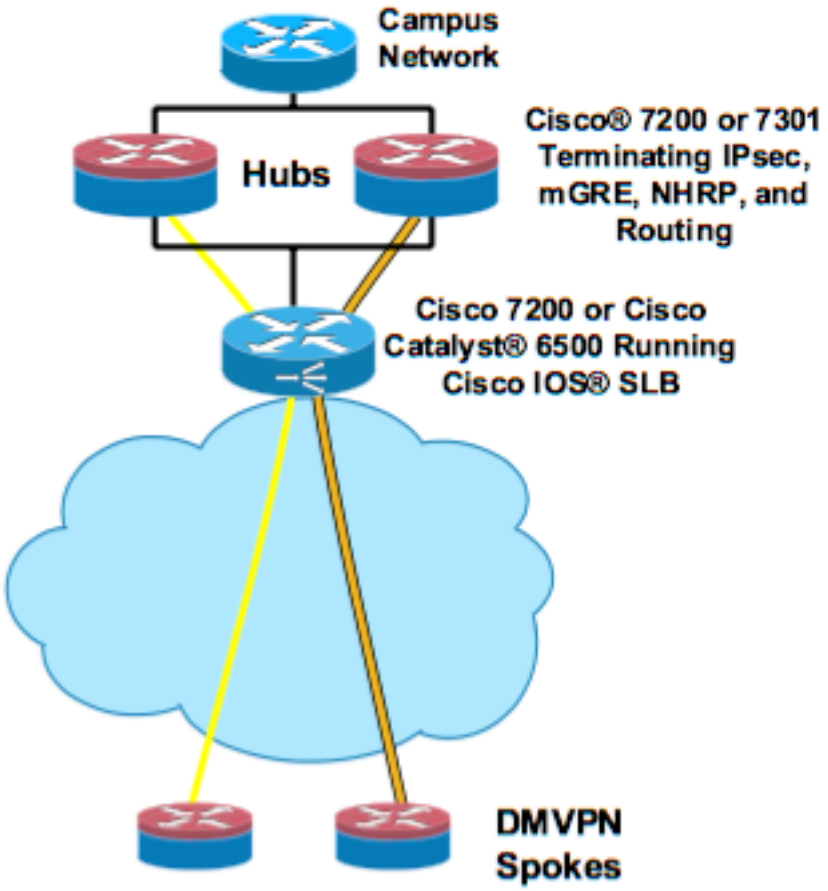

Figure 9. Distributed encryption with server load balancing [4] (page 31)

2. Integrated encryption with server load balancing.
   In this technique the encryption technique is deployed on load balancer server and the terminating mGRE, NHRP and Routing is done on Hub router. Fig. 10 shows integrated encryption with server load balancing.

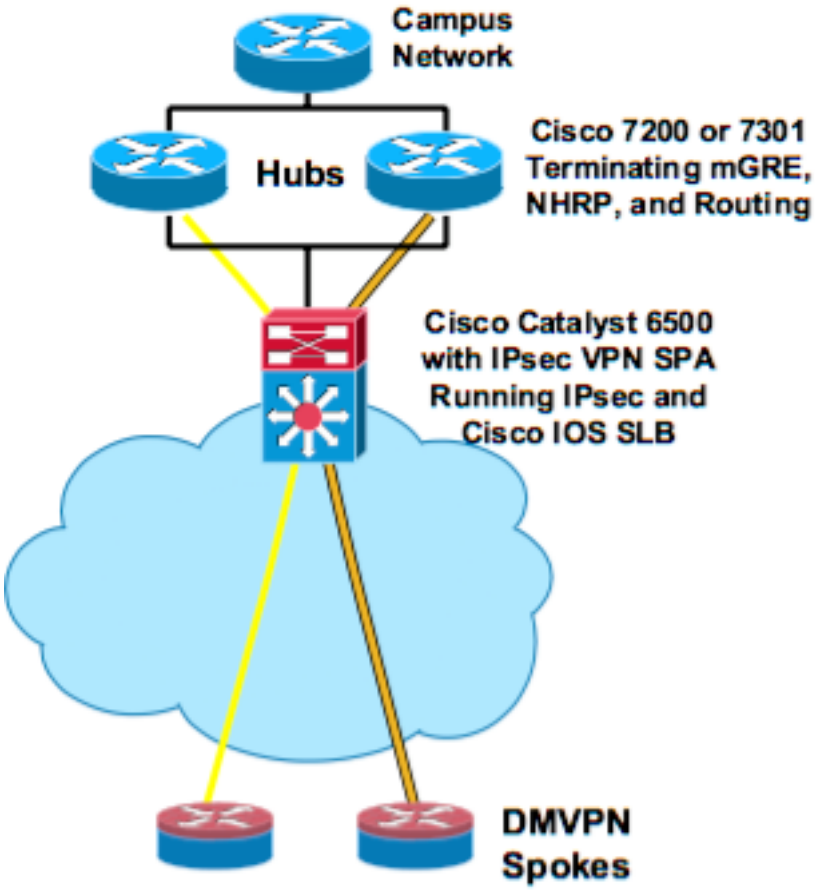

Figure 10. Integrated encryption with server load balancing [4] (page 31)

Spoke to Spoke:

In Spoke to spoke topology the communication between spokes is direct. Fig. 11 shows the spoke to spoke design topology where the green link represents a spoke to spoke link. The first time traffic goes through Hub and once the tunnel between spokes is established it starts flowing directly.

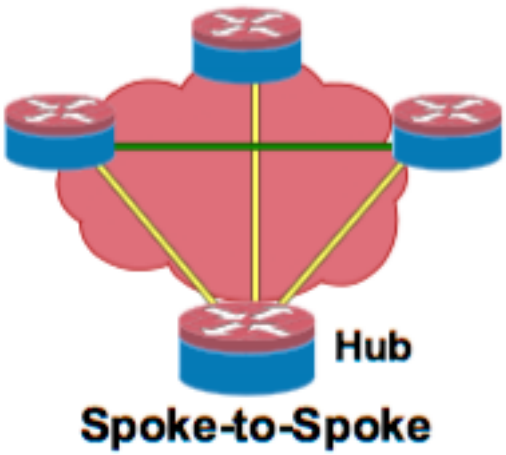

Figure 11. Spoke to Spoke design [4] (page 26)

This topology provides reduced load on hub. Also latency is reduced since when traffic was flowing through HUB is IPSEC encryption is enabled then IPSec encryption and decryption was done multiple times but I this case the encryption and decryption is done just once.

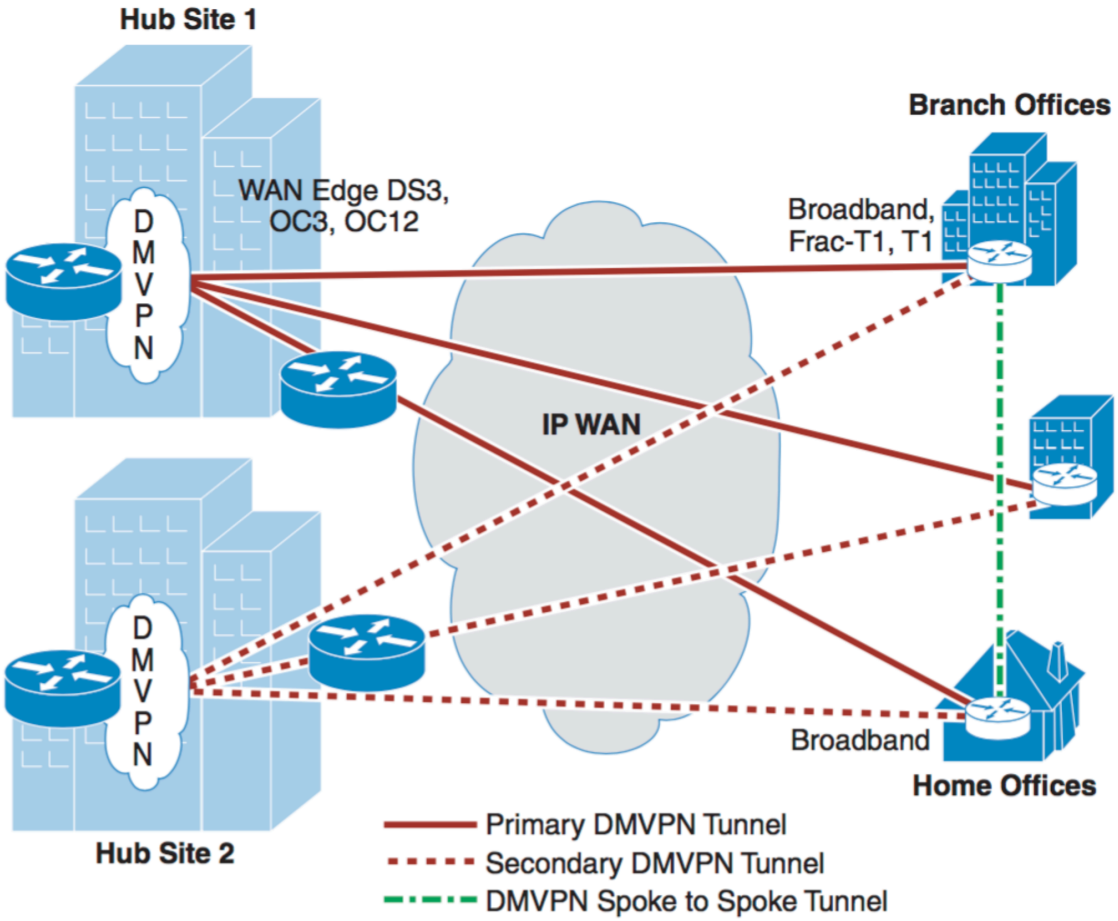

Figure 12. DMVPN Spoke to Spoke Topology Design [5] (page 38)

Fig. 12 shows the dual HUB DMVPN spoke to spoke topology where this provides redundancy for HUB. In this design topology individual branch office routers can dynamically establish tunnels with other branch office. But there should always be there a connection to headend before we can establish tunnel between sites. IN this case the headend router needs to have static IP but the branch routers can have either static or dynamic IP. Redundancy can be achieved by connecting every site to two headend so that in case one headend fails the site can establish connection to second headend. Fig.13 shows a single hub but multiple remote sites with spoke to spoke capability.

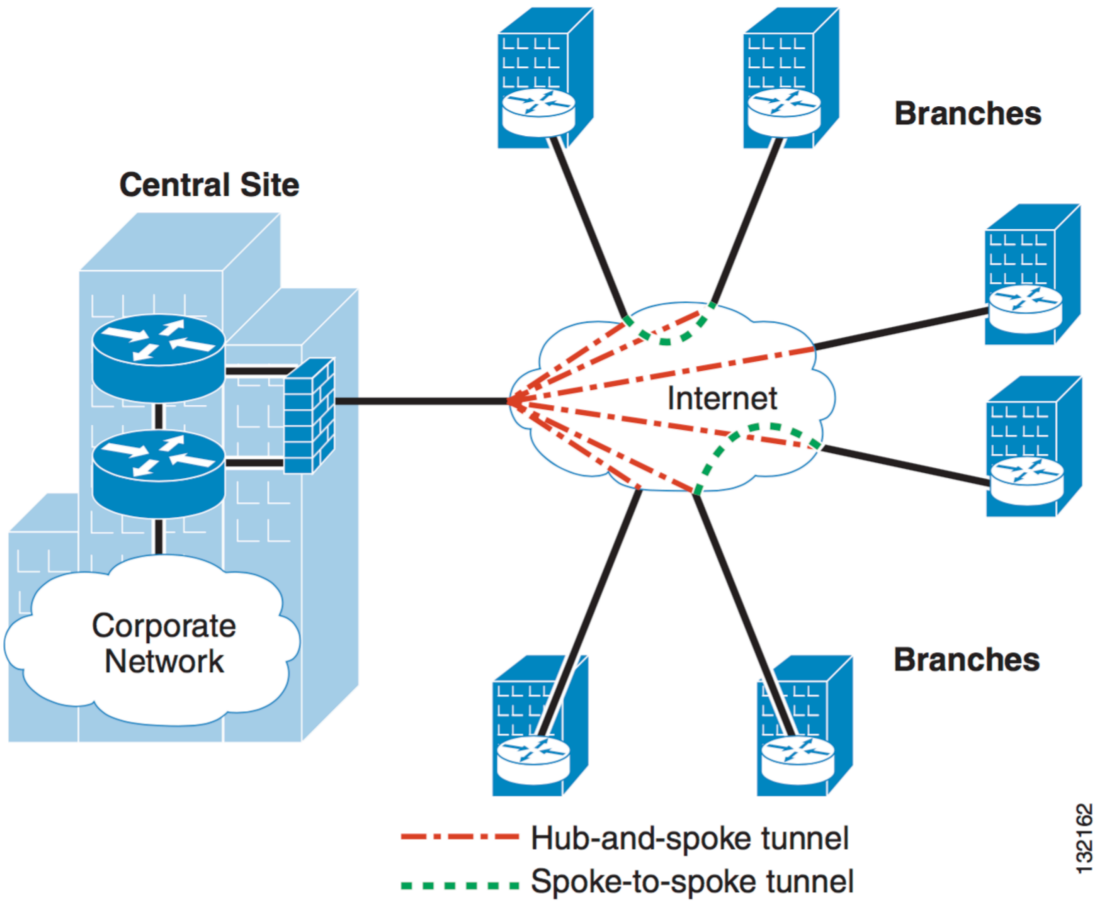

Figure 13. DMVPN spoke to spoke VPN topology [5] (page 8)

2.6 DMVPN Header

C is the checksum bit and if the checksum is present it is set to 1.
K is the Key bit and if a key is present it is set to 1.
S is sequence number bit and if a sequence number is present it is set to 1.
Reserved0 is reserved bits and it is set to 0.
Version is the GRE Version number and it is set to 0.
Protocol Type field indicates the ether protocol type of the encapsulated payload.
Checksum is present only if the C bit is set which as mentioned early is the checksum bit and contains the checksum for the GRE header and payload.
Reserved1 is present if the C bit is set and it is set to 0.
Key field contains application-specific key value and is present if the K bit is set.
Sequence Number is a sequence number for the GRE and is present if the S bit is set.

2.7 Network Diagram

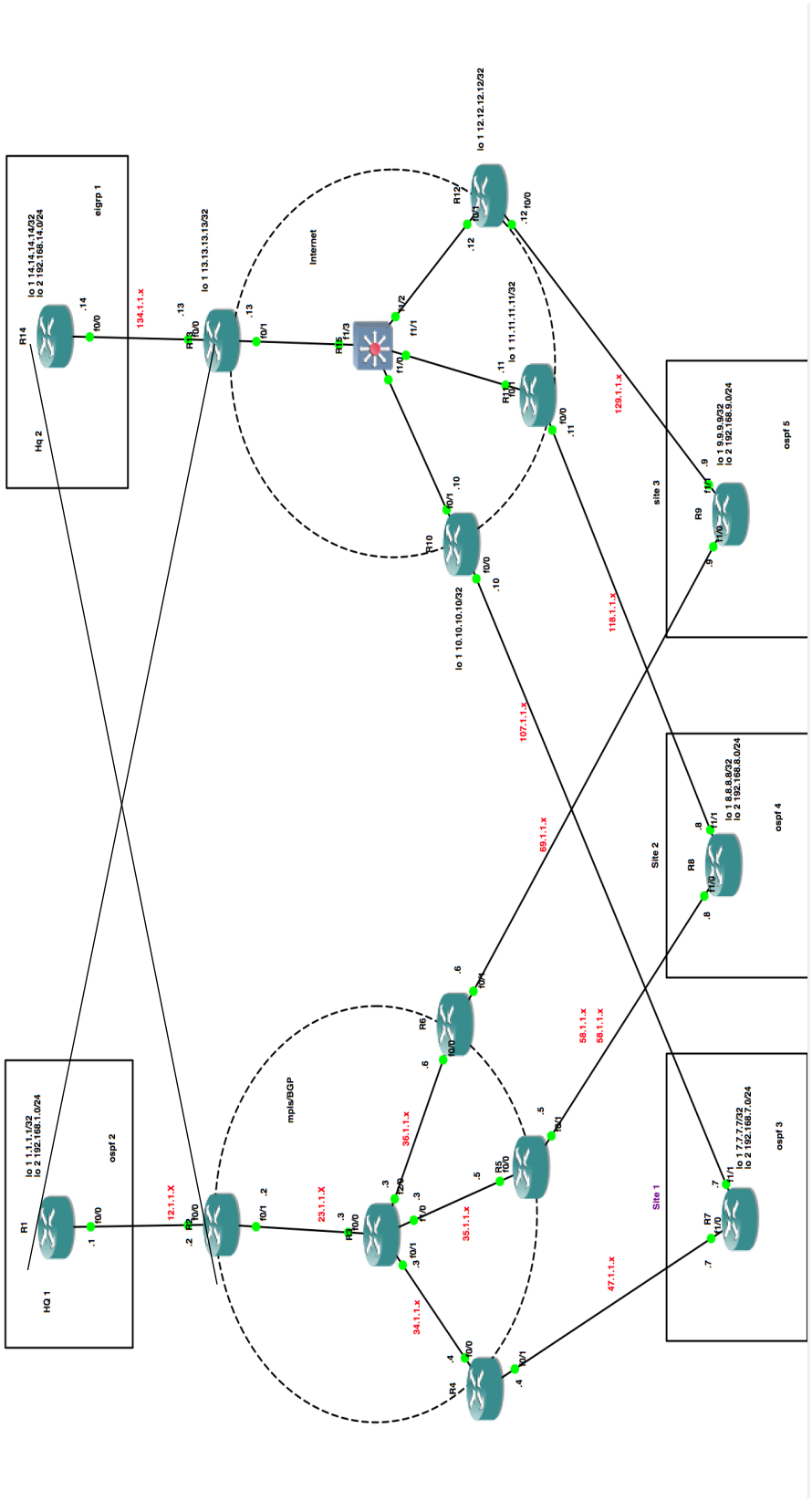

Figure 14. Network Diagram

Fig. 14 shows the network diagram used in GNS3 to emulate the network required to implement different VPN technologies in network. In our case DMVPN and IPSec is implemented.

2.8 Protocol Diagram

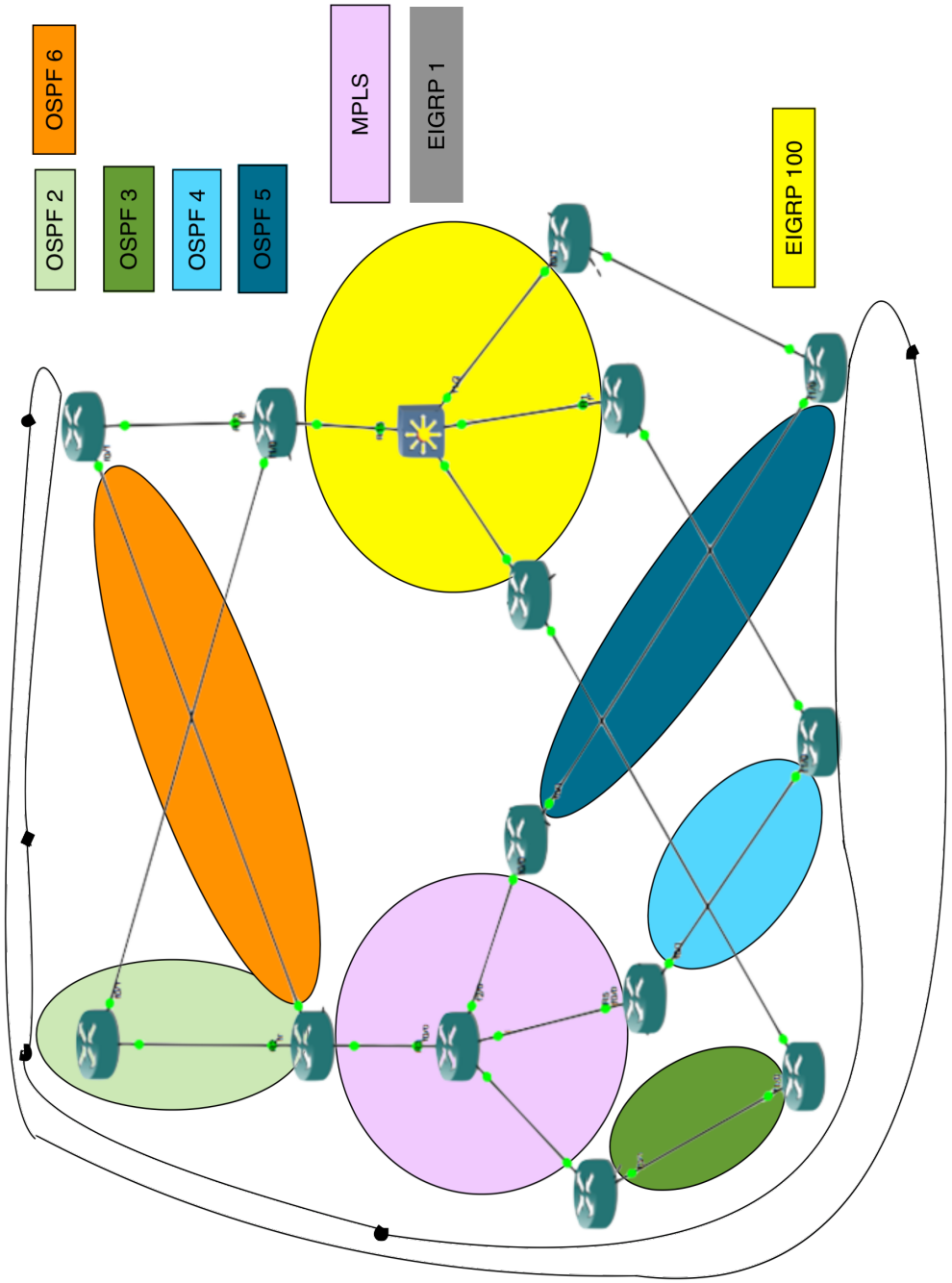

Figure 15. Protocol Diagram

Fig. 15 shows the protocol diagram. This protocl diagram simplifies the understanding of what routing protocols are used in the network to implement DMPN and IPSec.

2.9 Configuration

Router 1

```
Interface Loopback1
 Ip address 1.1.1.1 255.255.255.255
!
Interface Loopback2
 Ip address 192.168.1.1 255.255.255.0
!
Interface FastEthernet0/0
 Ip address 12.1.1.1 255.255.255.0
 Duplex auto
 Speed auto
!
Interface FastEthernet0/1
 Ip address 131.1.1.1 255.255.255.0
 Speed 100
 Full-duplex
!
Router ospf 2
 Log-adjacency-changes
 network 1.1.1.1 0.0.0.0 area 0
 Network 12.1.1.1 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 131.1.1.13
```

Router 2

```
mpls label protocol ldp
!
interface Loopback1
 ip address 2.2.2.2 255.255.255.255
!
interface FastEthernet0/0
 ip address 12.1.1.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 23.1.1.2 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet1/0
 ip address 141.1.1.2 255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 23.1.1.2 0.0.0.0 area 0
!
router ospf 2
 log-adjacency-changes
 redistribute bgp 1 metric 100 metric-type 1
subnets
 network 12.1.1.2 0.0.0.0 area 0
!
router ospf 6
 log-adjacency-changes
 redistribute bgp 1 metric 100 metric-type 1
subnets
 network 141.1.1.2 0.0.0.0 area 0
!
router bgp 1
 bgp log-neighbor-changes
 neighbor 4.4.4.4 remote-as 1
 neighbor 4.4.4.4 update-source Loopback1
 neighbor 5.5.5.5 remote-as 1
 neighbor 5.5.5.5 update-source Loopback1
 neighbor 6.6.6.6 remote-as 1
 neighbor 6.6.6.6 update-source Loopback1
 !
 address-family ipv4
  redistribute ospf 2 metric 10
  redistribute ospf 6 metric 10
  neighbor 4.4.4.4 activate
  neighbor 4.4.4.4 next-hop-self
  neighbor 5.5.5.5 activate
  neighbor 6.6.6.6 activate
  no auto-summary
  no synchronization
  bgp redistribute-internal
 exit-address-family
```

Router 3

```
mpls label protocol ldp

interface Loopback1
 ip address 3.3.3.3 255.255.255.255
!
interface FastEthernet0/0
 ip address 23.1.1.3 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet0/1
 ip address 34.1.1.3 255.255.255.0
 duplex auto
 speed auto
 mpls ip
```

```
!
interface FastEthernet1/0
 ip address 35.1.1.3 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet2/0
 ip address 36.1.1.3 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 3.3.3.3 0.0.0.0 area 0
 network 23.1.1.3 0.0.0.0 area 0
 network 34.1.1.3 0.0.0.0 area 0
 network 35.1.1.3 0.0.0.0 area 0
 network 36.1.1.3 0.0.0.0 area 0
```

Router 4

```
mpls label protocol ldp
!
interface Loopback1
 ip address 4.4.4.4 255.255.255.255
!
interface FastEthernet0/0
 ip address 34.1.1.4 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet0/1
 ip address 47.1.1.4 255.255.255.0
 ip ospf dead-interval 100
 speed 100
 full-duplex
!
router ospf 1
 log-adjacency-changes
 network 4.4.4.4 0.0.0.0 area 0
 network 34.1.1.4 0.0.0.0 area 0

router ospf 3
 log-adjacency-changes
 redistribute bgp 1 subnets
 network 47.1.1.4 0.0.0.0 area 0
!
router bgp 1
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 1
 neighbor 2.2.2.2 update-source Loopback1
 !
 address-family ipv4
  redistribute ospf 3 metric 10
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 next-hop-self
  no auto-summary
  no synchronization
  bgp redistribute-internal
  network 4.4.4.4 mask 255.255.255.255
 exit-address-family
```

Router 5

```
mpls label protocol ldp


interface Loopback1
 ip address 5.5.5.5 255.255.255.255
!
interface FastEthernet0/0
 ip address 35.1.1.5 255.255.255.0
 speed 100
 full-duplex
 mpls ip
!
interface FastEthernet0/1
 ip address 58.1.1.5 255.255.255.0
 ip ospf dead-interval 80
 speed 100
 full-duplex
!
router ospf 1
 log-adjacency-changes
 network 5.5.5.5 0.0.0.0 area 0
 network 35.1.1.5 0.0.0.0 area 0
!
router ospf 4
 log-adjacency-changes
 redistribute bgp 1 subnets
 network 58.1.1.5 0.0.0.0 area 0

router bgp 1
 no synchronization
 bgp log-neighbor-changes
 bgp redistribute-internal
 redistribute ospf 4 metric 10
 neighbor 2.2.2.2 remote-as 1
 neighbor 2.2.2.2 update-source Loopback1
 no auto-summary
```

Router 6

```
mpls label protocol ldp
interface Loopback1
 ip address 6.6.6.6 255.255.255.255
!
interface FastEthernet0/0
```

```
 ip address 36.1.1.6 255.255.255.0
 speed 100
 full-duplex
 mpls ip
!
interface FastEthernet0/1
 ip address 69.1.1.6 255.255.255.0
 ip ospf dead-interval 80
 speed 100
 full-duplex
!
router ospf 1
 log-adjacency-changes
 network 6.6.6.6 0.0.0.0 area 0
 network 36.1.1.6 0.0.0.0 area 0
!
router ospf 5
 log-adjacency-changes
 redistribute bgp 1 subnets
 network 69.1.1.6 0.0.0.0 area 0
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 bgp redistribute-internal
 redistribute ospf 5 metric 10
 neighbor 2.2.2.2 remote-as 1
 neighbor 2.2.2.2 update-source Loopback1
 no auto-summary
```

Router 7

```
no ip domain lookup
no ipv6 cef

track 1 ip sla 1

interface Loopback1
 ip address 7.7.7.7 255.255.255.255
!
interface Loopback2
 ip address 192.168.7.1 255.255.255.0
!
interface Tunnel1
 ip address 147.1.1.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip hold-time eigrp 100 35
 ip hold-time eigrp 1 300
 ip nhrp map multicast dynamic
 ip nhrp map 147.1.1.2 134.1.1.14
 ip nhrp map multicast 134.1.1.14
 ip nhrp network-id 1
 ip nhrp nhs 147.1.1.2 priority 1
 ip nhrp shortcut
 tunnel source FastEthernet1/1
 tunnel mode gre multipoint
!
interface FastEthernet1/0
 ip address 47.1.1.7 255.255.255.0
 ip ospf dead-interval 100
 speed auto
 duplex auto
!
interface FastEthernet1/1
 ip address 107.1.1.7 255.255.255.0
 speed auto
 duplex auto
!
!
router eigrp 1
 network 7.7.7.7 0.0.0.0
 network 147.1.0.0
!
router ospf 3
 network 7.7.7.7 0.0.0.0 area 0
 network 47.1.1.7 0.0.0.0 area 0
 network 192.168.7.1 0.0.0.0 area 0
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 107.1.1.10
!
ip sla 1
 icmp-echo 141.1.1.14 source-interface
Loopback1
 frequency 6
ip sla schedule 1 life forever start-time now

event manager applet hq2
 event track 1 state down
 action 1.0 cli command "enable"
 action 1.5 cli command "config t"
 action 2.0 cli command "ip route 0.0.0.0
0.0.0.0 107.1.1.10"
event manager applet hq2up
 event track 1 state up
 action 3.0 cli command "enable"
 action 3.5 cli command "config t"
 action 4.0 cli command "no ip route 0.0.0.0
0.0.0.0 107.1.1.10"
```

Router 8

```
track 1 ip sla 1

interface Loopback1
 ip address 8.8.8.8 255.255.255.255
!
interface Loopback2
 ip address 192.168.8.1 255.255.255.255
!
interface Tunnel1
```

```
 ip address 147.1.1.8 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip hold-time eigrp 1 300
 ip nhrp map multicast dynamic
 ip nhrp map 147.1.1.2 134.1.1.14
 ip nhrp map multicast 134.1.1.14
 ip nhrp network-id 1
 ip nhrp nhs 147.1.1.2 priority 1
 ip nhrp shortcut
 tunnel source FastEthernet1/1
 tunnel mode gre multipoint
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet1/0
 ip address 58.1.1.8 255.255.255.0
 ip ospf dead-interval 100
 speed auto
 duplex auto
!
interface FastEthernet1/1
 ip address 118.1.1.8 255.255.255.0
 speed auto
 duplex auto
!
!
router eigrp 1
 network 8.8.8.8 0.0.0.0
 network 147.1.1.0 0.0.0.255
 network 192.168.8.0
!
router ospf 4
 network 8.8.8.8 0.0.0.0 area 0
 network 58.1.1.8 0.0.0.0 area 0

ip route 0.0.0.0 0.0.0.0 118.1.1.11
!
ip sla 1
 icmp-echo 141.1.1.14 source-interface
Loopback1
ip sla schedule 1 life forever start-time now

event manager applet hq2
 event track 1 state down
 action 1.0 cli command "enable"
 action 1.5 cli command "config t"
 action 2.0 cli command "ip route 0.0.0.0
0.0.0.0 118.1.1.11"
event manager applet hq2up
 event track 1 state up
 action 3.0 cli command "enable"
 action 3.5 cli command "config t"
 action 4.0 cli command "no ip route 0.0.0.0
0.0.0.0 118.1.1.11"
!
end
```

Router 9

```
track 1 ip sla 1
!
interface Loopback1
 ip address 9.9.9.9 255.255.255.255
!
interface Loopback2
 ip address 192.168.9.1 255.255.255.0
!
interface Tunnel1
 ip address 147.1.1.9 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip hold-time eigrp 1 300
 ip nhrp map multicast dynamic
 ip nhrp map 147.1.1.2 134.1.1.14
 ip nhrp map multicast 134.1.1.14
 ip nhrp network-id 1
 ip nhrp nhs 147.1.1.2 priority 1
 ip nhrp shortcut
 tunnel source FastEthernet1/1
 tunnel mode gre multipoint
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet1/0
 ip address 69.1.1.9 255.255.255.0
 ip ospf dead-interval 80
 speed auto
 duplex auto
!
interface FastEthernet1/1
 ip address 129.1.1.9 255.255.255.0
 speed auto
 duplex auto
!
!
router eigrp 1
 network 9.9.9.9 0.0.0.0
 network 147.1.1.0 0.0.0.255
 network 192.168.9.0
!
router ospf 5
 network 9.9.9.9 0.0.0.0 area 0
 network 69.1.1.9 0.0.0.0 area 0
 network 192.168.9.1 0.0.0.0 area 0
!
```

```
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 129.1.1.12
!
ip sla 1
 icmp-echo 141.1.1.14 source-interface Loopback1
 frequency 6
ip sla schedule 1 life forever start-time now

!
event manager applet hq2
 event track 1 state down
 action 1.0 cli command "enable"
 action 1.5 cli command "config t"
 action 2.0 cli command "ip route 0.0.0.0 0.0.0.0 129.1.1.12"
```

Router 10

```
interface Loopback1
 ip address 10.10.10.10 255.255.255.255
!
interface FastEthernet0/0
 ip address 107.1.1.10 255.255.255.0
 speed 100
 full-duplex
!
interface FastEthernet0/1
 ip address 110.1.1.2 255.255.255.0
 speed 100
 full-duplex
!
router eigrp 100
 redistribute connected
 network 10.10.10.0 0.0.0.255
 network 110.1.1.0 0.0.0.255
 no auto-summary
```

Router 11

```
interface Loopback1
 ip address 11.11.11.11 255.255.255.255
!
interface FastEthernet0/0
 ip address 118.1.1.11 255.255.255.0
 speed 100
 full-duplex
!
interface FastEthernet0/1
 ip address 111.1.1.2 255.255.255.0
 speed 100
 full-duplex
!
router eigrp 100
 redistribute connected
 network 11.11.11.11 0.0.0.0
 network 111.1.1.0 0.0.0.255
 no auto-summary
```

Router 12

```
interface Loopback1
 ip address 12.12.12.12 255.255.255.255
!
interface FastEthernet0/0
 ip address 129.1.1.12 255.255.255.0
 speed 100
 full-duplex
!
interface FastEthernet0/1
 ip address 112.1.1.2 255.255.255.0
 speed 100
 full-duplex
!
router eigrp 100
 redistribute connected
 network 12.12.12.12 0.0.0.0
 network 112.1.1.0 0.0.0.255
 no auto-summary
```

Router 13

```
interface Loopback1
 ip address 13.13.13.13 255.255.255.255
!
interface FastEthernet0/0
 ip address 134.1.1.13 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 113.1.1.2 255.255.255.0
 speed 100
 full-duplex
!
interface FastEthernet1/0
 ip address 131.1.1.13 255.255.255.0
 duplex auto
 speed auto
!
router eigrp 100
 redistribute connected
 network 13.13.13.13 0.0.0.0
 network 113.1.1.0 0.0.0.255
 no auto-summary
!
ip forward-protocol nd
```

```
ip route 14.14.14.14 255.255.255.255 134.1.1.14
ip route 192.168.14.0 255.255.255.0 134.1.1.14
 network 192.168.14.0 0.0.0.255 area 0
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 134.1.1.13
```

Router 14

```
interface Loopback1
 ip address 14.14.14.14 255.255.255.255
!
interface Loopback2
 ip address 192.168.14.1 255.255.255.0
!
interface Tunnel1
 ip address 147.1.1.2 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip hold-time eigrp 1 300
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp shortcut
 ip nhrp redirect
 no ip split-horizon eigrp 1
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
!
interface FastEthernet0/0
 ip address 134.1.1.14 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 141.1.1.14 255.255.255.0
 shutdown
 speed 100
 full-duplex
!
router eigrp 1
 network 14.14.14.14 0.0.0.0
 network 147.1.0.0
 network 192.168.14.0
 no auto-summary
!
router ospf 6
 log-adjacency-changes
 network 14.14.14.14 0.0.0.0 area 0
 network 141.1.1.14 0.0.0.0 area 0
```

Router 15

```
interface FastEthernet1/0
 switchport access vlan 10
 duplex full
 speed 100
!
interface FastEthernet1/1
 switchport access vlan 11
 duplex full
 speed 100
!
interface FastEthernet1/2
 switchport access vlan 12
 duplex full
 speed 100
!
interface FastEthernet1/3
 switchport access vlan 13
 duplex full
 speed 100
!
interface Vlan10
 ip address 110.1.1.1 255.255.255.0
!
interface Vlan11
 ip address 111.1.1.1 255.255.255.0
!
interface Vlan12
 ip address 112.1.1.1 255.255.255.0
!
interface Vlan13
 ip address 113.1.1.1 255.255.255.0
!
router eigrp 100
 network 110.1.1.0 0.0.0.255
 network 111.1.1.0 0.0.0.255
 network 112.1.1.0 0.0.0.255
 network 113.1.1.0 0.0.0.255
 no auto-summary
```

2.10 Template for Configuration of routers

Site Routers

The configuration on site routers consists of:

1. Tunnel configuration
2. Routing protocol configuration

Routing Protocol is needed to run over the tunnels to provide reachability between all networks at the end of tunnel. Two physical interfaces are needed to provide connectivity to site using MPLS and Internet respectively. Different protocols can be used to provide connectivity to between all networks running over site, which in our case is OSPF over MPLS and EIGRP over DMVPN. Site routers have a default route configured on link that is connected to the Internet. The default route is not in the routing table until the users on Site can reach HQ networks using MPLS link but when MPLS link goes down a default route towards the internet is automatically installed thus providing redundant connection to HQ for Site users.

Tunnel Configuration:

The tunnel has a logical IP, which is given using command ip address x.x.x.x x.x.x.x, and it is mapped to a physical IP of the router using command ip nhrp map x.x.x.x y.y.y.y

SLA Monitor Configuration

The SLA monitor can be used to constantly check reachability to any point in the network and configuration can be done using commands ip sla x where x is the sea number and then sea can be configured to do a task based on one's need. In our case we use sla to ping an IP at the other HQ by using command icmp-echo x.x.x.x source-interface <interface> and we can also define frequency of this operation with command frequency x. Now since SLA is configured we need to start it using ip sla schedule x life forever start-time now. This command says that SLA x is scheduled for forever and start time is now. We can set the start time to some other Day at some specific time.

Event Manager Configuration

Event manager configuration enables the router to run a set of command when an event occurs that it has been configured to track . Configuration is done using event manager applet <name > and then the event manager is configured to track a IP SLA using command event track x state down, In our case its tracking state of IP SLA 1 . Then using command like action x cli command <command to run > the event manager is told to run a set of commands.

```
interface Tunnel1
 ip address x.x.x.x x.x.x.x
 no ip redirects
 ip mtu 1400
 ip nhrp map multicast dynamic
 ip nhrp map x.x.x.x y.y.y.y
 ip nhrp map multicast y.y.y.y
 ip nhrp network-id 1
 ip nhrp nhs x.x.x.x priority 1
 ip nhrp shortcut
 tunnel source FastEthernet1/1
 tunnel mode gre multipoint

interface FastEthernet1/0
 ip address x.x.x.x x.x.x.x
speed auto
 duplex auto

interface FastEthernet1/1
 ip address y.y.y.y y.y.y.y
 speed auto
 duplex auto

router eigrp x
```

```
 network x.x.x.x
!
router ospf x
 network x.x.x.x 0.0.0.0 area 0

ip route 0.0.0.0 0.0.0.0 x.x.x.x

ip sla x
 icmp-echo x.x.x.x source-interface <interface>
 frequency x
ip sla schedule x life forever start-time now

event manager applet <name>
 event track x state down
 action 1.0 cli command "enable"
 action 1.5 cli command "config t"
 action 2.0 cli command "ip route 0.0.0.0 0.0.0.0 x.x.x.x”
event manager applet <name>
 event track 1 state up
 action 3.0 cli command "enable"
 action 3.5 cli command "config t"
 action 4.0 cli command "no ip route 0.0.0.0 0.0.0.0 x.x.x.x”
```

HQ Routers

The configuration on HQ routers consists of:

1. Tunnel configuration
2. Routing protocol configuration

HQ routers tunnel configuration consists of making the HQ router as a hub for tunnel. Routing Protocol is needed to run over the tunnels to provide reachability between all networks at the end of tunnel. Two physical interfaces are needed to provide connectivity to site using MPLS and Internet respectively. Different protocols can be used to provide connectivity to between all networks running over site which in our case is OSPF over MPLS and EIGRP over DMVPN.

The tunnel has a logical IP which is given using command *ip address x.x.x.x x.x.x.x* and it is mapped to a physical IP of the router using command *ip nhrp map x.x.x.x y.y.y.y* . The command ip nhrp network-id x states the network for tunnels and this network-id number should match on site routers also for the tunnel to be UP. In our case we also need an extra command *no ip split-horizon eigrp x* because we are running EIGRP over tunnels thus at the hub when a packet comes in at an interface it will not be sent out through the same interface because of EIGRP Split-Horizon. The command *tunnel mode gre multipoint* tells the router that the tunnel should be configured multipoint.

Tunnel Configuration

```
interface Tunnel1
 ip address x.x.x.x x.x.x.x
 no ip redirects
 ip mtu 1400
 ip nhrp map multicast dynamic
 ip nhrp network-id x
 ip nhrp shortcut
 ip nhrp redirect
 no ip split-horizon eigrp x
tunnel source <interface>
```

```
 tunnel mode gre multipoint

router eigrp x
 network x.x.x.x
 no auto-summary

router ospf x
 network x.x.x.x x.x.x.x area 0

ip route 0.0.0.0 0.0.0.0 x.x.x.x
```

2.11 Results

Latency:
The DMVPN tunnel implemented in GNS3 the ping results showed latency of 79 ms.

Convergence:
The current configuration and emulation in GNS3 showed a convergence time of 1.794 seconds

2.12 Advantages of DMVPN Tunnel

1. Provides connectivity that is full meshed with simple configuration of hub and spoke thus providing dynamic spoke to spoke tunnels.

2. The spokes in DMVPN can be dynamically addressed.

3. Additional configuration is not required for addition of new spokes thus facilitating zero-touch configuration for addition of new spokes.

4. DMVPN supports IP unicast, IP multicast and dynamic routing protocols.

5. DMVPN can be used with or without IPSEC.

6. DMVPN supports thousands of spoke since it can be scaled to very large DMVPN

7. DMVPN supports excellent application support such as voice, video, multicast and non-ip application support.

8. DMVPN supports split tunneling at the spokes

2.13 Disadvantages of DMVPN Tunnel

1. DMVPN tunnel does not provide security if it is not used together with IPSEC.

IPSEC

3.1 Introduction

IP Security stands for IPSEC. IPSec is a protocol that provides secure exchange of packets over the IP layer. IPSec is widely used to implement Virtual Private Networks (VPNs). IPSec has two modes of encryption Tunnel and Transport. When data is sent over a link a header is attached to the data packet and this is where these two modes come into effect and Tunnel mode is the most secure mode since it encrypts both the data that is payload as well as header whereas the transport mode only encrypts the payload.

3.2 IPSec Protocols

There are two protocols used in IPSec : ESP and AH.

3.2.1 Encapsulating Security Protocol

ESP protocol combined with other parameters such as security parameters or transform protects data by making it indecipherable. The IP protocol number for ESP is 50.

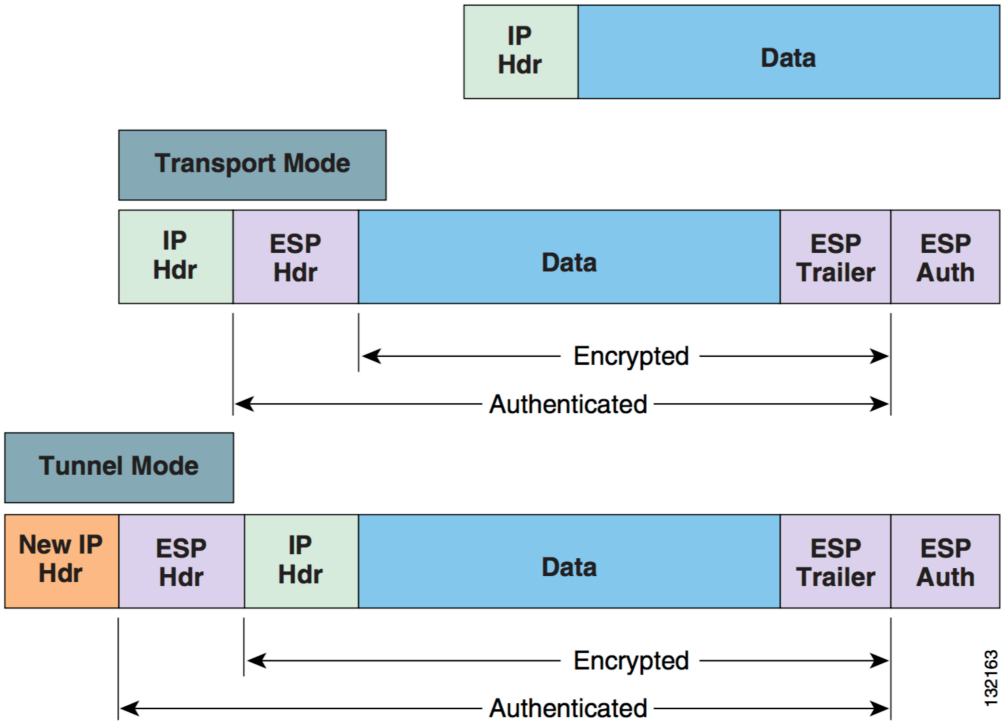

Figure 16. Encapsulating security payload [9]

Fig. 16 describes how ESP encapsulates a packet by attaching new header and trailer to the original IP packet thus increasing security for the data in packet

3.2.2 Authentication Header

Authentication header protocol has an IP protocol number of 51. Authentication header does not protect data as ESP but it adds a header, which acts as a seal to see in the receiving end if data is tampered with. Fig. 17 shows Authentication header format and as shown in the figure there is no trailer.

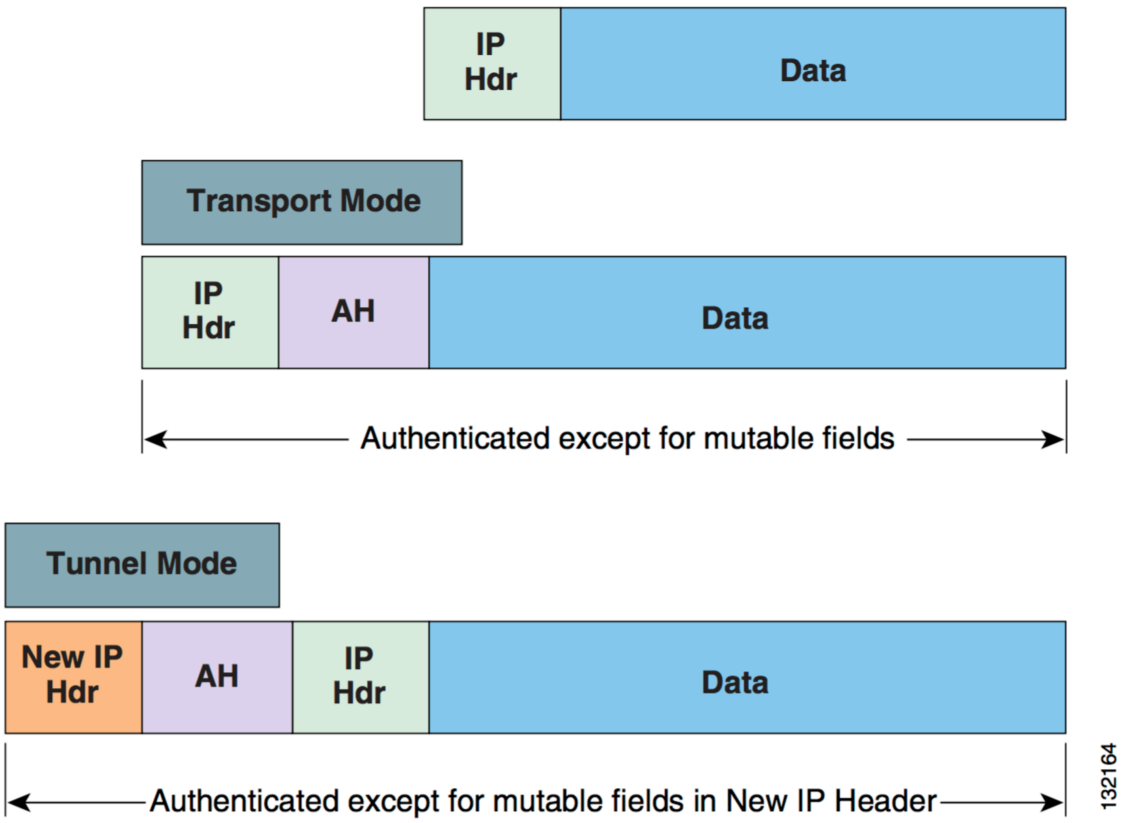

Figure 17. Authentication Header [9]

3.3 IPSec modes

IPSec has two modes that it can operate in which are tunnel mode and Transport mode.

Tunnel Mode:
In tunnel mode the entire packet is protected. The packet is usually pre encrypted so in tunnel mode a new header is attached to the packet to successfully forward the packet. Tunnel mode can be used with both ESP and AH. Tunnel mode results in packet being expanded than its original size as new header is attached. Tunnel mode is more secure than transport mode because it protects that is encapsulates both the source and destination IP address of the original packet. Fig. 18 shows the IPSec tunnel mode where a new IP header is added to the old IP packet.

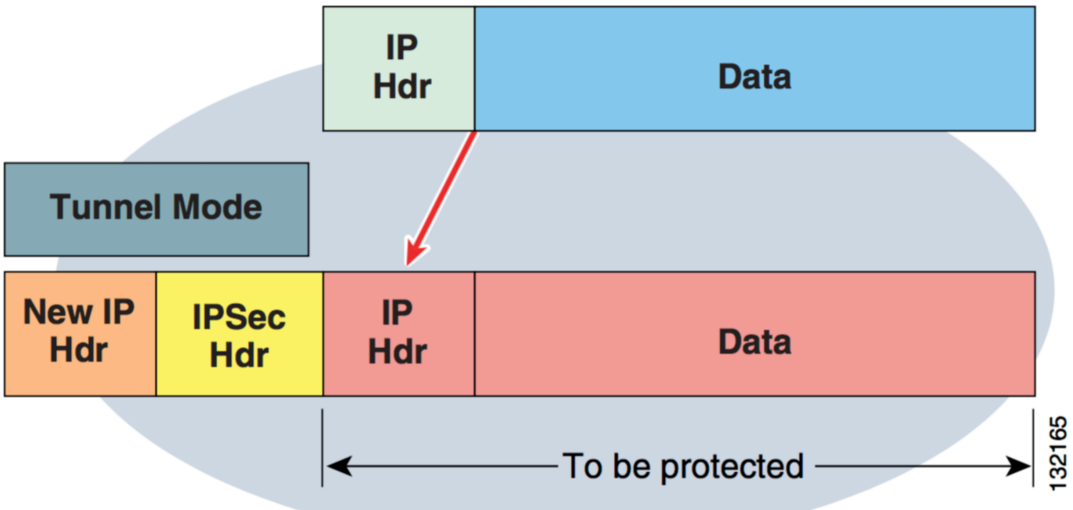

Figure 18. IPSec tunnel mode [9]

Transport Mode:

The transport mode is different from tunnel mode because instead of attaching a new header on top of IPSec header that is on top of our original packet that is to be protected, transport mode just inserts IPSec header between data and IP header. As a result after encryption the data is protected but the source and destination IP addresses are visible in IP header. But since there is one less header than Tunnel mode there is less packet expansion. Transport mode can also be deployed with both ESP and AH. Fig. 19 shows IPSec transport mode where the IP header remains except for security a IPSec header is added in between.

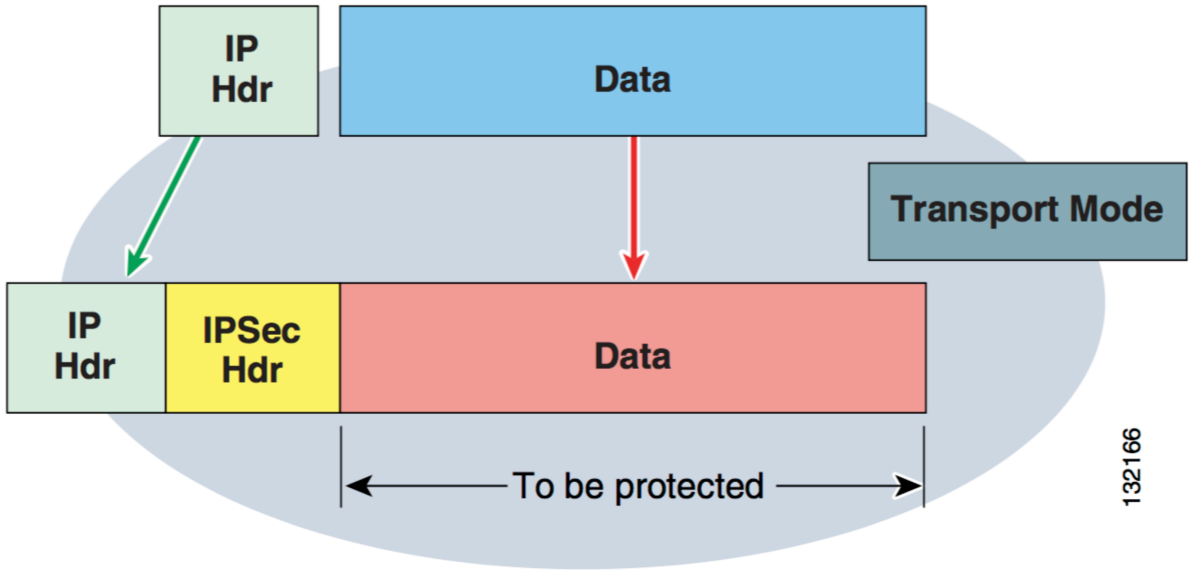

Figure 19. IPSec transport mode [9]

3.4 Working

IPSec operation basically can be divided into five main steps. The steps can be defined as follows:

1. Interesting traffic initiates the IPSec process
2. IKE phase one
3. IKE phase two
4. Data transfer
5. IPSec tunnel Termination

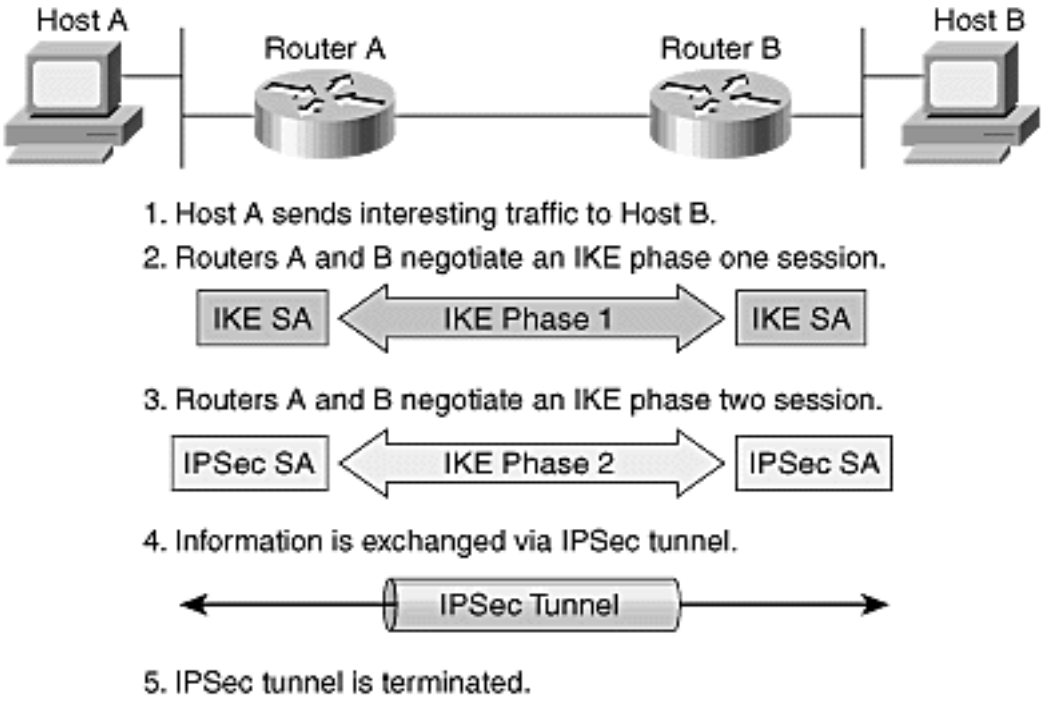

Figure 20. The five steps of IPSec (Figure 1-15) [10]

Fig. 20 shows five steps of IPSec where step 1 is sending Interesting traffic which initiates the IPSec process this traffic is deemed interesting using access lists when configuring IPSec security policy in IPSec peers. Next step is now after configuration is done to establish IKE security associations. IKE helps to authenticate IPSec peers and a secure channel is established for negotiating IPSec SAs in phase two. After Phase 1 is done both routers negotiate IKE phase two session. Now that SA are established phase 4 is data transfer over the tunnel between IPSec peers based on the IPSec parameters and keys stored in the SA database. The final step is tunnel termination that is IPSec SAs terminate through deletion or by timing out. Fig. 21 shows the definition of interesting traffic using Access lists.

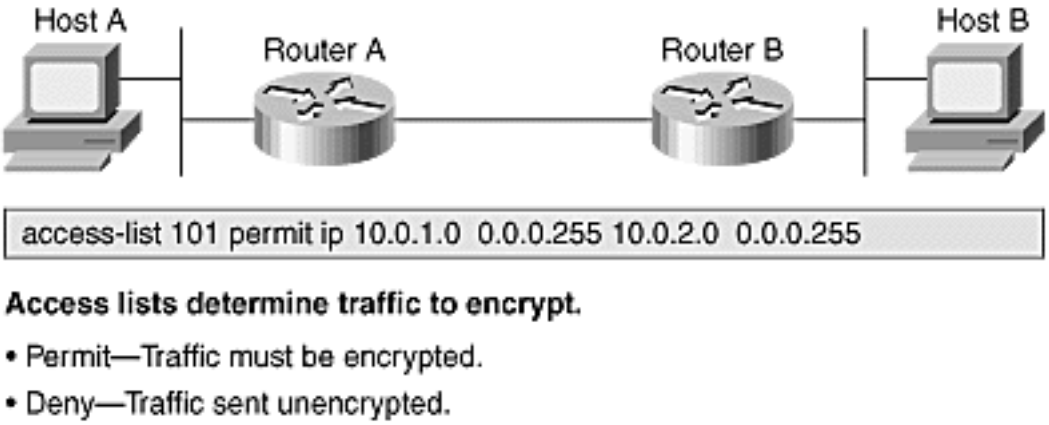

Figure 21. Defining Interesting Traffic (Figure 1-16) [10]

3.4.1 Defining Interesting Traffic

The following figure is an example of interesting traffic that is in the following figure it is the traffic from network 10.0.1.0/24 to 10.0.2.0/24. A part of formulating a security policy for use of a VPN is determining what type of traffic is defined interesting. After the traffic is deemed interesting the policy is implemented in the configuration interface for each particular IPSec peer. The way this interesting traffic actually works is that they are defined in Cisco routers using access lists that are used to determine the traffic to encrypt. These access lists are assigned to a crypto policy. The permit statement indicates that the selected traffic must be encrypted. Deny statements can also be used together with permit statements to indicate that the selected traffic must be sent unencrypted. IKE phase one exchange is negotiated when interesting traffic is generated or transits the IPSec client.

3.4.2 IKE Phase One

IKE phase one has the following functions:
1. The identities of the IPSec peers are protected and they are authenticated.
2. The IKE exchange is protected by Negotiating a matching IKE SA policy between peers
3. The Diffie-Hellman exchange is performed as a result both peers have matching shared secret keys
4. Establishes a secure tunnel to negotiate IKE phase two parameters

IKE phase one is completed in two modes:

1. Main mode
2. Aggressive mode

Main Mode

There are three two-way exchanges between the initiator and receiver in Main mode.
First exchange**:**
The first exchange involves algorithms and hashes that are used to secure the IKE communications in matching IKE SAs in each peer.

Second exchange:

The second exchange involves a Diffie-Hellman exchange to generate shared secret keys. These shared secret keys are numbers, which are sent to the other end of the tunnel and then signed by the peer and returned which proves their identity.

Third exchange:
The third exchange verifies the identity of the peer. The IPSec peer's IP address is the identity value but it is in encrypted form. The IKE exchanges further should be protected between IKE SA peers and that the main outcome form main mode. The SA defines the following things for the IKE exchange:

- Method used for authentication
- The encryption algorithms
- Lifetime of SA
- Shared secret key values.

Aggressive Mode

Aggressive mode involves less packet exchange as compared to main mode. Everything is exchanged within the first packet i.e into IKE SA values. Then the receiver sends back all information to complete the exchange. But the drawback of using aggressive approach is that information is exchanged even before a secure channel is established. But it is faster than the main mode.

3.4.3 IKE Phase Two

Phase ensures the identity of peers is correct i.e it authenticates and are going to be part of phase two where in phase two IPSEC SA are negotiated to set ipse tunnel. IKE phase two has the following functions:

- Negotiating IPSec SA parameters that are protected by IKE SA that already exists.
- Establishing IPSec security associations.
- Renegotiating IPSec SAs periodically to ensure security.

IKE phase 2 has just one mode, which is called quick mode. It occurs after phase one when IKE has established the secure tunnel. After phase one a shared IPSec policy is negotiated and IPSec SAs are established. Quick mode also renegotiates a new IPSec SA when the IPSec SA lifetime expires.

Perfect Forward Secrecy

When the key material has greater key material life then it offers more resistance to cryptographic attacks. This can be achieved in IPSEC by specifying perfect forward secrecy (PFS) in the IPSec policy as a result of this a new Diffie-Hellman exchange is performed with each quick mode. Drawback of this approach is that each exchange requires large exponentiations, thereby increasing CPU use and also increasing cost of performance.

3.4.4: IPSec Encrypted Tunnel

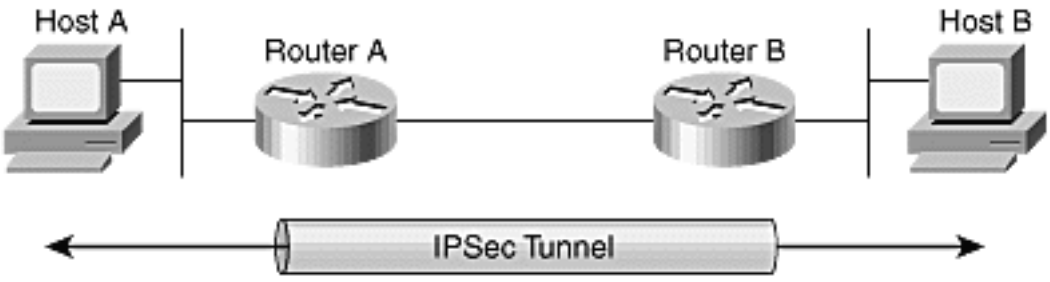

Figure 22. IPSec encrypted tunnel (figure 1-18) [10]

Fig. 22 shows example of IPSec tunnel between routers thus securing the traffic between Host A and Host B. The completion of phase one and phase two allows information now to be exchanged by an IPSec tunnel. IPSec tunnel allow packets to be encrypted and decrypted using the encryption specified in the IPSec SA.

3.4.5: Tunnel Termination

Every IPSec SA have a timeout thus after that time they are terminated. The keys are also discarded when the SA terminate. If there is need for an IPSec SA again then the phase two is repeated. It is not necessary to interrupt the flow since new SA can be established before the old SA expires and thus not interrupting a given flow.

3.5 IPSec Header

Authentication Header format																															
Offsets	$Octet_{16}$	0								1								2								3					
$Octet_{16}$	Bit_{10}	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	*Next Header*								*Payload Len*								*Reserved*															
4	32	*Security Parameters Index (SPI)*																															
8	64	*Sequence Number*																															
C	96	*Integrity Check Value (ICV)*																															
...	...	...																															

Figure 23. Authentication header format [13]

Authentication Header

Fig. 23 shows the authentication header format. Authentication header IPSec makes sure the origin of data authentication and integrity of IP packets. For example in IPv4 AH protects the IP payload and header fields of IP datagram. AH operated on top of IP header and has a protocol number of 51.

The authentication header consists of following fields:

1. Next Header (8 bits)
   This field indicates the type of next header inside the packet and the value is usually ip protocol number.
2. Payload Len (8 bits)
   The length of this *Authentication Header* in 4-octet unit
3. *Reserved* (16 bits)
   It is reserved for future use but till now its all zero.

4. Security Parameters Index (32 bits)
   It contains a number that identifies the SA of receiving party. It is a random number joined together with detention IP address.
5. Sequence Number (32 bits)
   This number is a continuously increasing number that increases with every incoming packet. The main use of this number is to prevent all replay attacks. It prevents them by never reusing the same number again.
6. *Integrity Check Value* (multiple of 32 bits)
   It is a variable length check value.

3.6 Design Selection

IPSec Direct Encapsulation Design:

This design model enables IPSec to act itself as a tunnel and thus it can alone be used as a connection method. IPSec direct encapsulation design cannot transport dynamic routing protocols.

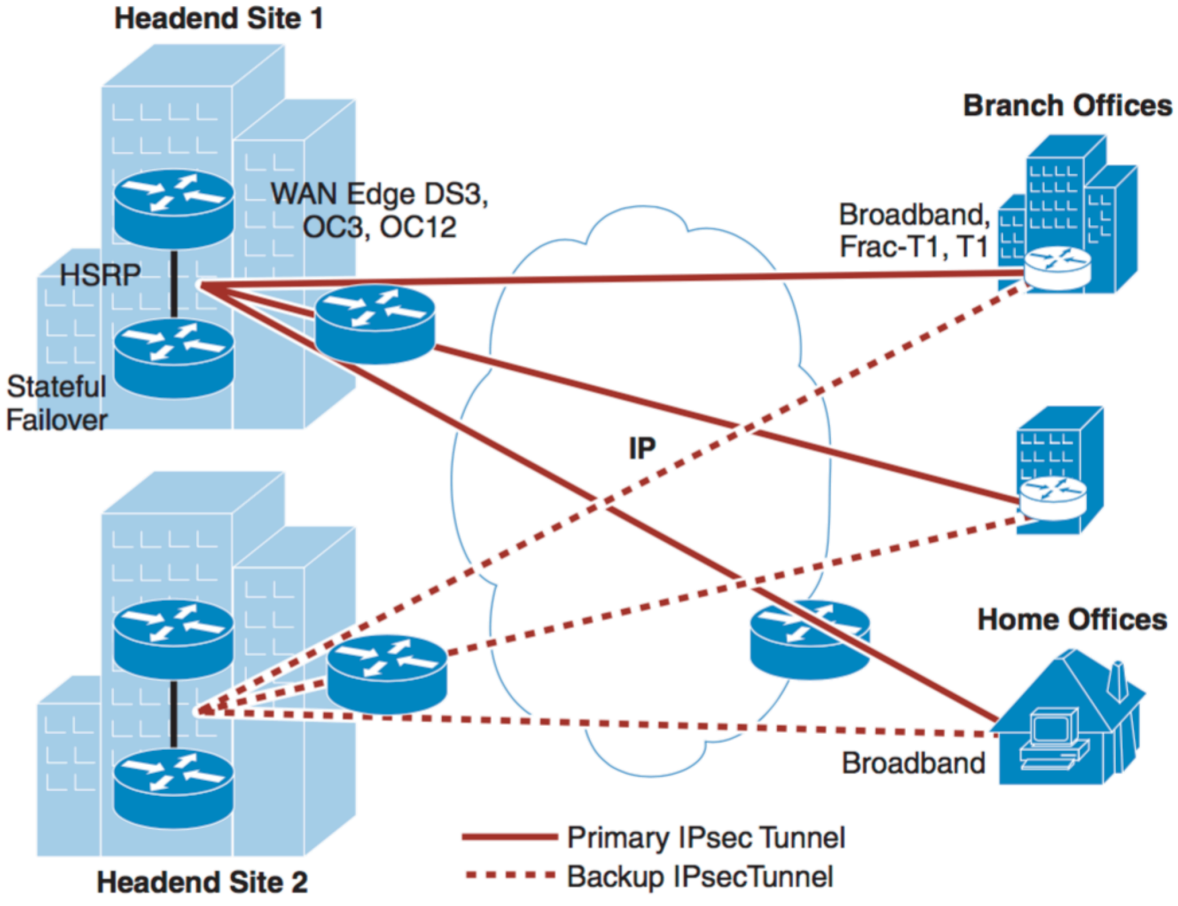

Figure 24. IPSec direct encapsulation design [5] (page 30)

Fig. 24 shows the IPSec design topology where the remote sites have connection to two sites. In this design topology the remote have an IPSec tunnel to a predefined headend i.e. usually a HQ. Remote Sites can have static or dynamic ip addresses but the headend is only supposed to have static IP address. Branch routers i.e. remote are configured with a list of heads ends as a result if a router is not able to connect to the first headend it can establish a connection with the next one and will keep trying until it establishes a

connection with one of the headend. In our designed topology we are using two Headend. The advantages to go with this design is that it can all cisco IOS router platforms support this design i.e. 870, ISP2800/3800 etc. Also interoperability with non-cisco devices can be achieved when using IPSec direct encapsulation. IT is usually used in designs where we don’t have any requirement for dynamic IGP routing, or we have only one subnet.

3.7 Network Diagram

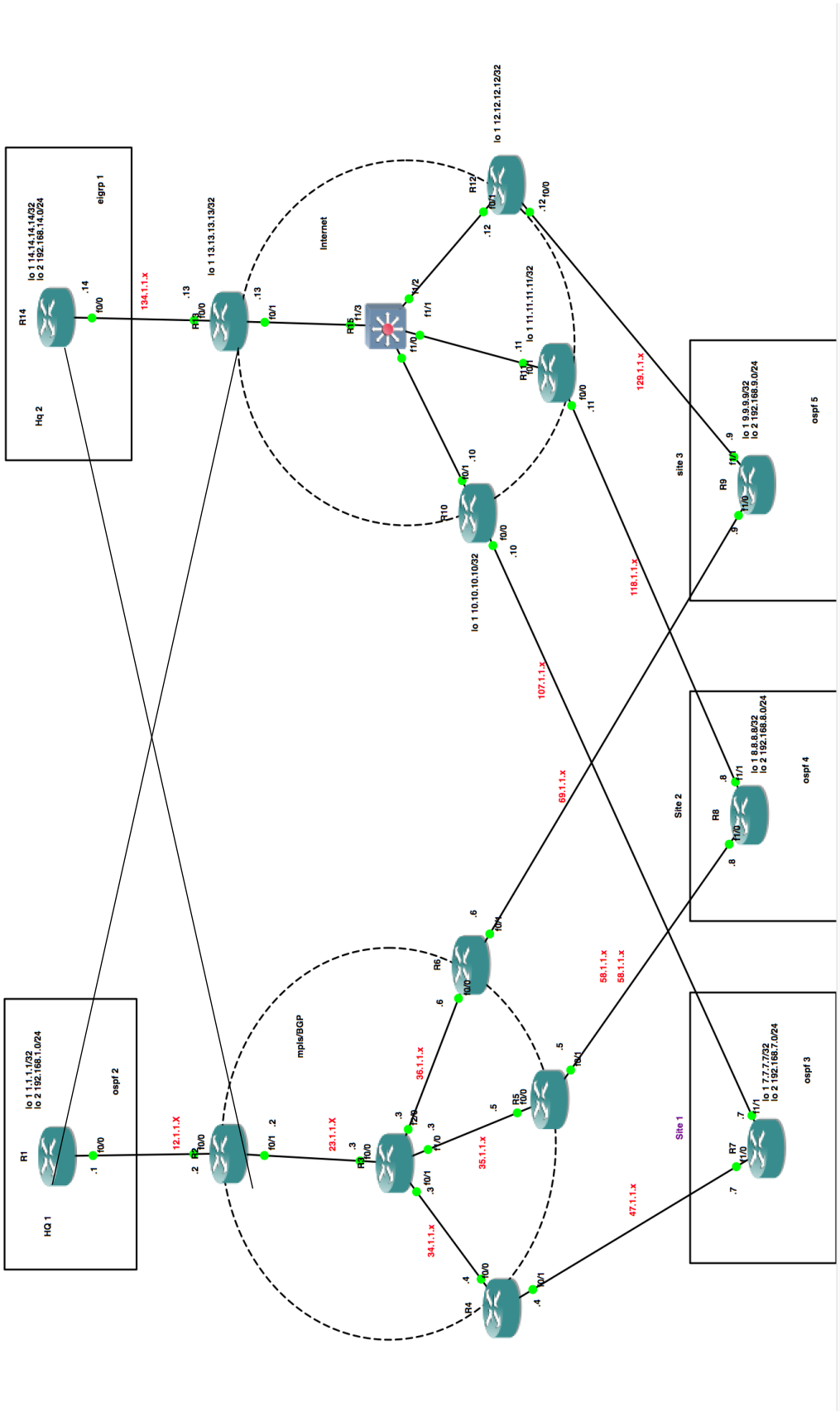

Figure 25. Network Diagram

Fig. 25 shows the network diagram used in GNS3 to emulate the network required to implement IPSec in network.

3.8 Configuration

Router 1

```
hostname hq1

interface Loopback1
 ip address 1.1.1.1 255.255.255.255
!
interface Loopback2
 ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 12.1.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 131.1.1.1 255.255.255.0
 speed 100
 full-duplex
!
router ospf 2
 log-adjacency-changes
 network 1.1.1.1 0.0.0.0 area 0
 network 12.1.1.1 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 131.1.1.13
```

Router 2

```
hostname R2

interface Loopback1
 ip address 2.2.2.2 255.255.255.255
!
interface FastEthernet0/0
 ip address 12.1.1.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 23.1.1.2 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet1/0
 ip address 141.1.1.2 255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 23.1.1.2 0.0.0.0 area 0
!
router ospf 2
 log-adjacency-changes
 redistribute bgp 1 metric 100 metric-type 1
subnets
 network 12.1.1.2 0.0.0.0 area 0
!
router ospf 6
 log-adjacency-changes
 redistribute bgp 1 metric 100 metric-type 1
subnets
 network 141.1.1.2 0.0.0.0 area 0
!
router bgp 1
 bgp log-neighbor-changes
 neighbor 4.4.4.4 remote-as 1
 neighbor 4.4.4.4 update-source Loopback1
 neighbor 5.5.5.5 remote-as 1
 neighbor 5.5.5.5 update-source Loopback1
 neighbor 6.6.6.6 remote-as 1
 neighbor 6.6.6.6 update-source Loopback1
 !
 address-family ipv4
  redistribute ospf 2 metric 10
  redistribute ospf 6 metric 10
  neighbor 4.4.4.4 activate
  neighbor 4.4.4.4 next-hop-self
  neighbor 5.5.5.5 activate
  neighbor 6.6.6.6 activate
  no auto-summary
  no synchronization
  bgp redistribute-internal
 exit-address-family
```

Router 3

```
hostname R3

interface Loopback1
 ip address 3.3.3.3 255.255.255.255
!
interface FastEthernet0/0
 ip address 23.1.1.3 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet0/1
 ip address 34.1.1.3 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
```

```
interface FastEthernet1/0
 ip address 35.1.1.3 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet2/0
 ip address 36.1.1.3 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 3.3.3.3 0.0.0.0 area 0
 network 23.1.1.3 0.0.0.0 area 0
 network 34.1.1.3 0.0.0.0 area 0
 network 35.1.1.3 0.0.0.0 area 0
 network 36.1.1.3 0.0.0.0 area 0
```

Router 4

```
hostname R4

interface Loopback1
 ip address 4.4.4.4 255.255.255.255
!
interface FastEthernet0/0
 ip address 34.1.1.4 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet0/1
 ip address 47.1.1.4 255.255.255.0
 ip ospf dead-interval 100
 speed 100
 full-duplex
!
router ospf 1
 log-adjacency-changes
 network 4.4.4.4 0.0.0.0 area 0
 network 34.1.1.4 0.0.0.0 area 0
!
router ospf 3
 log-adjacency-changes
 redistribute bgp 1 subnets
 network 47.1.1.4 0.0.0.0 area 0
!
router bgp 1
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 1
 neighbor 2.2.2.2 update-source Loopback1
 neighbor 5.5.5.5 remote-as 1
 neighbor 5.5.5.5 update-source Loopback1
 neighbor 6.6.6.6 remote-as 1
 neighbor 6.6.6.6 update-source Loopback1
 !
 address-family ipv4
  redistribute ospf 3 metric 10
  neighbor 2.2.2.2 activate
  neighbor 5.5.5.5 activate
  neighbor 6.6.6.6 activate
  no auto-summary
  no synchronization
  bgp redistribute-internal
  network 4.4.4.4 mask 255.255.255.255
 exit-address-family
```

Router 5

```
hostname R5

interface Loopback1
 ip address 5.5.5.5 255.255.255.255
!
interface FastEthernet0/0
 ip address 35.1.1.5 255.255.255.0
 speed 100
 full-duplex
 mpls ip
!
interface FastEthernet0/1
 ip address 58.1.1.5 255.255.255.0
 ip ospf dead-interval 100
 speed 100
 full-duplex
!
router ospf 1
 log-adjacency-changes
 network 5.5.5.5 0.0.0.0 area 0
 network 35.1.1.5 0.0.0.0 area 0
!
router ospf 4
 log-adjacency-changes
 redistribute bgp 1 subnets
 network 58.1.1.5 0.0.0.0 area 0
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 bgp redistribute-internal
 redistribute ospf 4 metric 10
 neighbor 2.2.2.2 remote-as 1
 neighbor 2.2.2.2 update-source Loopback1
 neighbor 4.4.4.4 remote-as 1
 neighbor 4.4.4.4 update-source Loopback1
 neighbor 6.6.6.6 remote-as 1
 neighbor 6.6.6.6 update-source Loopback1
 no auto-summary
```

Router 6

```
hostname R6

mpls label protocol ldp
multilink bundle-name authenticated

interface Loopback1
 ip address 6.6.6.6 255.255.255.255
!
interface FastEthernet0/0
 ip address 36.1.1.6 255.255.255.0
 speed 100
 full-duplex
 mpls ip
!
interface FastEthernet0/1
 ip address 69.1.1.6 255.255.255.0
 ip ospf dead-interval 80
 speed 100
 full-duplex
!
router ospf 1
 log-adjacency-changes
 network 6.6.6.6 0.0.0.0 area 0
 network 36.1.1.6 0.0.0.0 area 0
!
router ospf 5
 log-adjacency-changes
 redistribute bgp 1 subnets
 network 69.1.1.6 0.0.0.0 area 0
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 bgp redistribute-internal
 redistribute ospf 5 metric 10
 neighbor 2.2.2.2 remote-as 1
 neighbor 2.2.2.2 update-source Loopback1
 neighbor 4.4.4.4 remote-as 1
 neighbor 4.4.4.4 update-source Loopback1
 neighbor 5.5.5.5 remote-as 1
 neighbor 5.5.5.5 update-source Loopback1
 no auto-summary
```

Router 7

```
hostname site1

track 1 ip sla 1

crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key connecthq address 134.1.1.14
!
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
 mode tunnel

crypto map CMAP 10 ipsec-isakmp
 set peer 134.1.1.14
 set transform-set TS
 match address VPN

interface Loopback1
 ip address 7.7.7.7 255.255.255.255
!
interface Loopback2
 ip address 192.168.7.1 255.255.255.0

interface FastEthernet1/0
 ip address 47.1.1.7 255.255.255.0
 ip ospf dead-interval 100
 speed auto
 duplex auto
!
interface FastEthernet1/1
 ip address 107.1.1.7 255.255.255.0
 speed auto
 duplex auto
 crypto map CMAP

router eigrp 1
 network 7.7.7.7 0.0.0.0
 network 147.1.0.0
!
router ospf 3
 network 7.7.7.7 0.0.0.0 area 0
 network 47.1.1.7 0.0.0.0 area 0
 network 192.168.7.1 0.0.0.0 area 0

ip access-list extended VPN
 permit ip 192.168.7.0 0.0.0.255 192.168.14.0 0.0.0.255
 permit ip 7.7.7.0 0.0.0.255 192.168.14.0 0.0.0.255
 permit ip 7.7.7.0 0.0.0.255 14.14.14.0 0.0.0.255
 permit ip 192.168.7.0 0.0.0.255 14.14.14.0 0.0.0.255
 permit ip 192.168.7.0 0.0.0.255 8.8.8.0 0.0.0.255
 permit ip 7.7.7.0 0.0.0.255 8.8.8.0 0.0.0.255
 permit ip 7.7.7.0 0.0.0.255 9.9.9.0 0.0.0.255
 permit ip 192.168.7.0 0.0.0.255 9.9.9.0 0.0.0.255
!
ip sla 1
```

```
 icmp-echo 141.1.1.14 source-interface Loopback1
 frequency 6
ip sla schedule 1 life forever start-time now

event manager applet hq2
 event track 1 state down
 action 1.0 cli command "enable"
 action 1.5 cli command "config t"
 action 2.0 cli command "ip route 0.0.0.0 0.0.0.0 107.1.1.10"
event manager applet hq2up
 event track 1 state up
 action 3.0 cli command "enable"
 action 3.5 cli command "config t"
 action 4.0 cli command "no ip route 0.0.0.0 0.0.0.0 107.1.1.10"
```

Router 8

```
hostname site2

track 1 ip sla 1

crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key consite2 address 134.1.1.14
!
!
crypto ipsec transform-set TS2 esp-3des esp-md5-hmac
 mode tunnel

crypto map CMAP 20 ipsec-isakmp
 set peer 134.1.1.14
 set transform-set TS2
 match address VPN

interface Loopback1
 ip address 8.8.8.8 255.255.255.255
!
interface Loopback2
 ip address 192.168.8.1 255.255.255.255

interface FastEthernet1/0
 ip address 58.1.1.8 255.255.255.0
 ip ospf dead-interval 100
 speed auto
 duplex auto
!
interface FastEthernet1/1
 ip address 118.1.1.8 255.255.255.0
 speed auto
 duplex auto
 crypto map CMAP
!
!
router eigrp 1
 network 8.8.8.8 0.0.0.0
 network 147.1.1.0 0.0.0.255
 network 192.168.8.0
!
router ospf 4
 network 8.8.8.8 0.0.0.0 area 0
 network 58.1.1.8 0.0.0.0 area 0

ip access-list extended VPN
 permit ip 192.168.8.0 0.0.0.255 192.168.14.0 0.0.0.255
 permit ip 8.8.8.0 0.0.0.255 192.168.14.0 0.0.0.255
 permit ip 8.8.8.0 0.0.0.255 14.14.14.0 0.0.0.255
 permit ip 192.168.8.0 0.0.0.255 14.14.14.0 0.0.0.255
 permit ip 8.8.8.0 0.0.0.255 7.7.7.0 0.0.0.255
 permit ip 8.8.8.0 0.0.0.255 9.9.9.0 0.0.0.255
!
ip sla 1
 icmp-echo 141.1.1.14 source-interface Loopback1
ip sla schedule 1 life forever start-time now

event manager applet hq2
 event track 1 state down
 action 1.0 cli command "enable"
 action 1.5 cli command "config t"
 action 2.0 cli command "ip route 0.0.0.0 0.0.0.0 118.1.1.11"
event manager applet hq2up
 event track 1 state up
 action 3.0 cli command "enable"
 action 3.5 cli command "config t"
 action 4.0 cli command "no ip route 0.0.0.0 0.0.0.0 118.1.1.11"
```

Router 9

```
hostname site3

track 1 ip sla 1

crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key consite3 address 134.1.1.14
```

```
crypto ipsec transform-set TS3 esp-3des esp-
md5-hmac
 mode tunnel

crypto map CMAP 30 ipsec-isakmp
 set peer 134.1.1.14
 set transform-set TS3
 match address VPN

interface Loopback1
 ip address 9.9.9.9 255.255.255.255
!
interface Loopback2
 ip address 192.168.9.1 255.255.255.0

interface FastEthernet1/0
 ip address 69.1.1.9 255.255.255.0
 ip ospf dead-interval 80
 speed auto
 duplex auto
!
interface FastEthernet1/1
 ip address 129.1.1.9 255.255.255.0
 speed auto
 duplex auto
 crypto map CMAP
!
!
router eigrp 1
 network 9.9.9.9 0.0.0.0
 network 147.1.1.0 0.0.0.255
 network 192.168.9.0
!
router ospf 5
 network 9.9.9.9 0.0.0.0 area 0
 network 69.1.1.9 0.0.0.0 area 0
 network 192.168.9.1 0.0.0.0 area 0
!

no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 129.1.1.12
!
ip access-list extended VPN
 permit ip 192.168.9.0 0.0.0.255 192.168.14.0
0.0.0.255
 permit ip 9.9.9.0 0.0.0.255 192.168.14.0
0.0.0.255
 permit ip 9.9.9.0 0.0.0.255 14.14.14.0
0.0.0.255
 permit ip 192.168.9.0 0.0.0.255 14.14.14.0
0.0.0.255
 permit ip 9.9.9.0 0.0.0.255 7.7.7.0 0.0.0.255
 permit ip 9.9.9.0 0.0.0.255 8.8.8.0 0.0.0.255
!
ip sla 1
 icmp-echo 141.1.1.14 source-interface
Loopback1
 frequency 6
ip sla schedule 1 life forever start-time now

event manager applet hq2
 event track 1 state down
 action 1.0 cli command "enable"
 action 1.5 cli command "config t"
 action 2.0 cli command "ip route 0.0.0.0
0.0.0.0 129.1.1.12"
!
end
```

Router 10

```
hostname R10

interface Loopback1
 ip address 10.10.10.10 255.255.255.255
!
interface FastEthernet0/0
 ip address 107.1.1.10 255.255.255.0
 speed 100
 full-duplex
!
interface FastEthernet0/1
 ip address 110.1.1.2 255.255.255.0
 speed 100
 full-duplex
!
router eigrp 100
 redistribute connected
 network 10.10.10.0 0.0.0.255
 network 110.1.1.0 0.0.0.255
 no auto-summary
```

Router 11

```
hostname R11

interface Loopback1
 ip address 11.11.11.11 255.255.255.255
!
interface FastEthernet0/0
 ip address 118.1.1.11 255.255.255.0
 speed 100
 full-duplex
!
interface FastEthernet0/1
 ip address 111.1.1.2 255.255.255.0
 speed 100
 full-duplex
!
router eigrp 100
 redistribute connected
```

```
 network 11.11.11.11 0.0.0.0
 network 111.1.1.0 0.0.0.255
 no auto-summary
```

Router 12

```
hostname R12

interface Loopback1
 ip address 12.12.12.12 255.255.255.255
!
interface FastEthernet0/0
 ip address 129.1.1.12 255.255.255.0
 speed 100
 full-duplex
!
interface FastEthernet0/1
 ip address 112.1.1.2 255.255.255.0
 speed 100
 full-duplex
!
router eigrp 100
 redistribute connected
 network 12.12.12.12 0.0.0.0
 network 112.1.1.0 0.0.0.255
 no auto-summary
```

Router 13

```
hostname R13

interface Loopback1
 ip address 13.13.13.13 255.255.255.255
!
interface FastEthernet0/0
 ip address 134.1.1.13 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 113.1.1.2 255.255.255.0
 speed 100
 full-duplex
!
interface FastEthernet1/0
 ip address 131.1.1.13 255.255.255.0
 duplex auto
 speed auto
!
router eigrp 100
 redistribute connected
 network 13.13.13.13 0.0.0.0
 network 113.1.1.0 0.0.0.255
 no auto-summary
!
ip forward-protocol nd
ip route 14.14.14.14 255.255.255.255 134.1.1.14
ip route 192.168.14.0 255.255.255.0 134.1.1.14
```

Router 14

```
hostname R14
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key connecthq address 107.1.1.7
crypto isakmp key consite2 address 118.1.1.8
crypto isakmp key consite3 address 129.1.1.9
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
crypto ipsec transform-set TS2 esp-3des esp-md5-hmac
crypto ipsec transform-set TS3 esp-3des esp-md5-hmac
!
crypto map CMAP 10 ipsec-isakmp
 set peer 107.1.1.7
 set transform-set TS
 match address VPN
crypto map CMAP 20 ipsec-isakmp
 set peer 118.1.1.8
 set transform-set TS2
 match address VPN2
crypto map CMAP 30 ipsec-isakmp
 set peer 129.1.1.9
 set transform-set TS3
 match address VPN3

interface Loopback1
 ip address 14.14.14.14 255.255.255.255
!
interface Loopback2
 ip address 192.168.14.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 134.1.1.14 255.255.255.0
 duplex auto
 speed auto
 crypto map CMAP
!
interface FastEthernet0/1
 ip address 141.1.1.14 255.255.255.0
 speed 100
 full-duplex
!
router eigrp 1
```

```
 network 14.14.14.14 0.0.0.0
 network 147.1.0.0
 network 192.168.14.0
 no auto-summary
!
router ospf 6
 log-adjacency-changes
 network 14.14.14.14 0.0.0.0 area 0
 network 141.1.1.14 0.0.0.0 area 0
 network 192.168.14.0 0.0.0.255 area 0
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 134.1.1.13
!
ip access-list extended VPN
 permit ip 192.168.14.0 0.0.0.255 192.168.7.0
0.0.0.255
 permit ip 192.168.14.0 0.0.0.255 7.7.7.0
0.0.0.255
 permit ip 14.14.14.0 0.0.0.255 7.7.7.0
0.0.0.255
 permit ip 14.14.14.0 0.0.0.255 192.168.7.0
0.0.0.255
 permit ip 8.8.8.0 0.0.0.255 7.7.7.0 0.0.0.255
 permit ip 9.9.9.0 0.0.0.255 7.7.7.0 0.0.0.255
ip access-list extended VPN2
 permit ip 14.14.14.0 0.0.0.255 192.168.8.0
0.0.0.255
 permit ip 14.14.14.0 0.0.0.255 8.8.8.0
0.0.0.255
 permit ip 192.168.14.0 0.0.0.255 8.8.8.0
0.0.0.255
 permit ip 192.168.14.0 0.0.0.255 192.168.8.0
0.0.0.255
 permit ip 7.7.7.0 0.0.0.255 8.8.8.0 0.0.0.255
 permit ip 9.9.9.0 0.0.0.255 8.8.8.0 0.0.0.255
ip access-list extended VPN3
 permit ip 14.14.14.0 0.0.0.255 192.168.9.0
0.0.0.255
 permit ip 14.14.14.0 0.0.0.255 9.9.9.0
0.0.0.255
 permit ip 192.168.14.0 0.0.0.255 9.9.9.0
0.0.0.255
 permit ip 192.168.14.0 0.0.0.255 192.168.9.0
0.0.0.255
 permit ip 7.7.7.0 0.0.0.255 9.9.9.0 0.0.0.255
 permit ip 8.8.8.0 0.0.0.255 9.9.9.0 0.0.0.255
```

Router 15

```
hostname R15-SW

interface FastEthernet1/0
 switchport access vlan 10
 duplex full
 speed 100
!
interface FastEthernet1/1
 switchport access vlan 11
 duplex full
 speed 100
!
interface FastEthernet1/2
 switchport access vlan 12
 duplex full
 speed 100
!
interface FastEthernet1/3
 switchport access vlan 13
 duplex full
 speed 100

interface Vlan10
 ip address 110.1.1.1 255.255.255.0
!
interface Vlan11
 ip address 111.1.1.1 255.255.255.0
!
interface Vlan12
 ip address 112.1.1.1 255.255.255.0
!
interface Vlan13
 ip address 113.1.1.1 255.255.255.0
!
router eigrp 100
 network 110.1.1.0 0.0.0.255
 network 111.1.1.0 0.0.0.255
 network 112.1.1.0 0.0.0.255
 network 113.1.1.0 0.0.0.255


 no auto-summary
```

3.9 Template for Configuration of routers

Spoke Routers:

The configuration starts by defining IKE policies, which are defined using command crypto isakmp policy x, this command, enables IKE policy configuration command mode where we can specify the parameters that will be used during the IKE negotiation. Now after these parameters are defined, a pre shared key is defined and it should be identical at both peers. The command that is needed to run to achieve this is done on global configuration mode *crypto isakmp key <name > address <Ip address>.*

Now we need to define the parameters for IPSec policy to be used in phase 2. Configuration for IPSec policies is done using *crypto ipse transform-set <name> esp-3des esp-md5-hmac.* This enables the crypto transform configuration mode and where the transform sets that are used during an IPSec negotiation can be specified. Now we need to tell the router what will be used to establish IKE and then secure the IPSec SA. The command *crypto map <name> 10 ipsec-isakmp* indicates the IKE used to establish the IPSec security association for protecting the traffic specified by this crypto map entry. Under its configuration mode IP address of remote end can be specified using *set peer <ip-address>* and IPSec can also be configured to use the transform set that was defined earlier in the configuration using command *set transform-set <name>.* The last step is to match i.e specify the traffic to be encrypted that is done using *match address <access-list number>.*

The access lists that help in identifying the interesting traffic also needs to be defined and it is done using command *ip access-list extended <name >* and then specifying the traffic to be encrypted under it using *permit ip <source-network-address> <network-mask> <dest-network-address> <network-mask>.* The last step now is to apply this crypto map to the outgoing interface which is done by going in interface configuration mode and using command *crypto map <crypto-map name>.*

IPSec configuration

```
crypto isakmp policy x
 encr 3des
 hash md5
 authentication pre-share
 group 2

crypto isakmp key <isakmp-name> address <ip-address of HQ>

crypto ipsec transform-set <transform-set name> esp-3des esp-md5-hmac
 mode tunnel

crypto map <crypto-map-name> <number> ipsec-isakmp
 set peer <peer-ip address(hq)>
 set transform-set <transform-set name>
 match address <access-list name>

interface FastEthernet <x/x>
 ip address <ip address>
 speed auto
 duplex auto
 crypto map <crypto-map-name>
```

Routing Protocol Configuration

```
router ospf 3
 network x.x.x.x 0.0.0.0 area 0
```

Access-list configuration

```
ip access-list extended <access-list name>
```

```
 permit ip <source-network-address> <network-mask> <dest-network-address> <network-mask>!
```
IP sla configuration
```
ip sla <sla-number>
 icmp-echo <ip-address> source-interface <interface-name>
 frequency <seconds>
```

Scheduling SLA configuration
```
ip sla schedule <sla-number> life forever start-time now
```

Event Manager configuration
```
event manager applet <name-for-applet>
event track x state down
 action 1.0 cli command "enable"
 action 1.5 cli command "config t"
 action 2.0 cli command "ip route 0.0.0.0 0.0.0.0 x.x.x.x”

event manager applet <name>
 event track 1 state up
 action 3.0 cli command "enable"
 action 3.5 cli command "config t"
 action 4.0 cli command "no ip route 0.0.0.0 0.0.0.0 x.x.x.x”
```

Hub Routers:

The configuration for hub router is same as spoke router but the difference is it will have more number of crypto maps with different sequence number, one for each of the spoke. All crypto maps are given same name but different sequence number because only one crypto map can be applied to an interface, thus all peers are defined in a single crypto map.

Configuration starts with configuration for IKE policies, which enables the IKE policy configuration command mode where the parameters that are used during an IKE negotiation are defined. then a pre shared key is defined for each peer but key should be same on spoke routers. After that a transform set is defined to be used in IPSEC negotiation.

```
crypto isakmp policy x
 encr 3des
 hash md5
 authentication pre-share
 group 2


crypto isakmp key <name> address <peer1-ip-address>
crypto isakmp key <name> address <peer2-ip-address>
crypto isakmp key <name> address <peer3-ip-address>

crypto ipsec transform-set <name1> esp-3des esp-md5-hmac
crypto ipsec transform-set <name2> esp-3des esp-md5-hmac
crypto ipsec transform-set <name3> esp-3des esp-md5-hmac

crypto map <crypto-map-name> <SQ-number> ipsec-isakmp
 set peer <peer1-ip-address>
 set transform-set <name1>
 match address <ip-access-list-name1>
crypto map <crypto-map-name> <SQ-number2> ipsec-isakmp
 set peer <peer2-ip-address>
```

```
 set transform-set <name2>
 match address <ip-access-list-name2>
crypto map <crypto-map-name> <SQ-number> ipsec-isakmp
 set peer <peer3-ip-address>
 set transform-set <name3>
 match address <ip-access-list-name3>
```

Interface Configuration

```
interface FastEthernet x/x
 ip address x.x.x.x x.x.x.x
 duplex auto
 speed auto
 crypto map <crypto-map-name>
```

Routing protocol config

```
router eigrp x
network x.x.x.x
 no auto-summary

router ospf x
 log-adjacency-changes
 network x.x.x.x 0.0.0.0 area 0
```

Static route

```
ip route 0.0.0.0 0.0.0.0 <GW-ip>
```

Access list config

```
ip access-list extended <ip-access-list-name1>
  permit ip <source-network-address> <network-mask> <dest-network-address> <network-mask>!

ip access-list extended <ip-access-list-name2>
 permit ip <source-network-address> <network-mask> <dest-network-address> <network-mask>!

ip access-list extended<ip-access-list-name3>
 permit ip <source-network-address> <network-mask> <dest-network-address> <network-mask>!
```

3.10 Results

Latency:
The IPSec tunnel implemented in GNS3 the ping results showed latency of 87 ms.

Convergence:
The current configuration and emulation in GNS3 showed a convergence time of 1.827 seconds

3.11 Advantages of IPSec Tunnel

1. Network Layer level security:
   Unlike ssl VPN where VPN rely on application layer-specific protocols like SSL the IPSec Vpn become a part of network itself. The Advantages related to this is that it is completely invisible to end user while its in operation. As a result the end users are not required to learn about it and neither they have to manage or interact with IPSec.

2. Monitors all kind of traffic
   IPSec VPN operates at the network layer level as a result it can monitor as well as secure all kinds of internet traffic, inbound an outbound.

3. Strong Encryption

4. Transparent to Applications:
   IPSec is below transport layer that is TCP and UDP so as a result is IPSec is implemented over a firewall etc. it will not implement the functioning of firewall.
5. Costeffective
   Cost of getting a ISP connection is less than a wan circuit. The functionality of WAN circuit can be implemented on a ISP connection using VPN.

6. DeploymentFlexibility
   IPSec VPN can be easily implemented if an internet connection is available. This offers flexibility since it can be implemented in places where no WAN circuit or IP VPN services are present.

7. Resiliency
   Businesses often use applications such as VOIP and other mission critical applications that are deployed to branch offices. One way of providing redundancy was to use multiple WAN connections but this becomes Cost ineffective, whereas using IPSec over ISP connections provides a cost effective secondary wan connections for branch offices.

8. Scalability
   The flexibility of IPSec VPN enables a customer to expect large scale aggregations as compared to WANs.

9. Interoperability with non-cisco devices that are RFC complaint.

3.12 Disadvantages of IPSec Tunnel

1. IP multicast and other non-IP protocols are not supported by IPSec.

2. Routing protocols such as EIGRP and OSPF cannot be used therefore IPSec tunnel does not support dynamic Interior Gateway routing protocols.

3. Tunnel is only made logically by applying crypto map to outgoing interface thus only one tunnel can be formed at a time so if primary tunnel is lost then no secondary tunnel is already established to take over thus traffic will be dropped or sent unencrypted till new tunnel is formed.

4. Implementing QOS is not possible since there is a tunnel formed for every flow instead of just one tunnel.

5. IPSec anti-replay packet drop occurs when QOS service policies are configured with IPSec.

6. Scalability is a big problem in implementing IPSec tunnels thus they are difficult to scale because IPSec tunnel needs to be provisioned between each pair of IPSec gateways. Its more difficult to scale when a full mesh connectivity is required.

7. High CPU overhead is associated with IPSEC on VPN gateways because of processing of packet for encryption/decryption and authentication.

Router Selection

4.1 HUB Routers:

The model of router to be used in design is usually determined by the amount of bandwidth required at the wan aggregation site. The following table provides DMVPN hub router options and the options associated with it that is used to determine what router to be used at HUB. Table. 1 compared cisco router models for HUB.

Table 1. Cisco HUB router comparison [14] (page 19)

Option	Cisco 3925	Cisco 3945	ASR 1001	ASR 1002
Ethernet WAN	100 Mbps	150 Mbps	250 Mbps	500 Mbps
Software redundancy	None	None	Yes	Yes
Redundant power	Option	Option	Default	Default
Number of Sites	25	50	100	250

4.2 Remote Site Routers:

The router needed for remote site depends on the bandwidth required for the location. There are also various other factors to take care when choosing routers for remote sites such as amount required and traffic to be expected. Also enough interfaces should be present on the routers as well as proper licenses for the topology. Table. 2 shows cisco router model for remote sites.

Table 2. Cisco remote router comparison [14] (page 19)

Option	1941	2911	2921	2951	3925	3945
Ethernet WAN	25 Mbps	35 Mbps	50 Mbps	75 Mbps	100 Mbps	150 Mbps
GE ports	2	3	3	3	3	3
Service module slots	No	No	No	No	Yes	Yes

The dmvpn routers for spoke are directly connecting to Internet though the router interface. Having a Single link connecting to the Internet for DMVPN is the most basic requirement for any DMVPN site.
Selection of router varies because remote site can be configured to use single DMVPN with single link, as the primary WAN but in this case if failure occurs than there is no redundancy. Fig. 26 shows the single link DMVPN topology but no redundancy is provided my this design topology.

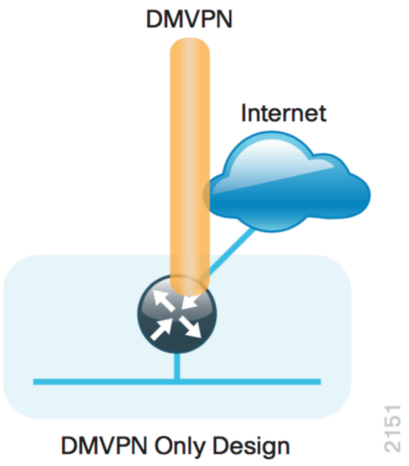

Figure 26. DMVPN remote site (Single link- single router) [14] (Page 20)

Fig. 27 shows the alternate to single link DMVPN topology that is two link design topology. Now the next case is to use single DMVPN with two links. These two links are connected to same router and in case one fails it will switch to other link. The last case is what if in single DMVPN, then both links will be down and as a result we will loose connectivity. In this case we have to be sure that the router has two interfaces so that it can connect

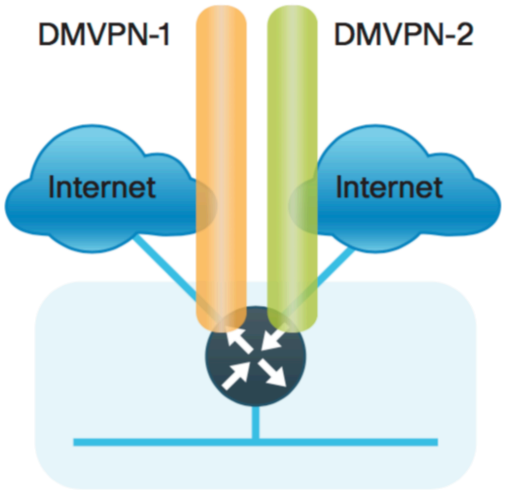

Figure 27. DMVPN +DMVPN remote site [14] (page 20)

Fig. 28 shows dual router dual link topology where redundancy is provided for both router and ink. Another option is Dual- DMVPN with dual links. But in my topology I am using single router with one WAN option as MPLS and other WAN option being DMVPN over Internet or IPSec over internet. In this case the cost of one more router increases.

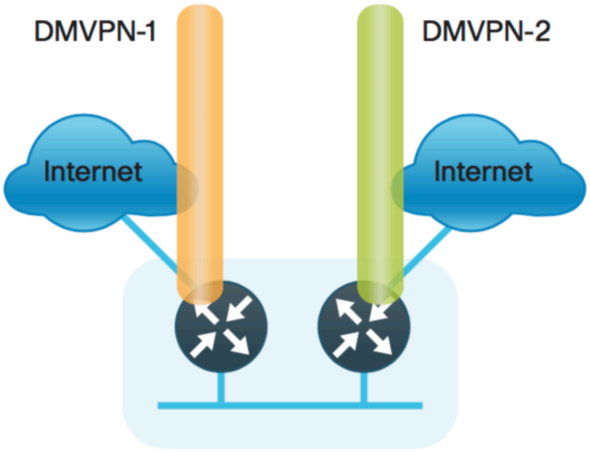

Figure 28. DMVPN + DMVPN dual router [14] (page 20)

Here are the two slightly different ways with which the cost of another router can be decreased but the cost will probably increases because MPLS feature has to be present in router. Fig. 29 is an example of MPLS usage in design topology.

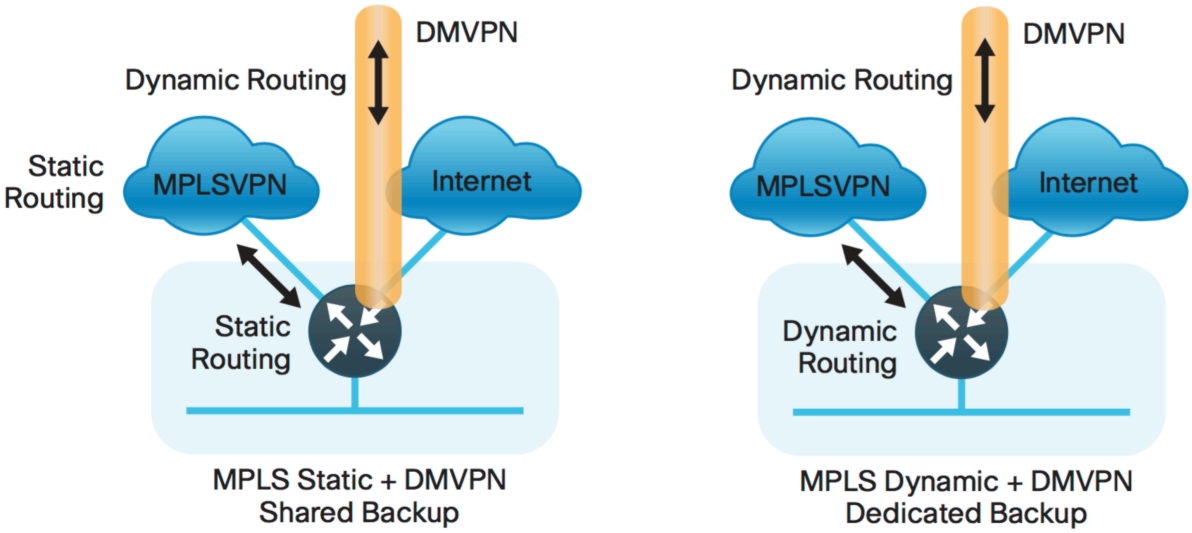

Figure 29. MPLS + DMVPN design [14] (Page 21)

BOM

Table 3. Bill of Materials

BOM

Enterprise VPN							
Customer Name	N/A						
Design name	Enterprise based VPN						
Network Total Price(CAD)	67857						
	Site ID	Product ID	Quantity	Unit Price(CAD)	Total Price(CAD)		
	Site1-10	CISCO3825	10	3990	39900		
		CAB-L620P-C13-US	10	25	250		
		CAB-RPS2300	10	600	6000		
		C3K-PWR-750WAC	10	462	4620		
	HQ	C3825-35UC-VSEC/K9	2	8025	16000		
		CAB-L620P-C13-US	1	25	25		
		CAB-RPS2300	1	600	600		
		C3K-PWR-750WAC	1	462	462		

Table. 3 that depicts the bill of materials that is an estimation of cost of network that the company will have to spend for 3 sites and two HQ.

Design Selection

Table 4 summarizes the features and requirements as compared in IPSec and DMVPN.

Table 4. Design IPSec/DMVPN

	IPSEC	**DMVPN**
Dynamic Routing	Partial mostly no	Yes
Tunnel Keepalive	N/A	No
HA	Statefull failover	RP
Dynamic Meshing	No	Yes
Branch Dynamic IP addresses	Yes	Yes
IP multicast	No	Yes
Per-Tunnel QOS	No	No

One major advantage of IPSec during selection is that it supports every platform that is Cisco 870, Cisco ISR 1800, and Cisco ISR 3800, Cisco 7200, Cisco 7301, Cisco 7600 and Cisco catalyst 6500. Whereas the DMVPN spoke to spoke does not support Cisco 7600 and Cisco catalyst 6500.

Some other things that needs to be taken care of while choosing a design are:

1. Requirement for IP unicast or IP unicast/ IP multicast.
   If the customer needs just IP unicast i.e. in that case its for branch offices that are relatively small then IPSec will be a good choice. Incase the customer requires IP multicast then DMVPN will be more promising option.

2. Number of Branch offices also affects the choice for VPN technology selection. If the number of branch offices is in hundreds then IPSec is better option but when the number of offices goes near thousand then DMVPN i.e. dynamic VPN is the best option to go with.

3. High availability is also considered as selection criteria for choosing IPSec versus DMVPN. If just 1-2 second state full failover is required then IPSec is a good option to go with but if the failover is more around 20-60 seconds then DMVPN is considered a better choice.

Conclusion

DMVPN requires us to deploy a certification authority server which is deployed only using a single shared key that is not secure enough but the main advantage of choosing DMVPN is that even though it is more hard to deploy but it is easier to maintain and it is usually preferred if the number of remote sites is likely to increase over time. Whereas in IPSec when number of remote sites increases while it is easier to setup but it is harder to maintain as adding a new site requires configuration both on hub and spoke, on the other hand in DMVPN hub configuration doesn't need to be changed because configuration is only required on HUB. So choosing DMVPN would be considered a better option than IPSEC in most cases because it would greatly decrease the configuration on HUB router. We can also have more routers when using DMVPN because routers will have less work with DMVPN as compared to routers using specified tunnels like IPSec. DMVPN also allows the spokes to have dynamic IP's as compared to IPSec tunnel. Having dynamic IP addresses help in future when the spoke router needs to be changed and its IP address is also going to be changed in that case no configuration is required as the new spoke will register to NHS via NHRP as a result the HUB will have dynamic mapping of public to private IPs of the spoke.

Another advantage of choosing DMVPN over IPSec will be that DMVPN would allow us to use dynamic routing instead of using static routing thus reducing a configuration load on routers for static mappings. But DMVPN does not offer security as IPSec does thus making IPSec a popular vpn for branch offices that have POS. But the solution for this problem is to use DMVPN for tunnels and IPSec as encryption method thus eliminating drawbacks of using DMVPN.

References

1. http://www.cisco.com/networkers/nw00/pres/2400.pdf (last checked 12/19/2015)
2. https://en.wikipedia.org/wiki/Generic_Routing_Encapsulation (last checked 12/19/2015)
3. https://supportforums.cisco.com/document/6996/mgre (last checked 12/19/2015)
4. http://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/DMVPN_Overview.pdf (last checked 12/19/2015)
5. https://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008074f22f.pdf (last checked 12/19/2015)
6. http://blog.ine.com/2008/08/02/dmvpn-explained/ (last checked 12/19/2015)
7. http://ieoc.com/forums/t/23485.aspx (last checked 12/19/2015)
8. http://www.webopedia.com/TERM/I/IPsec.html (last checked 12/19/2015)
9. http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/IPSec_Over.html#wp1001296 (last checked 12/19/2015)
10. http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=6(IPSEC) (last checked 12/19/2015)
11. http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14133-ios-hub-spoke.html (last checked 12/19/2015)
12. http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/7912-ios-hub-spoke2.html (last checked 12/19/2015)
13. https://en.wikipedia.org/wiki/IPsec (last checked 12/19/2015)
14. http://www.cisco.com/c/dam/en/us/td/docs/solutions/SBA/August2012/Cisco_SBA_BN_VPNWANDeploymentGuide-Aug2012.pdf (last checked 12/19/2015)
15. http://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/20/ip_security/provisioning/guide/IPsecPG1.html (last checked 12/19/2015)
16. https://vpn-services.bestreviews.net/advantages-and-disadvantages-of-ipsec/ (last checked 12/19/2015)
17. http://flylib.com/books/en/2.650.1.46/1/ (last checked 12/19/2015)
18. https://supportforums.cisco.com/discussion/10777651/dmvpn-vs-gre-ipsec (last checked 12/19/2015)
19. http://www.experts-exchange.com/Hardware/Networking_Hardware/Routers/Q_28486885.html (last checked 12/19/2015)