Alternatives to Redistribution Communities in Inter-domain traffic Engineering

Vivekanandan Mahadevan

Department of Information Technology, SRM University, Chennai
`Vivekanandan.ma@ktr.srmuniv.ac.in`

ABSTRACT

Today's internet routing mainly concentrates on controlling the ingress and egress traffic which occurs through border routers. There are different ways by which we can control the traffic between autonomous systems. In most cases redistribution communities are used for the control over traffic engineering. In this paper we focus on alternative approaches like Multi Protocol Label Switching (MPLS) and Ambient Networks, through which there can be an effective control over traffic engineering.

KEYWORDS

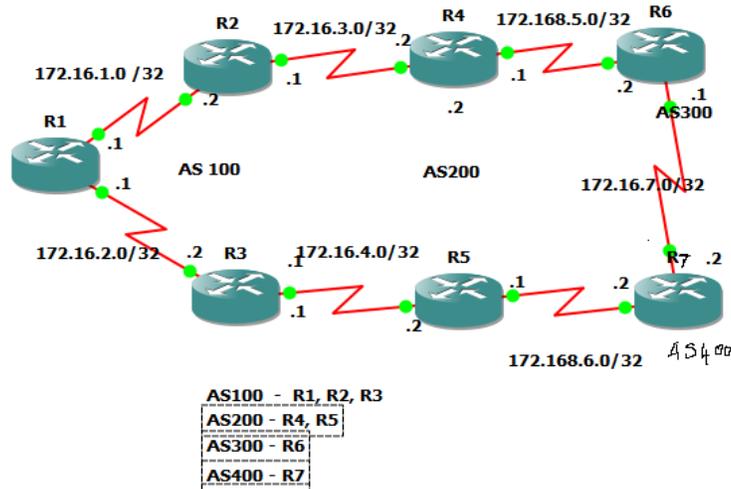*Traffic Engineering, BGP, MPLS, Local Preference, Ambient Networks.*

1. INTRODUCTION

BGP is the exterior gateway protocol which is used in the internet to exchange routing information between autonomous systems. The area of network infrastructure under a single administrative control is known as autonomous system. The flow of data towards an autonomous system from different destination is known as ingress traffic. On the other side, egress traffic flows towards destination from the source. ISP's should have proper border routers which are capable enough to balance this traffic. BGP acts like a RIP, if it is not properly tuned. Hence the network administrator has to properly tune their network to avoid unnecessary flow of data packets which will result in network congestion. To avoid such congestion we need traffic engineering. Traffic engineering should be implemented effectively so that ISP's can provide a better quality of service between its customers and the upstream providers. While controlling the traffic, some of the important parameters such as link capability, speed, next hop, bandwidth etc have to be considered. This paper exhibits the different ways by which we can do traffic engineering to obtain a better QOS.

The most well-known and commonly used traffic engineering technique is redistribution communities. Communities by themselves cannot have an impact of BGP decision making process. Flags are used in communities to mark a set of routes. These flags will be used by other autonomous system routers to apply those specific routing policies with in their network. Administrators will be using some of the BGP attributes like next-hop, local preference along with community attributes to control the ingress and egress traffic. These community attributes have few drawbacks which limits its usage over the internet.

2. INGRESS AND EGRESS TRAFFIC CONTROL

Ingress and egress traffic can be effectively controlled using BGP attributes. Local preference and metric has been configured for the following topology in order to estimate the traffic characteristics of ingress and egress traffic. The result is as follows

AS100 - R1, R2, R3
AS200 - R4, R5
AS300 - R6
AS400 - R7

2.1. Local-preference

This attribute can be mainly used to control the path that egress traffic takes. Using the topology in Figure 1 local preference is configured to control the outgoing traffic from AS100 to AS300 and AS400. The network 100.100.100.0 is in AS300-R6 and 200.100.100.0 network is in AS 400-R7. Initially without tuning, BGP makes the routing decision based on next hop. The shortest path from R1 to R6 is via 172.168.3.2 and to R7 is through 172.168.4.2

Before configuring BGP Attributes:

Network	Next Hop	Metric	LocPf	Weight	Path
*>i 100.100.100.0/24	172.168.3.2	0	100	0	200 300 i
* i	172.168.4.2	0	100	0	200 400 300 i
*>i 200.100.100.0	172.168.4.2	0	100	0	200 400 i
* i	172.168.3.2	0	100	0	200 300 400 i

After configuring Local preference

Network	Next Hop	Metric	LocPf	Weight	Path
*i 100.100.100.0/24	**172.168.3.2**	**0**	**100**	**0**	**200 300 i**
*> i	**172.168.4.2**	**0**	**100**	**0**	**200 400 300 i**
*i 200.100.100.0	**172.168.4.2**	**0**	**100**	**0**	**200 400** i
*> i	**172.168.3.2**	**0**	**100**	**0**	**200 300 400 i**

From the above table it is clear that an administrator can have an effective control over an outgoing traffic using LP within his autonomous system.

2.2. Metric

Metric is the only attribute which can be used to control the incoming traffic from other autonomous systems. Here we are going to configure metric values to the border routers on an autonomous system so that the route of ingress traffic towards this autonomous system is changed. Before configuring it, in order to explain metric, some changes have been made to the topology in the figure. A serial link is connected between routers R3 and R4. Network 60.0.0.0 is configured on router R4. Extended ping has been used to test the connectivity from router R3 to R4 via 172.16.2.2 of the serial interface.

Before configuring metric the obtained ping result is

 Target IP address: 60.0.0.1

Repeat count [5]: 1

Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y

Source address or interface: 172.168.2.2

Reply to request 0 (56 ms). Received packet has options

Total option bytes= 40, padded length=40

Record route: (172.168.8.1)

        (60.0.0.1)

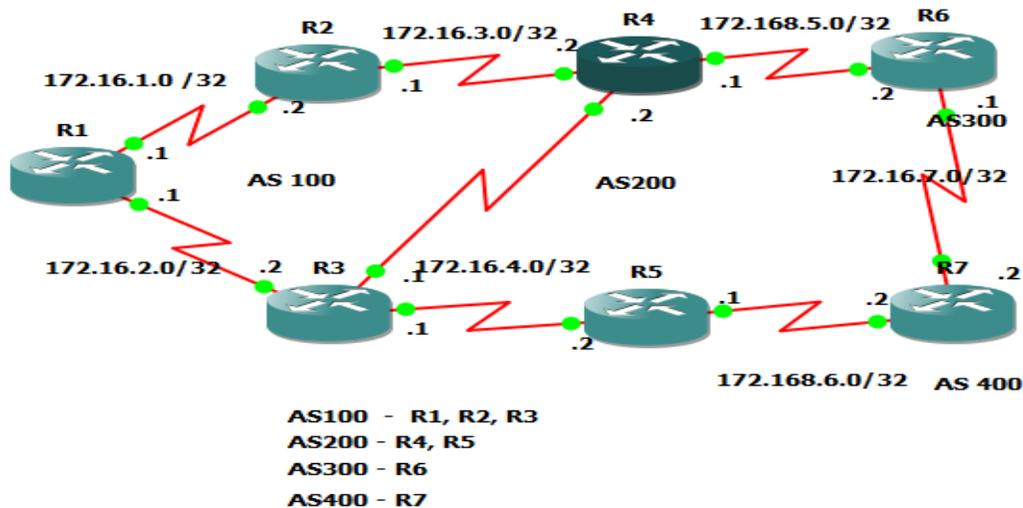   (172.168.8.2)

        (172.168.2.2) <*>

Figure2.Routing using metrics

After configuring metric:

Reply to request 0 (112 ms). Received packet has options

Total option bytes= 40, padded length=40

Record route: (172.168.8.1)

        (60.0.0.1)

        (172.168.3.2)

        (172.168.1.2)

        (172.168.2.1)

        (172.168.2.2) <*>

Hence from this it is to be noted that an administrator can even have a control over ingress traffic using metric. Even here an administrator can only control the external interface of an autonomous system from which the administrator is receiving ingress traffic and not the other autonomous system.

3. Community Attributes

Finally it has to be noted that if an administrator wants to have a control over the other autonomous system, the administrator should find a way to pass the necessary attribute values to the other autonomous system. This can be done by making use of community attribute. But there are drawbacks that have to be considered while passing an attribute along with BGP table to the other autonomous system.

Some of the drawbacks of the community attributes are:

- Whenever an autonomous system wants to use communities, it should advertise its own community value to all other external peers. There is no standard method for anyone to advertise this community value.

- Using BGP attributes results in more human errors which affect the global internet routing to a greater extent.

- While including community attributes, several route filters have to be applied appropriately. This further increases the complexity of the BGP routing table.

- Finally the most prominent drawback of redistribution communities is that it requires manual configuration at every router.

In the next two sections we are going to see two different methods for traffic engineering i.e. Multi Protocol Label Switching and Ambient Networks. The following focus on how these two methods are suitable for traffic engineering.

4. MULTI PROTOCOL LABEL SWITCHING (MPLS)

Multi Protocol Label Switching (MPLS) is an improved packet forwarding scheme which can offer advanced IP services and it is highly scalable. It is rather a new technology that is used to address issues concerned with packet forwarding. In this paper we are going to focus on how MPLS can be used for traffic engineering. The First section focuses on the introduction of MPLS, the new terms used in it and its working mechanism. Later part explains how MPLS can be used in Traffic Engineering.

4.1 How MPLS works

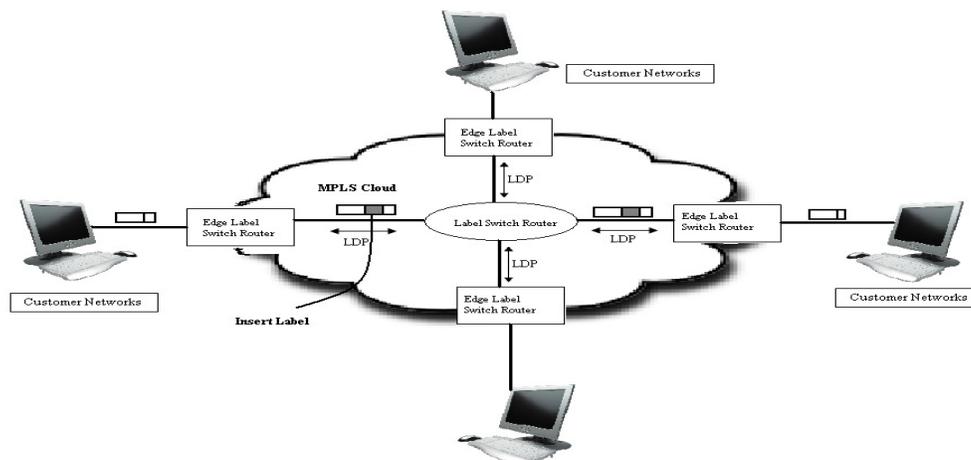The Following figure explains how a packet flows through a MPLS network.

Figure3. MPLS Network

Now at the ingress traffic of each edge LSR, a MPLS label or header is included based on the information from the Label Distribution Protocol (LDP). Within the MPLS cloud this label is used by the LSR to lookup its forwarding table and then it changes the label if required and forwards it to the next LSR where the process is repeated. Finally at the egress Edge LSR, the

MPLS label is removed. This MPLS label is composed of 32 bits and these bits are divided as shown in figure
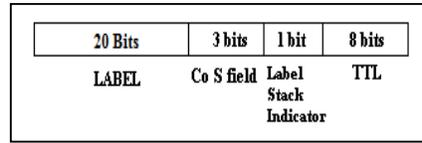

Figure4. MPLS Label format

The path followed by the packet between the two edge LSR's is called Label Switched Path (LSP), and these LSP's are created with the routing information available in the LDP table. The LSP paths are controlled by assigning attributes, where each LSP has its own attributes.

The various attributes used are,

1. Bandwidth

2. Path Attribute

3. Setup Priority

4. Affinity

5. Adaptability

6. Holding Priority

7. Resilience

4.2 Traffic Engineering with MPLS

The following explains some of the features in the MPLS architecture that makes it suitable for traffic engineering and then how these features are being used for traffic engineering. The table describes the features [8],

In MPLS-TE a Label Switched Path is established in order to forward the traffic. This LSP can be established by using different signalling methods and the most common method is Constraint Based Routing Label Distribution Protocol (CR-LDP).

Feature	Description
Separation of Control and Forwarding	The key architectural principle of MPLS is a clean separation of control and forwarding. This separation enables effective service integration including QoS transparency between service layers.
Forwarding	The forwarding component of MPLS is

Component	designed to be simple and efficient. While this is motivated by a desire to allow the forwarding to occur in hardware, it also makes the forwarding algorithm independent of control module.
Label Stack	MPLS allows an arbitrary number of labels. The labels are simply stacked. A field in the label encapsulation indicates whether this label is the bottom of the stack. There are three label operations, push, pop, and swap.
MPLS Control Components	Many possible control planes can operate in an MPLS environment. These include unicast routing, multicast, Resource Reservation Protocol (RSVP), virtual private networks, frame relay, and traffic engineering. Multiple control planes can manipulate labels on a single packet; combinations of control planes allow many services. In fact, MPLS could stand for *multipurpose label switching*.

Table1. MPLS Architectural features for Traffic Engineering

Constraint Based Routing computes the path for a packet in a way that the load is balanced to all paths. It not only considers the network topology but also other path constraints such as bandwidth and administrative policy. Finally it establishes an explicit route and this route do not have to be the shortest path, since it can select a lightly loaded path in order to prevent the usage of a heavily loaded shortest path. Hence by combining MPLS and CBR, traffic engineering can be done much better.

The method described above is for an MPLS specific module. There are other methods in which enhancements to already existing modules such as Resource Reservation Protocol (RSVP) and IGP's are done in order to support MPLS-TE. For example in RSVP, extensions are done to the message formats to support traffic attributes during signaling processes and a complete explicit route is established. Routing by Resource Reservation (RRR) is a new method by which traffic engineering is implemented. MPLS-TE has been used along with RRR to avoid network congestion and optimally utilize the network resources that are available.

Advantages of MPLS in Traffic Engineering

1. Reduces operation cost by using the network backbone infrastructure efficiently.
2. It increases network scalability and simplifies the overall network management.

3. MPLS-TE can be supported by modifying existing signaling protocols.

4. It provides an alternative path when the primary path fails.

5. Avoids manual configuration and provides effective forwarding rate using layer2 address.

6. Avoids human error to an greater extent.

5. AMBIENT NETWORKS

Definition (Views): [Abrahamsson] expresses Ambient Network as a new network technology platform that will be able to bring together the cooperation of different networks regardless of their different domains. Another view of the Ambient Network, considers the network as a technology that will bridge incompatibilities of different network functions [Bength]. With the recent improvements in modern technological developments like mobile technology and wireless links, this network has the ability to combine features like WLAN, GSM and 3G to work together.

Figure5. Ambient Network

5.1 Architecture

The architecture of the ambient network is built to integrate features like mobile communication networks and 3G [Bengt11]. The Ambient Network internetworking phase is divided into two main frameworks i.e. Connectivity Framework and Naming Framework [Bength]. The Connectivity Framework encompasses the Ambient Control Space (ACS….refer to diagram) which controls all functions of the network integration through its interfaces (Resource Interface and Service Interface) [6th Prg].
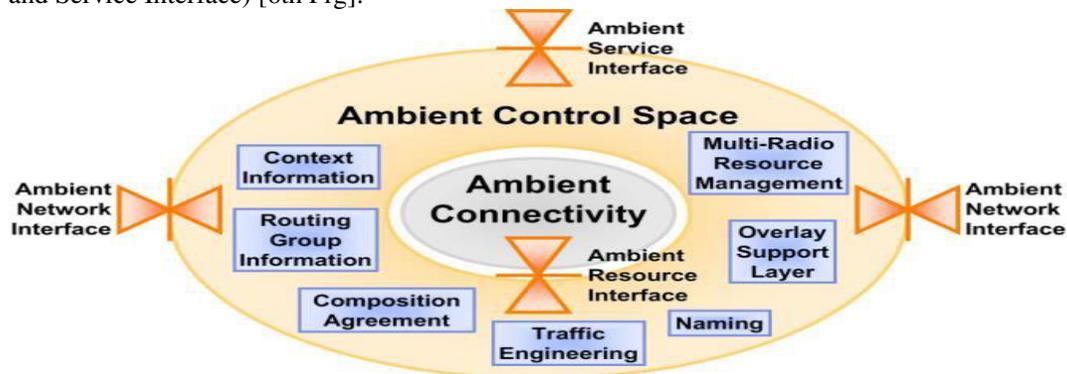

Figure6. Control space modularization and interfaces

Figure 6, shows how different technologies are connected by their links through the AN platform. As this connectivity will include nodes, there will also be an exhibition sequence of traffics between any two nodes (and these sequence pattern can be regarded as paths) within a provided time [Bength].

The Naming Framework is based on "entities" and not the names of the entities such as namespace used in every important layers [Bengths 9]. Bengt et al [], describes four categories Ambient Network Naming layers. These are:

- *Naming Layers*: deals with entities like applications, services and data.
- *Dynamic Binding between Levels*: so that entities can become location free.
- *Indirect and Delegation*: creates an advance mobility series and gives control to processes like NAT, so that an entity can attach itself to any network in any location.
- *Bridging Across Different Addressing Realms*: uses translation from foreign domain to a native and also uses common namespace that can be used by all networks.
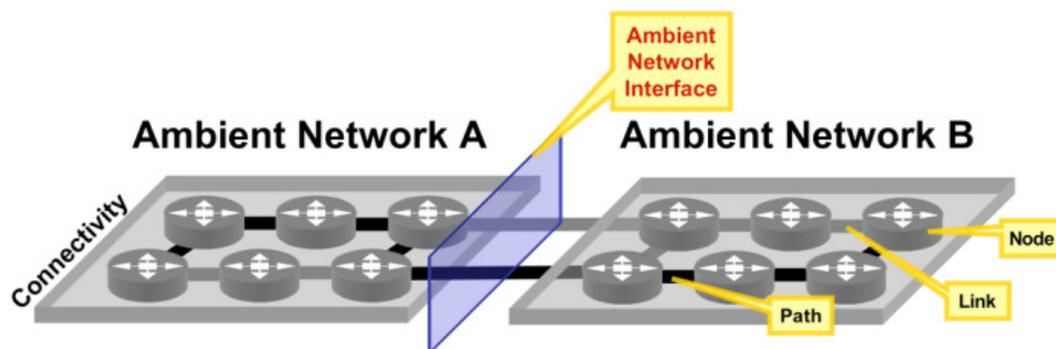

Figure7. Abstract connectivity planes in *Ambient Networks*

5.2 Effects of Ambient Networks on Traffic Engineering

Integration is the main purpose of Ambient Networks and the need to handle traffic loads must be an essential focus. Since there will be different devices on different networks, a dynamic traffic distribution system is needed to maintain a proper flow of the information delivery [Abra]. To enable AN deal with the traffic engineering, the following methods can help,

a. *Multi-Commodity Flow Optimization*: by tackling MCF problems (global optimal solution can calculate global information with regards to its links capabilities and traffic demands). The advantage of using this solution is its faster ability to calculate thousands of global optimal solutions which can aid in faster delivery of packets. Using these optimization methods can be configured as the primary path determinant. Attributes of the traditional routing protocols e.g. OSPF can also be used as secondary path determinant.

Figure8. Traffic Engineering Process (Source [Towards])

The collaboration of the above two information processes can create a division of labour, where a global optimal solution handles the topology connectivity using routing protocols like OSPF. While the attributes can handle the traffic demands like load balancing.

b. *Local State Perspective*: depends on taking local decisions e.g. load balancing in a dynamic network environment which traffic demand increase can shift location from heavy or a low consumed paths. Also the use of new improve algorithms like the Multi Path-Routing with Dynamic Variance (MRDV) can also aid in distributing and localizing multi-path routing [towards paper 8]. An MRDV algorithm includes the load of the next hop router which can help to determine a lesser load link to use.

Brunners et al [], states that traffic engineering in AN "which needs to provide connectivity anywhere, anytime, at a low cost" needs to address problems of shifting traffic demands and network topology with dynamic emphasis [4] [5]. These problems could be solved by the implementation to two steps [7],

Sufficient information gathering: this method is used to increase the optimization of routing in the network. Two ways of collecting information from source to destination are by using the Traffic Matrix (enables the capturing and analyzing of data entering backbones that runs a BGP routing protocol) and Link loads (to enable load balancing and also allows creates scalability and redundancy).

Optimization of routing configuration: - the use of forwarding system like MPLS (which can use label switch path) can result to an improve traffic.

6. FUTURE ENHANCEMENT:

To make MPLS better and to use it globally, certain flag attributes have to be inserted along with label distribution protocol to control the traffic manually. This will not add to the BGP payload because LDP is a separate protocol which is used to forward only the labels. Finally we came to know about an emerging technology known as ambient networks which can be considered as an alternative for traffic engineering in the future, where it may be required to combine different networks in different domains.

7. RELATED WORK

An in depth explanation of the MPLS Architecture is seen in [9]. The various features of MPLS that make it suitable and its advantages for traffic engineering are explained in [8]. There have been recent implementations of MPLS along with other signaling protocols in certain areas. For example MPLS is used with Routing by Resource reservation (RRR) in order to improve traffic engineering. It is possible that in the near feature we will need combining of networks from different domains and Ambient Networks is considered to be a suitable solution. Traffic engineering and its feasibility in Ambient Networks is seen in [4]. Broader knowledge of the architecture of Ambient Networks was studied in [6]. The use of MPLS and Ambient Networks can prove to be more suitable for traffic engineering than Redistribution Communities in the near feature considering the drawbacks of redistribution communities. It is also possible to combine MPLS with BGP in order to obtain better traffic engineering which in turn gives better QoS.

6. CONCLUSION

Thus in this paper we analyzed the different way of controlling the ingress and egress traffic especially between different autonomous systems. The most usual way by which these traffic's

were controlled by using community attributes. Our analysis and prediction says that if MPLS is used for controlling traffic, the rate can be controlled in a much brisk pace, since it is using layer2 forwarding. This also reduces human error to a greater extent.

REFERENCES

[1]   Jerome Saltzer. On the Naming and Binding of Network Destinations. In P. Ravasio et al. (ed.), Local Computer Networks, North-Holland Publishing Company, Amsterdam, 1982, pp. 311-317. (Reprinted as RFC1498, August 1993.)

[2]   Bengt Ahlgren, Lars Eggert, Börje Ohlman and Andreas Schieder: "Bridging Heterogeneous Network Domains". European Union Commission. Sixth Framework Programme. March 30th, 2005 Pg 1-5.

[3]   Marcus Brunner, Alex Galis , Lawrence Cheng, Jorge Andrés Colás, Bengt Ahlgren, Anders Gunnar, Henrik Abrahamsson, Robert Szabo, Simon Csaba, Johan Nielsen, Alberto Gonzalez Prieto, Rolf Stadler, Gergely Molnar: "Towards Ambient Networks Management". Ambient Networks - Information Society Technologies Project. European Union Commission. Accessed: http://www.ambientnetworks.org/phase1web/publications/Tow ards_Ambient_Networks_Management.pdf on 14th Feb, 2010.

[4]   Henrik, Abrahamsson. & Anders, Gunnar: "Traffic Engineering in Ambient Networks: Challenges and Approaches". Swedish Computer Institute. Accessed on: http://www.sics.se/~henrik/ante-sncnw-final.pdf on 13th Feb, 2010.

[5]   Sixth Framework Programme: Ambient Network. "Ambient Network Management –Technologies and Strategies". Project 507134. 21st Dec, 2004. Pg 1-124

[6]   Sixth Framework Programme: Ambient Network. "AN Framework Architecture". Project 507134. 30th Dec, 2005. Pg 1-120

[7]   Stefan Schmid, Lars Eggert, Marcus Brunner and Jürgen Quittek. Towards Autonomous Network Domains. Proc. 8th IEEE Global Internet Symposium, Miami, FL, USA, March 17-18, 2005. ….Bengt 11

[8]   George Swallow, "MPLS Advantages for Traffic Engineering", Cisco Systems.

[9]   John Evans, "MPLS Architecture", Cisco Systems.Authors

Author

VIVEKANANDAN .M

8807163574
E-mail: anandanviv@yahoo.co.in, anandanviv1@gmail.com
F-9, People flats, Nerkundram, Chennai - 107
CCNP Network Academy Certified Professional

Obtained letter of appreciation from CISCO for all CCNA and CCNP modules Academy
Working in Ideaon Think as a Senior Network Trainer as well as working in SRM University as a Assistant Professor cum research analyst in Cisco Network Academy.
Worked with Cable and Wireless Worldwide as a Network Engineer for 6 Months
Have Masters in Computer Network Engineering (2010) (Grade 5) , HALMSTADUniversity, Sweden
Excellent communication & presentation skills in working area.
Worked in team environment and had expertise in the complete project development Lifecycle.
Worked as a Network trainer in Linsun Technologies for 1year.
Worked as a trainee in ALCATEL LUCENT for 8 months, in the telecommunication domain, i.e. we wrote testing codes to automate PABX and we automated the PABX by making use of 2 tools (PILOT2a,C-AUTECO-which is very similar to C++) provided by the company.