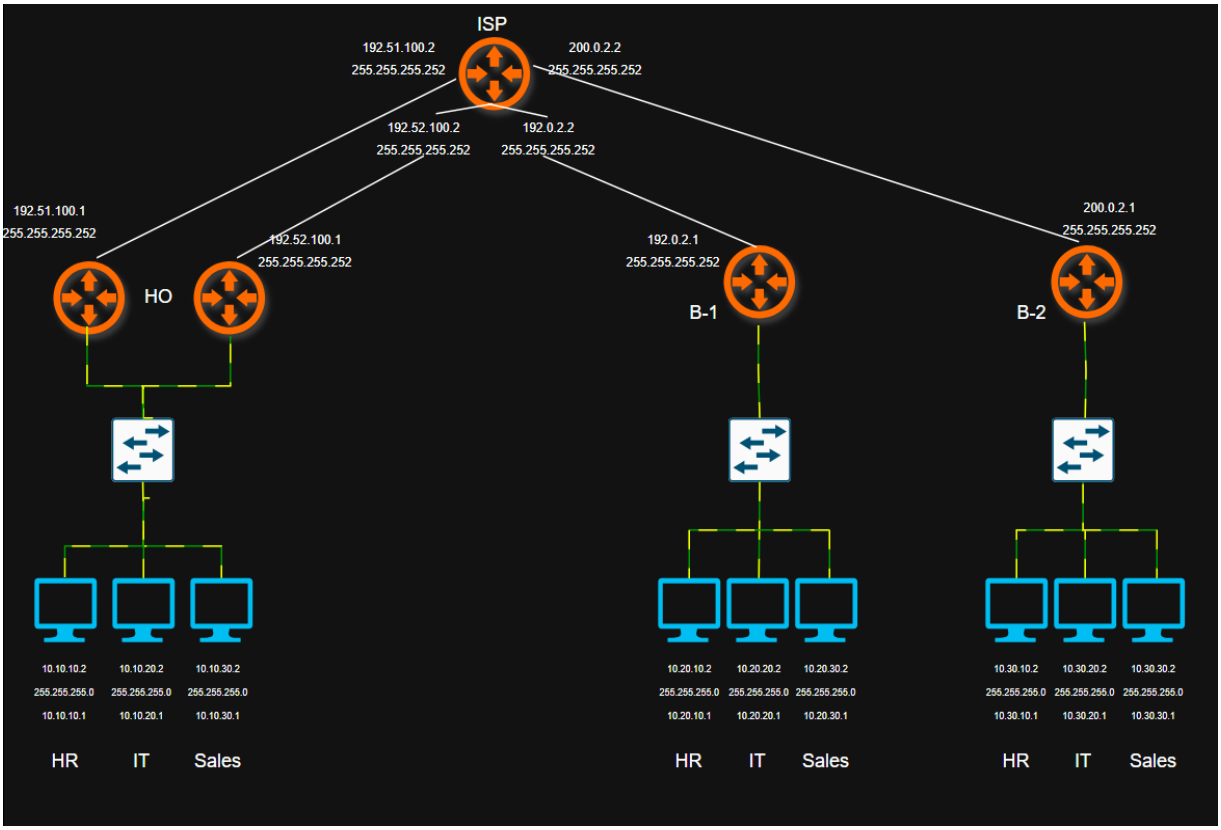
NETWORK ENGINEER PROJECT

PROJECT TITLE:-

“Enterprise Multi-Site Network Simulation using GNS3 with VLAN segmentation, OSPF routing, ACLs, NAT, and GRE over IPsec VPN.”

BY:- PRINSON RODRIGUES

Project Design:-

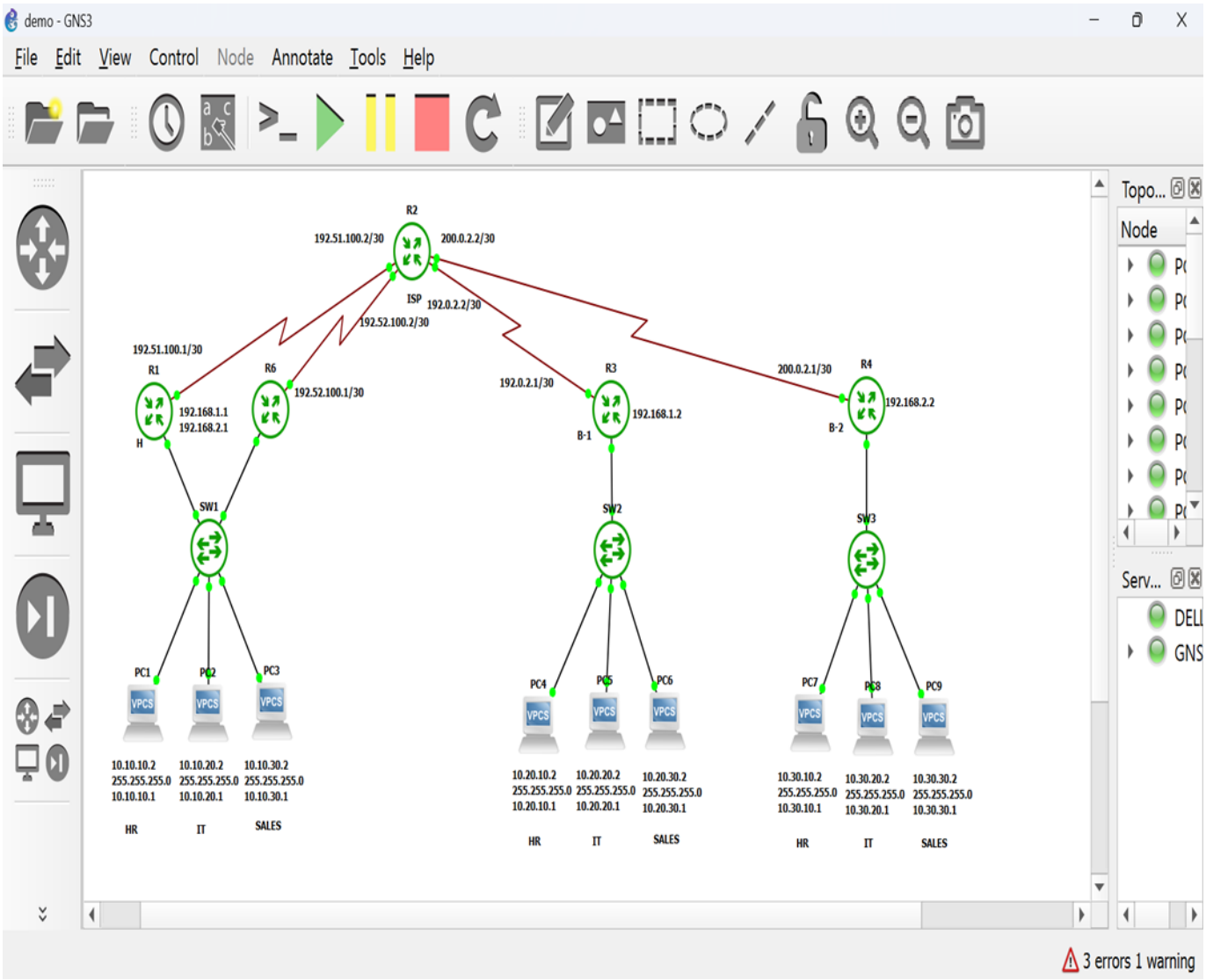


H0 - Head Office

B-1 – Branch 1

B-2 – Branch 2

GNS3 Topology:-



IP Address Plan:-

LAN:-

VLAN	Subnets	Gateways
10	10.10.10.0/24	10.10.10.1
10	10.20.10.0/24	10.20.10.1
10	10.30.10.0/24	10.30.10.1
20	10.10.20.0/24	10.10.20.1
20	10.20.20.0/24	10.20.20.1
20	10.30.20.0/24	10.30.20.1
30	10.10.30.0/24	10.10.30.1
30	10.20.30.0/24	10.20.30.1
30	10.30.30.0/24	10.30.30.1

WAN:-

Device	WAN IP
R1 – R2	192.51.100.0/30
R3 – R2	192.0.2.0/30
R4 – R2	200.0.2.0/30
R6 – R1	192.52.100.0/30

Tunnel:-

Device	Tunnel IP	Tunnel
R1 – R3	192.168.1.0/24	0
R1 – R4	192.168.2.0/24	1
R6 – R3	192.168.3.0/24	2
R6 – R4	192.168.4.0/24	3

Key Configurations:-

Tunnel:-

 # interface Tunnel0

 # ip address 192.168.1.1 255.255.255.0

 # ip ospf network broadcast

 # tunnel source Serial8/0

 # tunnel mode ipsec ipv4

 # tunnel destination 192.0.2.1

 # tunnel protection ipsec profile CR_PR

IPSec:-

 # crypto isakmp policy 10

 # encryption aes

 # authentication pre-share

 # group 5

 # crypto isakmp key cisco123 address 192.0.2.1

 # crypto isakmp key cisco123 address 200.0.2.1

 # crypto ipsec transform-set TR_SET esp-aes

 # mode transport

 # crypto ipsec profile CR_PR

 # set transform-set TR_SET

DHCP:-

 # ip dhcp pool LAN10

 # network 10.10.10.0 255.255.255.0

 # default-router 10.10.10.1

 # ip dhcp pool LAN20

 # network 10.10.20.0 255.255.255.0

 # default-router 10.10.20.1

 # ip dhcp pool LAN30

 # network 10.10.30.0 255.255.255.0

 # default-router 10.10.30.1

ACL:-

 # access-list 1 permit 10.0.0.0 0.255.255.255

 # access-list 110 deny ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255

 # access-list 110 deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255

 # access-list 110 deny ip 10.10.10.0 0.0.0.255 10.30.20.0 0.0.0.255

 # access-list 110 permit ip any any

 # interface Serial8/0

 # ip address 192.51.100.1 255.255.255.252

 # ip access-group 110 in

 # ip nat outside

OSPF:-

 # router ospf 1

 # router-id 192.168.100.1

 # network 10.10.10.0 0.0.0.255 area 0

 # network 10.10.20.0 0.0.0.255 area 0

 # network 10.10.30.0 0.0.0.255 area 0

 # network 192.168.1.0 0.0.0.255 area 0

 # network 192.168.2.0 0.0.0.255 area 0

VLAN and Port Security:-

 # interface Ethernet0/0

 # switchport access vlan 10

 # switchport mode access

 # switchport port-security maximum 5

 # switchport port-security

 # switchport port-security violation restrict

 # switchport port-security mac-address sticky

 # switchport port-security mac-address sticky 0050.7966.6800

Verification Results:-

DHCP:-

```
PC1> ip dhcp
DORA IP 10.10.10.2/24 GW 10.10.10.1

PC1>
```

VLAN 10 and VLAN 30 allowed:-

```
PC4> ping 10.30.10.2

84 bytes from 10.30.10.2 icmp_seq=1 ttl=61 time=142.292 ms
84 bytes from 10.30.10.2 icmp_seq=2 ttl=61 time=127.273 ms
84 bytes from 10.30.10.2 icmp_seq=3 ttl=61 time=126.626 ms
84 bytes from 10.30.10.2 icmp_seq=4 ttl=61 time=127.932 ms
84 bytes from 10.30.10.2 icmp_seq=5 ttl=61 time=126.796 ms

PC4> ping 10.30.30.2

84 bytes from 10.30.30.2 icmp_seq=1 ttl=61 time=126.431 ms
84 bytes from 10.30.30.2 icmp_seq=2 ttl=61 time=127.418 ms
84 bytes from 10.30.30.2 icmp_seq=3 ttl=61 time=127.953 ms
84 bytes from 10.30.30.2 icmp_seq=4 ttl=61 time=126.859 ms
84 bytes from 10.30.30.2 icmp_seq=5 ttl=61 time=126.697 ms
```

Port Security:-

```
SW1#sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
-----------------------------------------------------------------------------
      Et0/0              5           1                  0         Restrict
      Et0/1              5           1                  0         Restrict
      Et0/2              5           1                  0         Restrict
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
SW1#
```

OSPF Neighborship:-

```
R1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
200.0.2.1         1   FULL/DR         00:00:36    192.168.2.2     Tunnel1
192.168.3.2       1   FULL/BDR        00:00:38    192.168.1.2     Tunnel0
192.168.200.1     1   FULL/DR         00:00:39    10.10.30.20     Ethernet0/0.30
192.168.200.1     1   FULL/DR         00:00:34    10.10.20.20     Ethernet0/0.20
192.168.200.1     1   FULL/DR         00:00:36    10.10.10.20     Ethernet0/0.10
R1#
```

NAT Translations:-

```
R1#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 192.51.100.1:1024 10.10.10.2:32036   200.0.2.2:32036    200.0.2.2:1024
icmp 192.51.100.1:1025 10.10.10.2:32292   200.0.2.2:32292    200.0.2.2:1025
icmp 192.51.100.1:1026 10.10.10.2:32548   200.0.2.2:32548    200.0.2.2:1026
icmp 192.51.100.1:1027 10.10.10.2:32804   200.0.2.2:32804    200.0.2.2:1027
icmp 192.51.100.1:1028 10.10.10.2:33060   200.0.2.2:33060    200.0.2.2:1028
R1#
```

Redundancy:-

```
R1#sh glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Et0/0.10    1    -   110 Active   10.10.10.1      local           10.10.10.20
Et0/0.10    1    1   -   Active   0007.b400.0101  local           -
Et0/0.10    1    2   -   Listen   0007.b400.0102  10.10.10.20     -
Et0/0.20    2    -   110 Active   10.10.20.1      local           10.10.20.20
Et0/0.20    2    1   -   Active   0007.b400.0201  local           -
Et0/0.20    2    2   -   Listen   0007.b400.0202  10.10.20.20     -
Et0/0.30    3    -   110 Active   10.10.30.1      local           10.10.30.20
Et0/0.30    3    1   -   Active   0007.b400.0301  local           -
Et0/0.30    3    2   -   Listen   0007.b400.0302  10.10.30.20     -
R1#
```

Access-List:-

```
R1#sh access-lists
Standard IP access list 1
    10 permit 10.0.0.0, wildcard bits 0.255.255.255 (18 matches)
Extended IP access list 110
    10 deny ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255
    20 deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
    30 deny ip 10.10.10.0 0.0.0.255 10.30.20.0 0.0.0.255
    40 permit ip any any (27876 matches)
R1#
```

ISAKMP:-

```
R1#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.51.100.1    192.0.2.1       QM_IDLE           1002 ACTIVE
192.51.100.1    200.0.2.1       QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

IPSec:-

```
R1#sh crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.51.100.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 192.0.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 11082, #pkts encrypt: 11082, #pkts digest: 11082
    #pkts decaps: 6155, #pkts decrypt: 6155, #pkts verify: 6155
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.51.100.1, remote crypto endpt.: 192.0.2.1
     path mtu 1500, ip mtu 1500
     current outbound spi: 0x9A23AA48(2586028616)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xA5B2D4E5(2779960549)
        transform: esp-aes ,
        in use settings ={Tunnel, }
        conn id: 15, flow_id: 15, sibling flags 80000040,  crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (263595912/2890)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
```

Not Permited:-

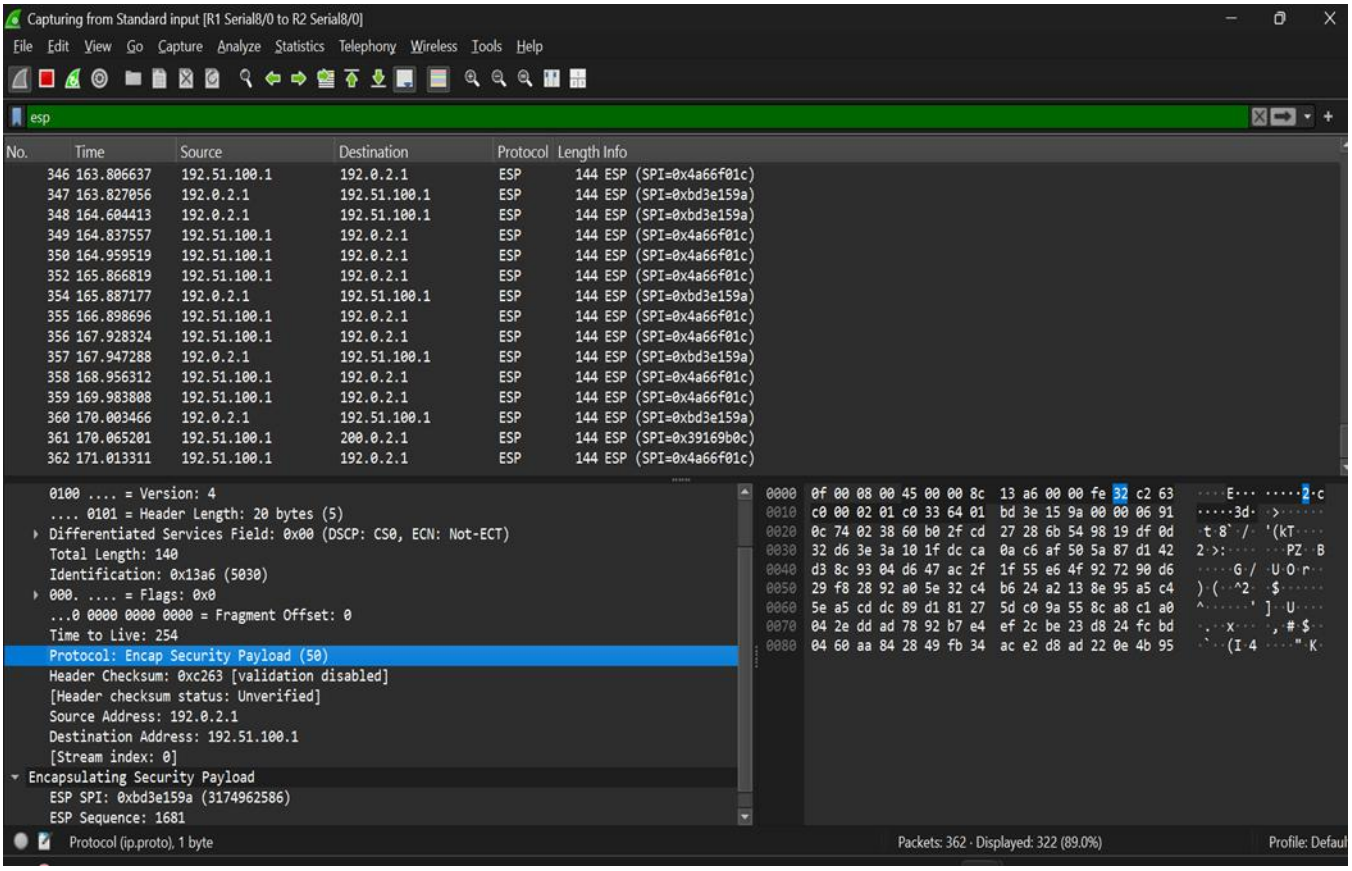
```
PC4> ping 10.20.20.2

*10.20.10.1 icmp_seq=1 ttl=255 time=4.173 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.10.1 icmp_seq=2 ttl=255 time=3.125 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.10.1 icmp_seq=3 ttl=255 time=3.418 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.10.1 icmp_seq=4 ttl=255 time=2.211 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.10.1 icmp_seq=5 ttl=255 time=3.761 ms (ICMP type:3, code:13, Communication administratively prohibited)

PC4>
```

Trobleshooting:-

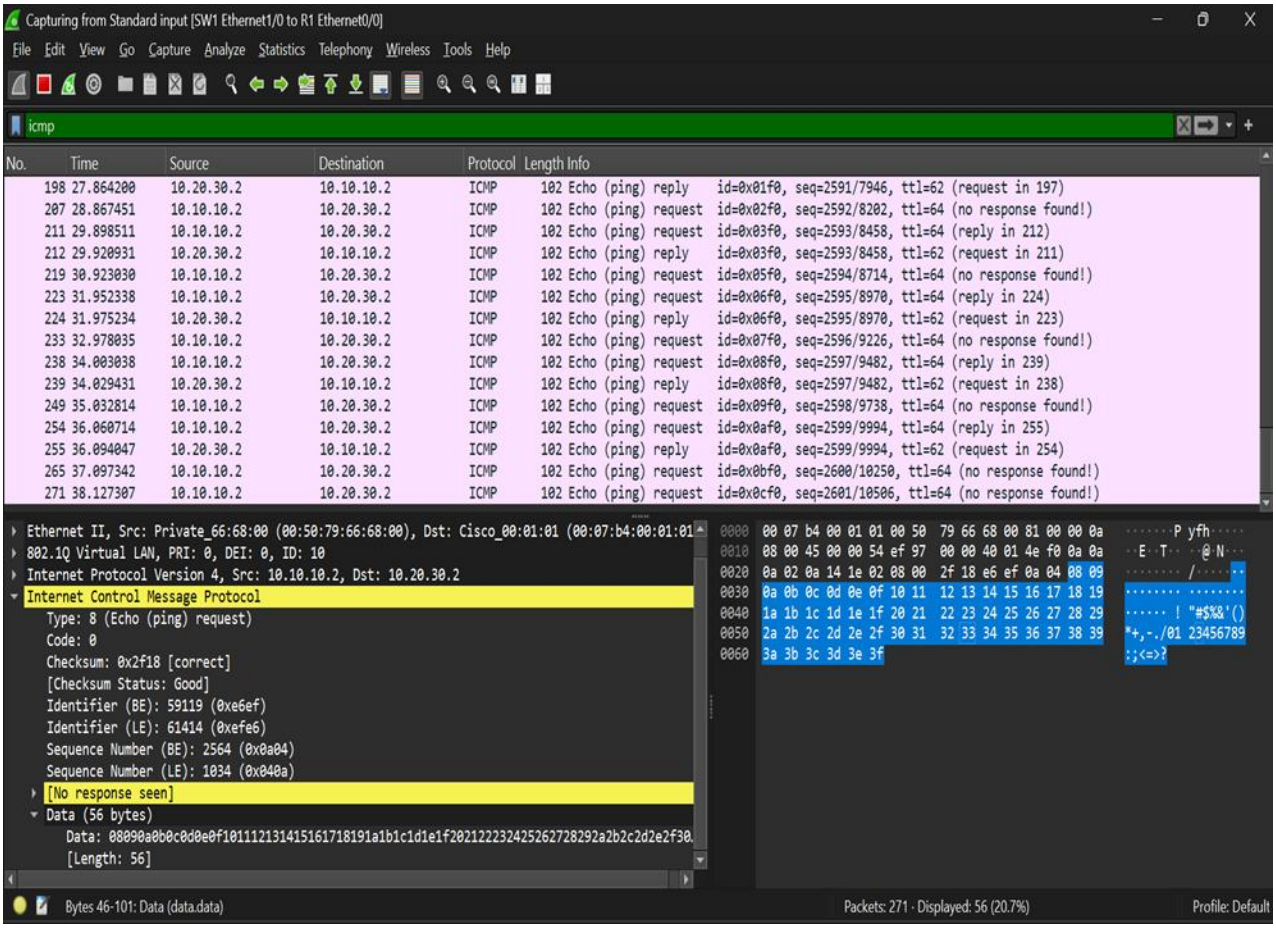
1. Problem:- Tunnel was going up and down for every few seconds. Neighborship was not forming.
   Solution:- Tunnel network mask was wrongly advertised.
2. Problem:- Only VLAN 20 & 30 Internet Access Issue
   Solution:- NAT was not enabled for VLAN 20&30
3. Problem:- Users were not able get IP through DHCP
   Solution:- DHCP snooping was enabled and all the ports were untrusted.

Packet Capture(Wireshark):-

WAN Traffic(Encrypted over Internet):-



LAN Traffic:-


Capturing from Standard input [SW1 Ethernet1/0 to R1 Ethernet0/0]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
198 27.864200 10.20.30.2 10.10.10.2 ICMP 102 Echo (ping) reply id=0x01f0, seq=2591/7946, ttl=62 (request in 197)
207 28.867451 10.10.10.2 10.20.30.2 ICMP 102 Echo (ping) request id=0x02f0, seq=2592/8202, ttl=64 (no response found!)
211 29.898511 10.10.10.2 10.20.30.2 ICMP 102 Echo (ping) request id=0x03f0, seq=2593/8458, ttl=64 (reply in 212)
212 29.920931 10.20.30.2 10.10.10.2 ICMP 102 Echo (ping) reply id=0x03f0, seq=2593/8458, ttl=62 (request in 211)
219 30.923030 10.10.10.2 10.20.30.2 ICMP 102 Echo (ping) request id=0x05f0, seq=2594/8714, ttl=64 (no response found!)
223 31.952338 10.10.10.2 10.20.30.2 ICMP 102 Echo (ping) request id=0x06f0, seq=2595/8970, ttl=64 (reply in 224)
224 31.975234 10.20.30.2 10.10.10.2 ICMP 102 Echo (ping) reply id=0x06f0, seq=2595/8970, ttl=62 (request in 223)
233 32.978035 10.10.10.2 10.20.30.2 ICMP 102 Echo (ping) request id=0x07f0, seq=2596/9226, ttl=64 (no response found!)
238 34.003038 10.10.10.2 10.20.30.2 ICMP 102 Echo (ping) request id=0x08f0, seq=2597/9482, ttl=64 (reply in 239)
239 34.029431 10.20.30.2 10.10.10.2 ICMP 102 Echo (ping) reply id=0x08f0, seq=2597/9482, ttl=62 (request in 238)
249 35.032814 10.10.10.2 10.20.30.2 ICMP 102 Echo (ping) request id=0x09f0, seq=2598/9738, ttl=64 (no response found!)
254 36.060714 10.10.10.2 10.20.30.2 ICMP 102 Echo (ping) request id=0x0af0, seq=2599/9994, ttl=64 (reply in 255)
255 36.094047 10.20.30.2 10.10.10.2 ICMP 102 Echo (ping) reply id=0x0af0, seq=2599/9994, ttl=62 (request in 254)
265 37.097342 10.10.10.2 10.20.30.2 ICMP 102 Echo (ping) request id=0x0bf0, seq=2600/10250, ttl=64 (no response found!)
271 38.127307 10.10.10.2 10.20.30.2 ICMP 102 Echo (ping) request id=0x0cf0, seq=2601/10506, ttl=64 (no response found!)
Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Cisco_00:01:01 (00:07:b4:00:01:01)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 10
Internet Protocol Version 4, Src: 10.10.10.2, Dst: 10.20.30.2
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x2f18 [correct]
[Checksum Status: Good]
Identifier (BE): 59119 (0xe6ef)
Identifier (LE): 61414 (0xefe6)
Sequence Number (BE): 2564 (0x0a04)
Sequence Number (LE): 1034 (0x040a)
[No response seen]
Data (56 bytes)
Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f30
[Length: 56]
0000 00 07 b4 00 01 01 00 50 79 66 68 00 81 00 00 0a
0010 08 00 45 00 00 54 ef 97 00 00 40 01 4e f0 0a 0a
0020 0a 02 0a 14 1e 02 08 00 2f 18 e6 ef 0a 04 08 09
0030 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19
0040 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29
0050 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39
0060 3a 3b 3c 3d 3e 3f
Bytes 46-101: Data (data.data)
Packets: 271 · Displayed: 56 (20.7%)
Profile: Default