*** Individual Case Study ***

ESP No: TNE20002_A01_T013

Thanh Nguyen 101607169 Thursday 11:30 ATC329 TNE20002

Please indicate status: Repeating

Specification Information

- Specification Number : 2.2
- Class A Internal network address : 67.32.0.0/19
- Class B NAT pool public address : 147.2.0.0/21
- Class C ISP network connection address: 207.2.2.0/30
- Class B ISP Internet Web server address: 147.17.2.0/30
- Wireless Deployment Site : Narpala
- Management VLAN Number : 33
- Percentage Growth (VLSM) : 30
- Who provided specification ? : Peter Granville

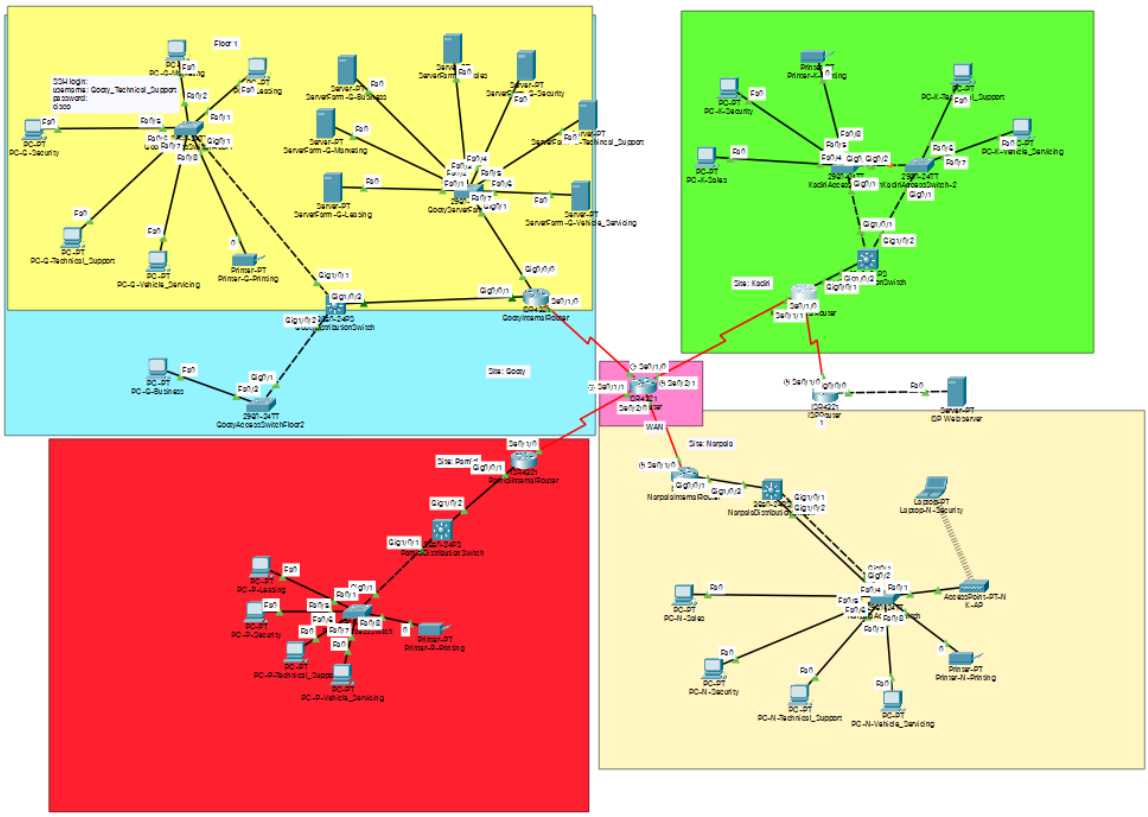
Contents

Section A: Specifications:

Address:

- Class A Internal network address : 67.32.0.0/19
- Class B NAT pool public address : 147.2.0.0/21
- Class C ISP network connection address: 207.2.2.0/30
- Class B ISP Internet Web server address: 147.17.2.0/30

Network Topology



Section B: Discussion of Network Design and Issues

IP VLSM Design:

The case study requires to take account the current amount staff in each department and account for the future growth in the five years. Variable-Length Subnet Masking (VLSM) allows to plan and maximise addresses. Table A shows all information network address and number of host addresses required. The number of server farm was decided based on number of VLAN in the company. The company didn't specify the number of hosts required for Management VLAN, Server Farm VLAN, Printer VLAN therefore, the number of hosts has been assigned to each VLAN above. The number of host addresses have been also accounted for future growth of 30% except for Management VLAN, Server Farm VLAN, Printer VLAN and serial links. The reason behind this decision because number of hosts was assigned by the designer not by the company which doesn't show proper user growth.

Routing Protocols:

The company decided to use OSPF (Open Shortest Path First) as its routing protocols. Since this network is designed to be in a WAN (Wide Area Network), there will a carrier router to route data between other company sites. Since this carrier router is not part of any company sites, it is not safe route through this router. OPSF MD5 authentication should be assigned to on the link between the company sites and the carrier router. For the prototype, MD 5 authentication was only assigned on the links of Gooty and Kadiri routers to towards the carrier router. Another issue with the OSPF implementation is the stability of it. Router ID has assigned to each router, but router ID uses the highest IP address on an active interface used by default. When those active interfaces go down, OSPF process crashes which cause connectivity in the network. To resolve this issue, a loopback interface should create as the loopback interface doesn't turn off normally. This implementation can be seen on prototype on "WANRouter". Non-routing interfaces within the network were set to passive to prevent unnecessary routing information being sent to the local networks. A default route was assigned to Kadiri router for accessibility to the ISP.

Switches: VLANs, STP, EtherChannel:

The switches in the prototype had set up to be in a Two-Tier Model which contains access switches and distribution switches. Access switches can create VLAN for the device on network in the different department and provide port security. Distribution switches help to bridge connection between the access switches and router via the subnets and VLANS. This model allows to have VLANs at different floor to be connected to the whole site. The specified VLANs are created at their respective company sites and the ports configured to be only accessible by those VLANs. All other ports that not used should be turned off for security purposes. Management VLAN should be configured to VLAN 33 based on the company requirement. Using a different Management VLAN number other than 1 allow to separate control traffic data and management purpose to improve security.

Spanning Tree Protocol (STP) and EtherChannel were implement at certain company sites based on company requirements. However, this implementation should be applied to all sites because it provides redundancy. STP prevent loops in the networks by learning where to forward packet to and block packets from. EtherChannel provides redundancy and better throughput. If one of physical link in the EtherChannel goes down, the connectivity still exists. Ethernet Channel are configured to be Link Aggregation Control Protocol (LACP) for dynamic configuration. These implementations will make the network very dynamic if one of the links in the network fails.

Wireless LANs and Site Layout for the specified site:

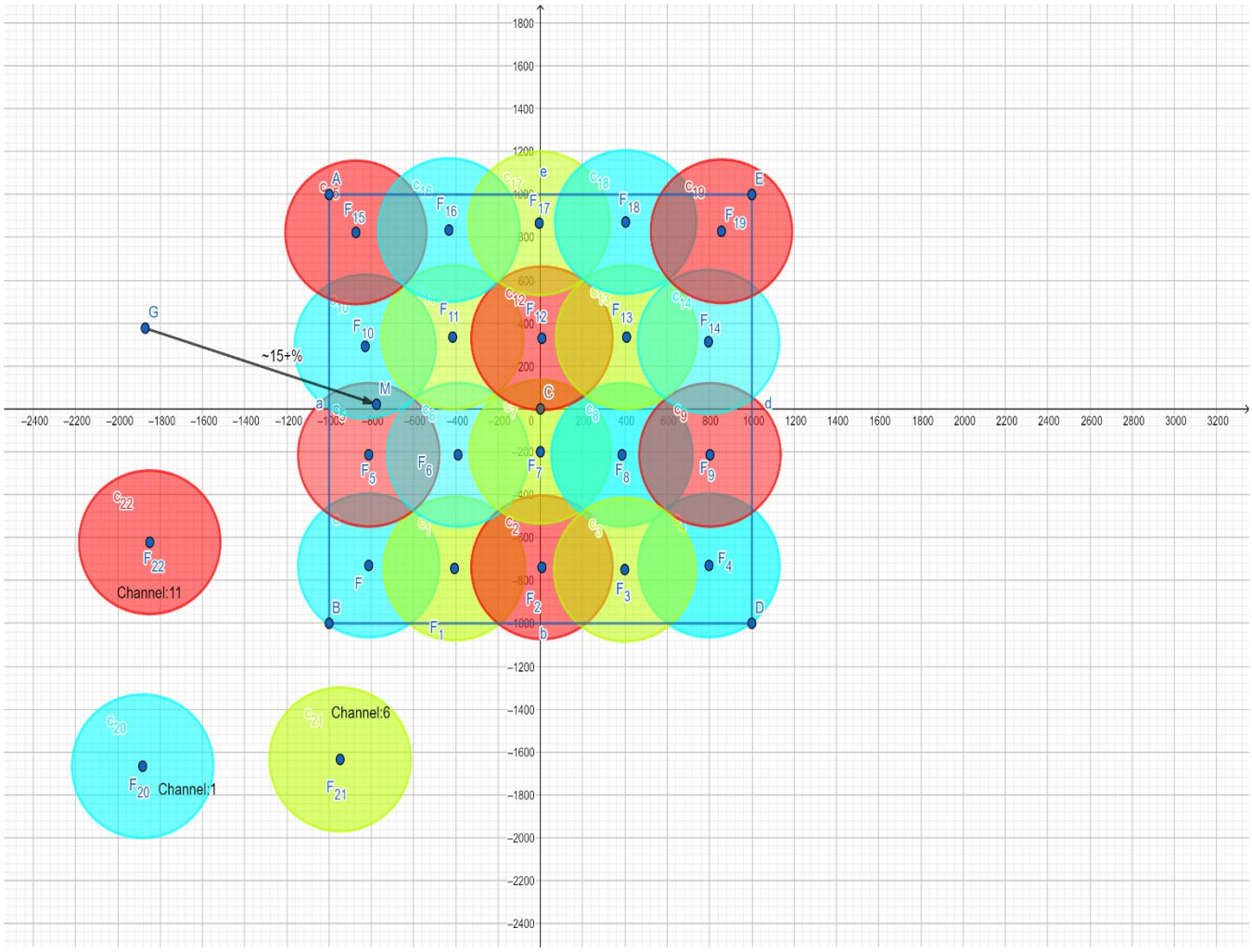


Figure 1:Deployment of Wireless Access Points

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/1570-DG/b_Aironet_AP1570_DG.html

The access point model that is used for deployment is the CISCO Aironet 1570 which is an outdoor access point. Based on the company site's specification, there is only one building and the wireless coverage needs to cover whole site. An outdoor access point will provide weather better protection if the wireless access point can't be placed indoors. For deployment, 2.4GHz is used for better range coverage. To determine the range, Aironet 1570 Deployment Guide reveals that for high throughput for 2.4GHz is 335m if the antenna -A is used. To calculate the minimum number of access points, the area of the site and area of wireless coverage of Aironet 1570 needs to be determined. Since the wireless coverage area is a circular shape, the area that is calculate will have flexible shape because calculation doesn't account shape. Within the calculation of the area of the wireless coverage, 15% of the area is removed to achieve ESS due to overlap. ESS allows the user roam between access points without changing SSID.

Calculation minimum number of access point:

Narpala's Site Size: 2,000m X 2,000m

Narpala's Area: 2,000 *2,000 = 4,000,000m^2

Wireless Radius: 335m

Wireless Area with 15% overlap: (100% – 15%)*Pi * r^2 = ~299680.45m^2

Calculation minimum number of access point: Narpala's Area/ Wireless Area with 15% overlap

4,000,000/299680.45= 13.347

Rounding up= 14 minimum number of access point.

Actual Deployment:

14 access points were place in simulation of the Narpala site. However due to area of wireless area doesn't account shape, the deployment needs more access points than expected. After implementing more access points to cover the sites, 20 access points are required for full coverage.

In Figure 1, each wireless point is configured channel 1, 6, 11 to prevent overlap interface which may cause connection disruption. However, in this deployment, no same channel cell might happen due limited non-overlapping channels. To solve this issue 5GHz will have 24 non-overlapping channels in exchange for less wireless range with more access points required but easier deployment to avoid same channel cells.

DHCP:

Dynamic Host Configuration Protocol (DHCP) was configured on Pamidi site. DHCP should be used because company has large number of staffs and to configure each those staff a static IP is tiresome. Static IP assignment will introduce duplicate IP address errors. With that reasoning, DHCP should be deployed in every site for the network to be robust and scalable. This reasoning also aligns the company's expect growth. The DHCP is configured on Pamidi router but this a bad configuration. This is a bad design because router will be at a single point of failure therefore no DHCP available for the network if router is removed. A solution to this issue configures the distribution switch with DHCP relay and connect to a DHCP server. The DHCP server will perform all DHCP actions. This is better for troubleshooting as DHCP servers provide logs to manage their IP address. DHCP servers can provide redundancy and high availability because if DHCP server shut down, the host keep their current IP addresses.

NAT:

Network Address Translation (NAT) conserve public IPv4 addresses and allows networks to use private IP address to be translated into public IP addresses. The benefit of Nat is to provide privacy and security to a network because it hides internal IPv4 addresses from outside networks NAT is implemented on Kadiri router since it is acting gateway toward the ISP router and other internal networks. The NAT Pool IP address was provided by case study. The network has static NATs because the Server Farms have a constant address that is accessible. This consumes some of NAT Pool IPs. The remaining NAT Pool IPs is divided by number of VLAN on numbers for dynamic NAT. For this network, the NAT Pool divide 9 for 9 different NAT Pool for each VLAN for full usage NAT Pool IP address. To ensure that VLAN have access to their own NAT Pool, ACLS (Access Control Lists) is used restrict access for other VLANs. Due to nature of Dynamic NAT, IP address are consumed quickly to fix PAT is required. Port address Translation (PAT) allows multiple private IP addresses to a single public IP address. To achieve this, every binding statement (ACL binds to the respective NAT Pool) will be overload.

Security and Access Control Policies:

The network uses various type of security technique to prevent malicious activities from occurring.

PPP CHAP

PPP & CHAP validate the identity of remote clients. CHAP provide protection against playback attacks. PPP CHAP is deployed on the links between gateway router and ISP. This allows only authorised users to access the network.

Port Security

Port Security allow only a specified number of source MAC addresses to be connected to a specific port. Port Security is deployed on Pamidi sites. Port Security is configured on the access switch which will permit traffic from known MAC addresses to continue sending traffic while dropping traffic from unknown MAC addresses by using the violation restrict. This network should have Port Security on every access switch to prevent unauthorised users.

SSH

SSH connection is used to give access to Technical Support group. SSH is safer to use than Telnet because it provides public-key encryption for authentication. This access will require a password, username and hides data. The SSH connection is deployed in Gooty site. A SSH connection will be required all sites if requiring access to a device on a network.

Local router password

Although the company requirement didn't specify configure a local password on the devices, it is recommended to assign one. This prevents any unauthorised local users from accessing and modifying the devices.

Access Control List (ACL)

ACL is a traffic filter which provides better security and network performance. ACL's security provide traffic flow control and restrict access on VLANs. Other than ACL that was deployed for NAT at Kadiri site, ACL was deployed at Gooty. When adopting ACL on Gooty, the following criteria should be considered:

1. Hosts on PC at Gooty need to be part of ACLs.

2. Any external host paths through Gooty's Internal Router need to be part of ACLs.

For example, one of the company requirements states "PC host in all other VLAN are denied to Technical Support VLAN". Based on the stated criteria above, the company requirement required the ACL to do two things.

1. PC Host on all VLAN other than Technical Support at Gooty should not have access to Technical Support at other sites.
2. PC Host on all VLAN other than Technical Support at all sites except for Gooty should not have access Technical Support at Gooty.

Therefore, an extended ACL will help control what IP address to deny access Technical Support while allowing Technical Support access itself at other sites.

System Testing and Verification Strategy:

System Testing involves checking end to end device for connectivity or denied access depend how the network is configured. Verification strategies narrow of the scope of an issue in the network. requires pinging end device in the network. Pinging end device will determine successful if the result match with expected results.

Example: Ping PC-G Security to PC- K – Security:

```
C:\>ping 67.32.7.50

Pinging 67.32.7.50 with 32 bytes of data:

Reply from 67.32.7.50: bytes=32 time=3ms TTL=125
Reply from 67.32.7.50: bytes=32 time=4ms TTL=125
Reply from 67.32.7.50: bytes=32 time=3ms TTL=125
Reply from 67.32.7.50: bytes=32 time=3ms TTL=125

Ping statistics for 67.32.7.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

This is a successful ping because a proper IP address and gateway IP was configured correctly. Check the right IP address and gateway IP to right device assign properly.

OSPF:

If a router can't ping to other router in a OSPF settings, check routers have formed an adjacency with each other, use - **show ip ospf neighbor**

Example of -show ip ospf neightbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
67.32.8.1	0	FULL/ -	00:00:37	67.32.7.225	Serial0/1/0
67.32.8.9	0	FULL/ -	00:00:37	67.32.8.9	Serial0/2/0
67.32.8.13	0	FULL/ -	00:00:37	67.32.8.13	Serial0/1/1
207.2.2.1	0	FULL/ -	00:00:37	67.32.8.5	Serial0/2/1

If all neighbour ID appear to correct and is full, most likely adjacency is formed.

"sh ip route"

If the OSPF is correct and yet no connection found is followed use **show ip route** to display the routing table on each router to check for:

- Check all the subnets are present
- Check there is a default route

Example of -show ip route:

```
C       67.32.7.64/28 is directly connected, GigabitEthernet0/0/1.60
L       67.32.7.65/32 is directly connected, GigabitEthernet0/0/1.60
C       67.32.7.80/28 is directly connected, GigabitEthernet0/0/1.70
L       67.32.7.81/32 is directly connected, GigabitEthernet0/0/1.70
O       67.32.7.96/28 [110/781] via 67.32.8.6, 00:13:19, Serial0/1/0
O       67.32.7.112/28 [110/781] via 67.32.8.6, 00:13:19, Serial0/1/0
O       67.32.7.128/28 [110/781] via 67.32.8.6, 00:13:19, Serial0/1/0
O       67.32.7.144/28 [110/781] via 67.32.8.6, 00:13:19, Serial0/1/0
O       67.32.7.160/28 [110/781] via 67.32.8.6, 00:13:19, Serial0/1/0
O       67.32.7.176/28 [110/781] via 67.32.8.6, 00:13:19, Serial0/1/0
O       67.32.7.192/29 [110/781] via 67.32.8.6, 00:13:19, Serial0/1/0
C       67.32.7.200/29 is directly connected, GigabitEthernet0/0/1.80
L       67.32.7.201/32 is directly connected, GigabitEthernet0/0/1.80
O       67.32.7.208/29 [110/781] via 67.32.8.6, 00:13:19, Serial0/1/0
O       67.32.7.216/29 [110/781] via 67.32.8.6, 00:13:19, Serial0/1/0
O       67.32.7.224/30 [110/780] via 67.32.8.6, 00:13:29, Serial0/1/0
O       67.32.7.228/30 [110/781] via 67.32.8.6, 00:13:19, Serial0/1/0
O       67.32.7.232/30 [110/781] via 67.32.8.6, 00:13:19, Serial0/1/0
O       67.32.7.236/30 [110/781] via 67.32.8.6, 00:13:19, Serial0/1/0
O       67.32.7.240/30 [110/781] via 67.32.8.6, 00:13:19, Serial0/1/0
O       67.32.7.244/30 [110/781] via 67.32.8.6, 00:13:19, Serial0/1/0
O       67.32.7.248/30 [110/781] via 67.32.8.6, 00:13:19, Serial0/1/0
O       67.32.7.252/30 [110/781] via 67.32.8.6, 00:13:19, Serial0/1/0
O       67.32.8.0/30 [110/781] via 67.32.8.6, 00:13:19, Serial0/1/0
C       67.32.8.4/30 is directly connected, Serial0/1/0
L       67.32.8.5/32 is directly connected, Serial0/1/0
O       67.32.8.8/30 [110/780] via 67.32.8.6, 00:13:29, Serial0/1/0
O       67.32.8.12/30 [110/780] via 67.32.8.6, 00:13:29, Serial0/1/0
     207.2.2.0/24 is variably subnetted, 3 subnets, 2 masks
C       207.2.2.0/30 is directly connected, Serial0/1/1
L       207.2.2.1/32 is directly connected, Serial0/1/1
C       207.2.2.2/32 is directly connected, Serial0/1/1
S*   0.0.0.0/0 is directly connected, Serial0/1/1
```

In this image, you can see a default route is configured and look like all the subnets are present. Although may look right, checking if routing protocol is not advertising a subnet, interface maybe down or incorrect subnetting will be required to check manually.

NAT Transaction

To check if the NAT is working if the private address converted a public address. After enabling all the debugging tools, ping hosts to ISP Web server.

a) Use **debug ip nat** on Kadiri router to watch NAT translations

```
NAT: s=67.32.7.2->147.2.4.109, d=147.17.2.2 [9]

NAT: s=67.32.7.2->147.2.4.109, d=147.17.2.2 [10]

NAT*: s=147.17.2.2, d=147.2.4.109->67.32.7.2 [1]

NAT: s=67.32.7.2->147.2.4.109, d=147.17.2.2 [11]

NAT*: s=147.17.2.2, d=147.2.4.109->67.32.7.2 [2]

NAT: s=67.32.7.2->147.2.4.109, d=147.17.2.2 [12]

NAT*: s=147.17.2.2, d=147.2.4.109->67.32.7.2 [3]
```

This image shows how the private address to converted to the public address. This information check if private address matches to assigned NAT Pool

b) Use **debug ip icmp** on ISP router to check ping request arrives

```
ICMP: time exceeded (time to live) send to 147.2.4.109 (dest was 147.2.4.108)

ICMP: time exceeded (time to live) send to 147.2.4.109 (dest was 147.2.4.108)

ICMP: time exceeded (time to live) send to 147.2.4.109 (dest was 147.2.4.108)

ICMP: time exceeded (time to live) send to 147.2.4.109 (dest was 147.2.4.108)
```

This show that ping did arrive at the ISP route.

c) **show ip nat translations**

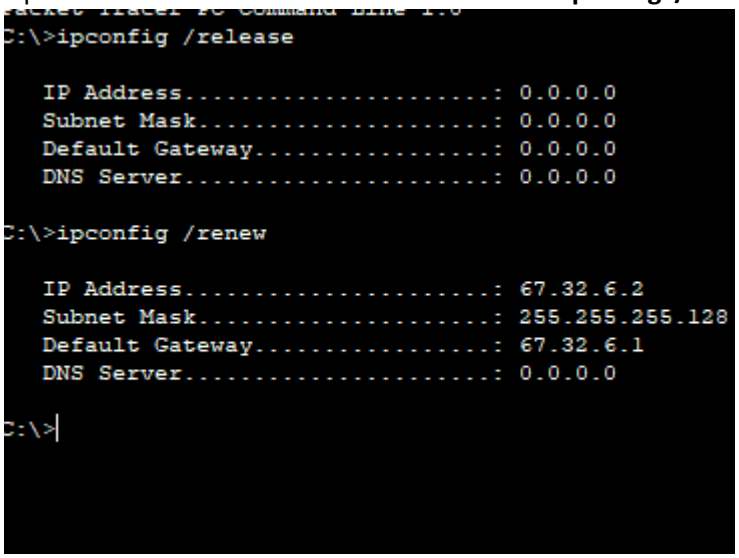
```
sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 147.2.4.109:17    67.32.7.2:17       147.2.4.108:17     147.2.4.108:17
---  147.2.7.249       67.32.7.234        ---                ---
---  147.2.7.250       67.32.8.2          ---                ---
```

This Nat translation show if translation has happened but also if the NAT Overload works by check if the IP address are assigned with a port number.

DHCP

To check if DHCP is automatically assigning IP to end device

a) Open DOS CMD window on PC at Pamidi site – **ipconfig /release** then **ipconfig /renew**



If address not obtained, to check configuration are right

– **show ip dhcp pool**, **show ip dhcp binding, show run**

```
Pool poolVLAN10 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 126
 Leased addresses               : 1
 Excluded addresses             : 5
 Pending event                  : none
```

Figure 2: show ip dhcp pool

```
PamidiInternalRouter#sh ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
67.32.6.2        0009.7C13.DA2A          --                      Automatic
67.32.7.146      0090.0C06.D97C          --                      Automatic
67.32.7.162      00D0.BC7E.ED57          --                      Automatic
67.32.7.178      000A.F3C3.0E4E          --                      Automatic
67.32.7.218      000A.F376.2DD0          --                      Automatic
```

Figure 3 show ip dhcp binding

ACL

To check if end devices are following ACL rules as intended:

1. **Use show access-lists**

```
Extended IP access list ACLVLAN60SF
    10 permit ip 67.32.7.248 0.0.0.3 67.32.7.16 0.0.0.15
    20 permit ip 67.32.7.248 0.0.0.3 67.32.7.160 0.0.0.15
    30 permit ip 67.32.7.248 0.0.0.3 67.32.7.112 0.0.0.15
    40 permit ip 67.32.7.248 0.0.0.3 67.32.7.64 0.0.0.15
    50 permit ip 67.32.7.248 0.0.0.3 147.17.2.0 0.0.0.3
    60 deny ip any any
Extended IP access list ACLVLAN70SF
    10 permit ip 67.32.7.252 0.0.0.3 67.32.7.32 0.0.0.15
    20 permit ip 67.32.7.252 0.0.0.3 67.32.7.176 0.0.0.15
    30 permit ip 67.32.7.252 0.0.0.3 67.32.7.128 0.0.0.15
    40 permit ip 67.32.7.252 0.0.0.3 67.32.7.80 0.0.0.15
    50 permit ip 67.32.7.252 0.0.0.3 147.17.2.0 0.0.0.3
    60 deny ip any any
```

2. Use clear access-list counters

Remove previous testing results.

3. Go to PC in intend VLAN for the ACL. Then attempt connect to a device (HTTP, ICMP, SSH, etc…)

```
    60 deny ip any any
Extended IP access list ACLVLAN70SF
    10 permit ip 67.32.7.252 0.0.0.3 67.32.7.32 0.0.0.15
    20 permit ip 67.32.7.252 0.0.0.3 67.32.7.176 0.0.0.15
    30 permit ip 67.32.7.252 0.0.0.3 67.32.7.128 0.0.0.15
    40 permit ip 67.32.7.252 0.0.0.3 67.32.7.80 0.0.0.15
    50 permit ip 67.32.7.252 0.0.0.3 147.17.2.0 0.0.0.3 (4 match(es))
    60 deny ip any any
```

One of the ACL rules was a match

Section C:

List information on the prototype that was implemented.

Table A: VLSM Design

Number of host addresses required	Subnet Network Address	Subnet Mask	Subnet Prefix	Max Number of Hosts Possible	Address Space Future Use Y/N	VLAN Name /Serial Links	Site Location
260	67.32.0.0	255.255.254.0	/23	510	Y	Business	Gooty
234	67.32.2.0	255.255.255.0	/24	254	Y	Marketing	Gooty
163	67.32.4.0	255.255.255.0	/24	254	Y	Leasing	Gooty
30	67.32.6.128	255.255.255.224	/27	30	N	Management	Gooty
7	67.32.7.0	255.255.255.240	/28	14	Y	Security	Gooty
7	67.32.7.16	255.255.255.240	/28	14	Y	Technical_ Support	Gooty
7	67.32.7.32	255.255.255.240	/28	14	Y	Vehicle_Servicing	Gooty
3	67.32.7.192	255.255.255.248	/28	6	N	Printing	Gooty
182	67.32.3.0	255.255.255.0	/24	254	Y	Sales	Narpala
30	67.32.6.192	255.255.255.224	/27	30	N	Management	Narpala
7	67.32.7.96	255.255.255.240	/28	14	Y	Security	Narpala
7	67.32.7.112	255.255.255.240	/28	14	Y	Technical_Support	Narpala
7	67.32.7.128	255.255.255.240	/28	14	Y	Vehicle_Servicing	Narpala
3	67.32.7.208	255.255.255.248	/28	6	N	Printing	Narpala
182	67.32.5.0	255.255.255.0	/24	254	Y	Sales	Kadiri
30	67.32.6.160	255.255.255.224	/27	30	N	Management	Kadiri
7	67.32.7.48	255.255.255.240	/28	14	Y	Security	Kadiri
7	67.32.7.64	255.255.255.240	/28	14	Y	Technical_Support	Kadiri
7	67.32.7.80	255.255.255.240	/28	14	Y	Vehicle_Servicing	Kadiri
3	67.32.7.200	255.255.255.248	/28	6	N	Printing	Kadiri

104	**67.32.6.0**	**255.255.255.128**	**/25**	**126**	**Y**	**Leasing**	**Pamidi**
30	**67.32.6.224**	**255.255.255.224**	**/27**	**30**	**N**	**Management**	**Pamidi**
7	**67.32.7.144**	**255.255.255.240**	**/28**	**14**	**Y**	**Security**	**Pamidi**
7	**67.32.7.160**	**255.255.255.240**	**/28**	**14**	**Y**	**Technical_Support**	**Pamidi**
7	**67.32.7.176**	**255.255.255.240**	**/28**	**14**	**Y**	**Vehicle_Servicing**	**Pamidi**
3	**67.32.7.216**	**255.255.255.248**	**/28**	**6**	**N**	**Printing**	**Pamidi**
2	**67.32.7.228**	**255.255.255.252**	**/30**	**2**	**N**	**SF-Business**	**Gooty**
2	**67.32.7.232**	**255.255.255.252**	**/30**	**2**	**N**	**SF-Leasing**	**Gooty**
2	**67.32.7.236**	**255.255.255.252**	**/30**	**2**	**N**	**SF-Management**	**Gooty**
2	**67.32.7.240**	**255.255.255.252**	**/30**	**2**	**N**	**SF-Sales**	**Gooty**
2	**67.32.7.244**	**255.255.255.252**	**/30**	**2**	**N**	**SF-Security**	**Gooty**
2	**67.32.7.248**	**255.255.255.252**	**/30**	**2**	**N**	**SF-Technical_Support**	**Gooty**
2	**67.32.7.252**	**255.255.255.252**	**/30**	**2**	**N**	**SF-Vehicle_Servicing**	**Gooty**
2	**67.32.8.0**	**255.255.255.252**	**/30**	**2**	**N**	**SF-Marketing**	**Gooty**
2	67.32.7.224	**255.255.255.252**	**/30**	**2**	**N**	**Serial Link 1**	
2	67.32.8.4	**255.255.255.252**	**/30**	**2**	**N**	**Serial Link 2**	
2	67.32.8.8	**255.255.255.252**	**/30**	**2**	**N**	**Serial Link 3**	
2	67.32.8.12	**255.255.255.252**	**/30**	**2**	**N**	**Serial Link 4**	

Table B: Switch Details

Name	Model	# of Physical Ports	Location	Management VLAN IP Address	Default Gateway IP Address	Management Vlan
GootyAccessSwitchFloor1	**2960-24TT**	**26**	**Gooty**	67.32.6.131	67.32.6.129	**33**
GootyAccessSwitchFloor2	**2960-24TT**	**26**	**Gooty**	67.32.6.132	67.32.6.129	**33**
GootyDistributionSwitch	**3650-24PS**	**28**	**Gooty**	67.32.6.130	67.32.6.129	**33**
GootyServerFarmSwitch	**2960-24TT**	**26**	**Gooty**	67.32.7.238	67.32.7.237	**33**
PamidiDistributionSwitch	**3650-24PS**	**28**	**Pamidi**	67.32.6.226	67.32.6.225	**33**
PamidiAccessSwitch	**2960-24TT**	**26**	**Pamidi**	67.32.6.227	67.32.6.225	**33**
NarpalaDistributionSwitch	**3650-24PS**	**28**	**Narpala**	67.32.6.194	67.32.6.193	**33**
NarpalaAccessSwitch	**2960-24TT**	**26**	**Narpala**	67.32.6.195	67.32.6.193	**33**
KadiriAccessSwitch-1	**2960-24TT**	**26**	**Kadiri**	67.32.6.163	67.32.6.161	**33**
KadiriAccessSwitch-2	**2960-24TT**	**26**	**Kadiri**	67.32.6.164	67.32.6.161	**33**
Kadiri Distribution	**3650-24PS**	**28**	**Kadiri**	67.32.6.162	67.32.6.161	**33**

Table C.1: Gooty Router Details

Site: c Router Name: GootyInternalRouter

Interface/Sub Interface Type/Number	Description and Purpose	Network/VLAN Name	Network Address	Interface IP address	Subnet Mask /value
G0/0/1.10	**Connection G-Leasing**	**Leasing**	**67.32.0.0**	**67.32.0.1**	**255.255.254.0**
G0/0/1.20	**Connection G-Marketing**	**Marketing**	**67.32.2.0**	**67.32.2.1**	**255.255.255.0**
G0/0/1.30	**Connection G-Business**	**Business**	**67.32.4.0**	**67.32.4.1**	**255.255.255.0**
G0/0/1.33	**Connection G-Management**	**Management**	**67.32.6.128**	**67.32.6.129**	**255.255.255.224**
G0/0/1.50	**Connection G-Security**	**Security**	**67.32.7.0**	**67.32.7.1**	**255.255.255.240**
G0/0/1.60	**Connection G-Technical Support**	**Technical_Support**	**67.32.7.16**	**67.32.7.17**	**255.255.255.240**
G0/0/1.70	**Connection G-Vehicle Servicing**	**Vehicle_Servicing**	**67.32.7.32**	**67.32.7.33**	**255.255.255.240**
G0/0/1.80	**Connection G-Printing**	**Printing**	**67.32.7.192**	**67.32.7.193**	**255.255.255.248**
G0/0/0.10	**Connection G-SF-Leasing**	**SF-Leasing**	**67.32.7.232**	**67.32.7.233**	**255.255.255.252**
G0/0/0.20	**Connection G-SF-Marketing**	**SF-Marketing**	**67.32.8.0**	**67.32.8.1**	**255.255.255.252**
G0/0/0.30	**Connection G-SF-Business**	**SF-Business**	**67.32.7.228**	**67.32.7.229**	**255.255.255.252**
G0/0/0.33	**Connection G-SF-Management**	**SF-Management**	**67.32.7.236**	**67.32.7.237**	**255.255.255.252**
G0/0/0.40	**Connection G-SF-Sales**	**SF-Sales**	**67.32.7.240**	**67.32.7.241**	**255.255.255.252**
G0/0/0.50	**Connection G-SF-Security**	**SF-Security**	**67.32.7.244**	**67.32.7.245**	**255.255.255.252**
G0/0/0.60	**Connection G-SF-Technical Support**	**SF-Technical_Support**	**67.32.7.248**	**67.32.7.249**	**255.255.255.252**
G0/0/0.70	**Connection G-SF-Vehicle Servicing**	**SF-Vehicle_Servicing**	**67.32.7.252**	**67.32.7.253**	**255.255.255.252**
S0/1/0	**Connection to WAN**		67.32.7.224	67.32.7.225	**255.255.255.252**

Table C.2: Pamidi Router Details

Site: Pamidi Router Name: PamidiInternalRouter

Interface/Sub Interface Type/Number	Description and Purpose	Network/VLAN Name	Network Address	Interface IP address	Subnet Mask /value
G0/0/1.10	**Connection P-Leasing**	**Leasing**	**67.32.6.0**	**67.32.6.1**	**255.255.255.128**
G0/0/1.33	**Connection P-Management**	**Management**	**67.32.6.224**	**67.32.6.225**	**255.255.255.224**
G0/0/1.50	**Connection P-Security**	**Security**	**67.32.7.144**	**67.32.7.145**	**255.255.255.240**
G0/0/1.60	**Connection P-Technical Support**	**Technical_Support**	**67.32.7.160**	**67.32.7.161**	**255.255.255.240**
G0/0/1.70	**Connection P-Vehicle Servicing**	**Vehicle_Servicing**	**67.32.7.176**	**67.32.7.177**	**255.255.255.240**
G0/0/1.80	**Connection P-Printing**	**Printing**	**67.32.7.216**	**67.32.7.217**	**255.255.255.248**
S0/1/0	**Connection to** WAN		67.32.8.12	67.32.8.13	**255.255.255.252**

Table C.3: Narpala Router Details

Site: Narpala Router Name: NarpalaInternalRouter

Interface/Sub Interface Type/Number	Description and Purpose	Network/VLAN Name	Network Address	Interface IP address	Subnet Mask /value
G0/0/1.33	**Connection N-Management**	**Management**	**67.32.6.192**	**67.32.6.193**	**255.255.255.224**
G0/0/1.40	**Connection N-Sales**	**Sales**	**67.32.3.0**	**67.32.3.1**	**255.255.255.0**
G0/0/1.50	**Connection N-Security**	**Security**	**67.32.7.96**	**67.32.7.97**	**255.255.255.240**
G0/0/1.60	**Connection N-Technical Support**	**Technical_Support**	**67.32.7.112**	**67.32.7.113**	**255.255.255.240**
G0/0/1.70	**Connection N-Vehicle Servicing**	**Vehicle_Servicing**	**67.32.7.128**	**67.32.7.129**	**255.255.255.240**
G0/0/1.80	**Connection N-** Printing	**Printing**	**67.32.7.208**	**67.32.7.209**	**255.255.255.248**
S0/1/0	**Connection to WAN**		67.32.8.8	67.32.8.9	**255.255.255.252**

Table C.3: Kadiri Router Details

Site: **Kadiri** Router Name: **Kadiri**InternalRouter

Interface/Sub Interface Type/Number	**Description and Purpose**	**Network/VLAN Name**	**Network Address**	**Interface IP address**	**Subnet Mask /value**
G0/0/1.33	**Connection K-Management**	**Management**	**67.32.6.160**	**67.32.6.161**	**255.255.255.224**
G0/0/1.40	**Connection K-Sales**	**Sales**	**67.32.5.0**	**67.32.5.1**	**255.255.255.0**
G0/0/1.50	**Connection K-Security**	**Security**	**67.32.7.48**	**67.32.7.49**	**255.255.255.240**
G0/0/1.60	**Connection K-Technical Support**	**Technical_Support**	**67.32.7.64**	**67.32.7.65**	**255.255.255.240**
G0/0/1.70	**Connection K-Vehicle Servicing**	**Vehicle_Servicing**	**67.32.7.80**	**67.32.7.81**	**255.255.255.240**
G0/0/1.80	**Connection K-Printing**	**Printing**	**67.32.7.200**	**67.32.7.201**	**255.255.255.248**
S0/1/0	**Connection to WAN**		67.32.8.4	67.32.8.5	**255.255.255.252**
S0/1/1	**Connection to ISP**	**ISP**	207.2.2.0	207.2.2.1	**255.255.255.252**

Table D: Pamidi DHCP Server Pool IP Host Addresses

VLAN Name	**IP Address Pool Range**	**Subnet mask** /value	**Default Gateway** IP Address
Leasing	67.32.6.0 - 67.32.6.127	**255.255.255.128**	67.32.6.1
Security	67.32.7.144 - 67.32.7.159	**255.255.255.240**	67.32.7.145
Technical_Support	67.32.7.160 - 67.32.7.175	**255.255.255.240**	67.32.7.161
Vehicle_Servicing	67.32.7.176 - 67.32.7.191	**255.255.255.240**	67.32.7.177
Printing	67.32.7.216 - 67.32.7.223	**255.255.255.248**	67.32.7.217

Table E: Statically assigned IP Host Addresses – Servers, Printers etc

End Devices Name	In which VLAN	IP Address	Subnet Mask /Value	Default Gateway IP Address	Service/s Provided
PC-G-Leasing	10	67.32.0.2	255.255.254.0	67.32.0.1	End-User
PC-G-Marketing	20	67.32.2.2	255.255.255.0	67.32.2.1	End-User
PC-G-Business	30	67.32.4.2	255.255.255.0	67.32.4.1	End-User
PC-G-Security	50	67.32.7.2	255.255.255.240	67.32.7.1	End-User
PC-G-Technical_Support	60	67.32.7.18	255.255.255.240	67.32.7.17	End-User
PC-G-Vehicle_Support	70	67.32.7.34	255.255.255.240	67.32.7.33	End-User
Printer-G-Printing	80	67.32.7.194	255.255.255.248	67.32.7.193	Printing Service
PC-N-Sales	40	67.32.3.2	255.255.255.0	67.32.3.1	End-User
PC-N-Security	50	67.32.7.98	255.255.255.240	67.32.7.97	End-User
PC-N-Technical_Support	60	67.32.7.114	255.255.255.240	67.32.7.113	End-User
PC-N-Vehicle_Support	70	67.32.7.130	255.255.255.240	67.32.7.129	End-User
Printer-N-Printing	80	67.32.7.210	255.255.255.248	67.32.7.209	Printing Service
Laptop-N-Security	50	67.32.7.99	255.255.255.240	67.32.7.97	End-User
PC-K-Sales	40	67.32.5.2	255.255.255.0	67.32.5.1	End-User
PC-K-Security	50	67.32.7.50	255.255.255.240	67.32.7.49	End-User
PC-K-Technical_Support	60	67.32.7.66	255.255.255.240	67.32.7.65	End-User
PC-K-Vehicle_Support	70	67.32.7.82	255.255.255.240	67.32.7.81	End-User
Printer-K-Printing	80	67.32.7.202	255.255.255.248	67.32.7.201	Printing Service
ISP Web server	-	147.17.2.2	255.255.255.252	147.17.2.1	Hosting web server
ServerFarm-G-Leasing	10	67.32.7.234	255.255.255.252	67.32.7.233	Hosting web server
ServerFarm - G-Marketing	20	67.32.8.2	255.255.255.252	67.32.8.1	Hosting web server

ServerFarm - G-Business	**30**	**67.32.7.230**	**255.255.255.252**	**67.32.7.229**	**Hosting web server**
ServerFarm - G-Sales	**40**	**67.32.7.242**	**255.255.255.252**	**67.32.7.241**	**Hosting web server**
ServerFarm - G-Security	**50**	**67.32.7.246**	**255.255.255.252**	**67.32.7.245**	**Hosting web server**
ServerFarm - G-Technical_Support	**60**	**67.32.7.250**	**255.255.255.252**	**67.32.7.249**	**Hosting web server**
ServerFarm G-Vehicle_ Support	**70**	**67.32.7.254**	**255.255.255.252**	**67.32.7.253**	**Hosting web server**

Table F: Wireless Access Point Details

Name	Model	SSID	Channel 2.4GHz	Channel 5GHz
K-AP	**AccessPoint -PT-N**	**101607169**	**1**	**36**

Table G: Record of ACL Testing

Source Host	Destination Host/Server	Protocol	Expected Result Permitted/Denied	Achieved Yes/No
Host on ALL VLAN	Internet Web Server	**IP**	**PERMITTED**	**YES**
Host ALL VLAN in all sites Unless specificized denied below	**Host ALL VLAN in all sites Unless specificized denied below**	**IP**	**Permitted**	**Yes**
Host on Marketing in Gooty	Host on Leasing in Gooty and Pamidi	**IP**	**Denied**	**YES**
Host on Leasing	ServerFarm-G-Leasing	**IP**	**PERMITTED**	**YES**
Host on Marketing	ServerFarm-G-**Marketing**	**IP**	**PERMITTED**	**YES**
Host on Business	ServerFarm-G-**Business**	**IP**	**PERMITTED**	**YES**
Host on Sales	ServerFarm-G-**Sales**	**IP**	**PERMITTED**	**YES**
Host on Security	ServerFarm-G-**Security**	**IP**	**PERMITTED**	**YES**
Host on Techincal_Support	ServerFarm-G-**Techincal_Support**	**IP**	**PERMITTED**	**YES**
Host on Vehicle_Servicing	ServerFarm-G-Leasing-**Vehicle_Servicing**	**IP**	**PERMITTED**	**YES**
Host on Vehicle_Service in Gooty	Host of All VLAN other than Vehicle_Service Outside of Gooty	**IP**	**Denied**	**Yes**
Host on Vehicle_Service in other sites except Gooty	Host of ALL VLAN other than Vehicle_Service in Gooty	**IP**	**Denied**	**Yes**
Host on ALL VLAN other than Techincal Support in Outside of Gooty	Host on Techincal_Support in Gooty	**IP**	**Denied**	**Yes**
Host on ALL VLAN other than Techincal Support in Gooty	Host & Server on Techincal_Support outside of Gooty	**IP**	**Denied**	**Yes**
Host on VLAN Techincal Support in All Sites	**Host on VLAN Techincal Support in All Sites**	**IP**	**Access**	**Yes**
Host on VLAN Vehicle Servicing in All Sites	**Host on VLAN Vehicle Servicing in All Sites**	**IP**	**Access**	**Yes**