Helsinki Metropolia University of Applied Sciences

Degree Programme in Information Technology

Prayash Bakhati

Simulating Technical ISP Environment

Final Year Project. 7 October 2010
Supervisor: Matti Puska, Principal Lecturer
Language advisor: Taru Sotavalta, Senior Lecturer

Contents

Helsinki Metropolia University of Applied Sciences **Abstract**

Author	Prayash Bakhati
Title	Simulating Technical ISP Environment
Number of Pages Date	51 7 October 2010
Degree Programme	Information Technology
Degree	Bachelor of Engineering
Supervisor	Matti Puska, Principal Lecturer

This project was carried out to study a small technical ISP environment. The goals of this project were to experiment in practice which network components, services and solutions are needed by a small ISP and what kind of information for customer support is available from ADSL connection and how.

The complete infrastructure of an ISP was built using the available resources. A topology was designed and Internet service was provided to the remote user using ADSL connection. Possible error generation and troubleshooting related to the customer support was done.

The information about the networking services and components needed to build a small ISP and possible Support and Remote Maintenance to the customer using the ADSL connection was gathered, which was the result of the project.

This thesis can be used as a reference guide by all the Internet users and networking students for the basic understanding of an ISP.

Keywords	ISP, ADSL

Abbreviations

ADSL	Asymmetric Digital Subscriber Line
AS	Autonomous System
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
DHCP	Dynamic Host Control Protocol
DNS	Domain Name System
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
FQDN	Fully Qualified Domain Name
FQDN	Fully Qualified Domain Name
IIS	Internet Information Services
InterNIC	Internet Network Information Center
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider
MIB	Management Information Base
MODEM	Modulator-Demodulator
OID	Object Identifier
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
RFC	Request for Comments
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
TCP/IP	Transport Control Protocol/Internet Protocol
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol

1 Introduction

The term "Internet" is one of the most used words in the world today. There are only few who are unaware of it. It is a connection of many computer networks together by means of electronic and optical networking technologies. It carries a lot of information from one network to another making it global. Due to its efficiency, all banks, academic institutions, business companies and many other sectors rely heavily on it. Despite knowing what it is and how to use in the day- to- day life, only few are aware about the fact that an Internet Service Provider (ISP) provides Internet service to them. They are only the remote users who access the Internet through ISP. The remote users from the ISP perspective are all customers.

This project dealt with the Technical ISP Environment. Designing, building and implementing the ISP by using the resources available in the laboratory and testing it with the remote user connectivity were the core concepts of the project. The goals of this project were to experiment in practice which network components, services and solutions are needed by a small ISP and what kind of information for customer support is available from the Asymmetric Digital Subscriber Line (ADSL) connection and how.

The order of the table of contents starting from access technology and ending with support and maintenance was arranged according to the Open Systems Interconnection (OSI) model. The reason behind this was to present the project concept more clearly from the customer perspective.

2 ISP Infrastructures

Understanding details about the Internet in the current world is complex. So, simply it is just a network of networks. Millions of small and large networks combine to make the Internet. Billions of customers' computers are connected to Internet through those small and large networks making them also part of a network. Those small and large networks that provide Internet access to customers are the ISP. Three combined together makes a simple network hierarchy with Internet being on top, ISP in the middle and customer at bottom. [1]

The size of the ISP heavily depends on the number of customers and different services ordered by them. An ISP located on a remote area might be smaller than an ISP located in a big city. No matter how big or small an ISP is, its main purpose is to provide Internet connection and services to the customer. ISP charge money from the customer for doing so. Customers are classified into two categories: private and business customers. Private customers buy an affordable Internet connection from the ISP for their personal use such as for e-banking and general internet use whereas business customers buy the high bandwidth Internet connection for their business purposes such as banks to provide twenty-four e-banking facilities to their customers and the small ISP company to provide internet services to their customers.

Either private or business customers, ISP provides different Internet connections and services to them according to their needs. The essential services, include Domain Name System (DNS) services, Dynamic Host Control Protocol (DHCP) services, (Internet Protocol) IP routing services, Web services, bandwidth services, maintenance services and billing services whereas additional services includes, for example, telephony, networking equipment supporting their ISP, advertisement, E-Mail. An ISP infrastructure is also another factor which is hugely affected by the number of customers and their service requirements. When it is increased, the infrastructure becomes more complex requiring additional resources. However the basic infrastructure for building a small or large ISP is the same. Every ISP maintains the map of its infrastructure, which in networking

terminology is called topology. This is very crucial for ISP since it helps to provide a clear picture of all the networking equipment, their placements and customers connected to them. This project was carried out considering a very basic infrastructure of a small ISP environment and basic services that could be available to a customer. The ISP infrastructure consists of networking equipment, operating systems and workstations. The networking equipment included routers, switches, Digital Subscriber Line Access Multiplexer (DSLAM) and Asymmetric Digital Subscriber Line (ADSL) modem. The operating system included Microsoft Windows Server 2008 x86 and Microsoft Windows Server 2003 x86. The workstations included three computers which were able to support the operating system defined above. Two of them were configured to be servers and one a customer.

A topology was designed using the infrastructure resources and it was implemented during the project. The complete view of the designed topology can be seen in Figure 1.

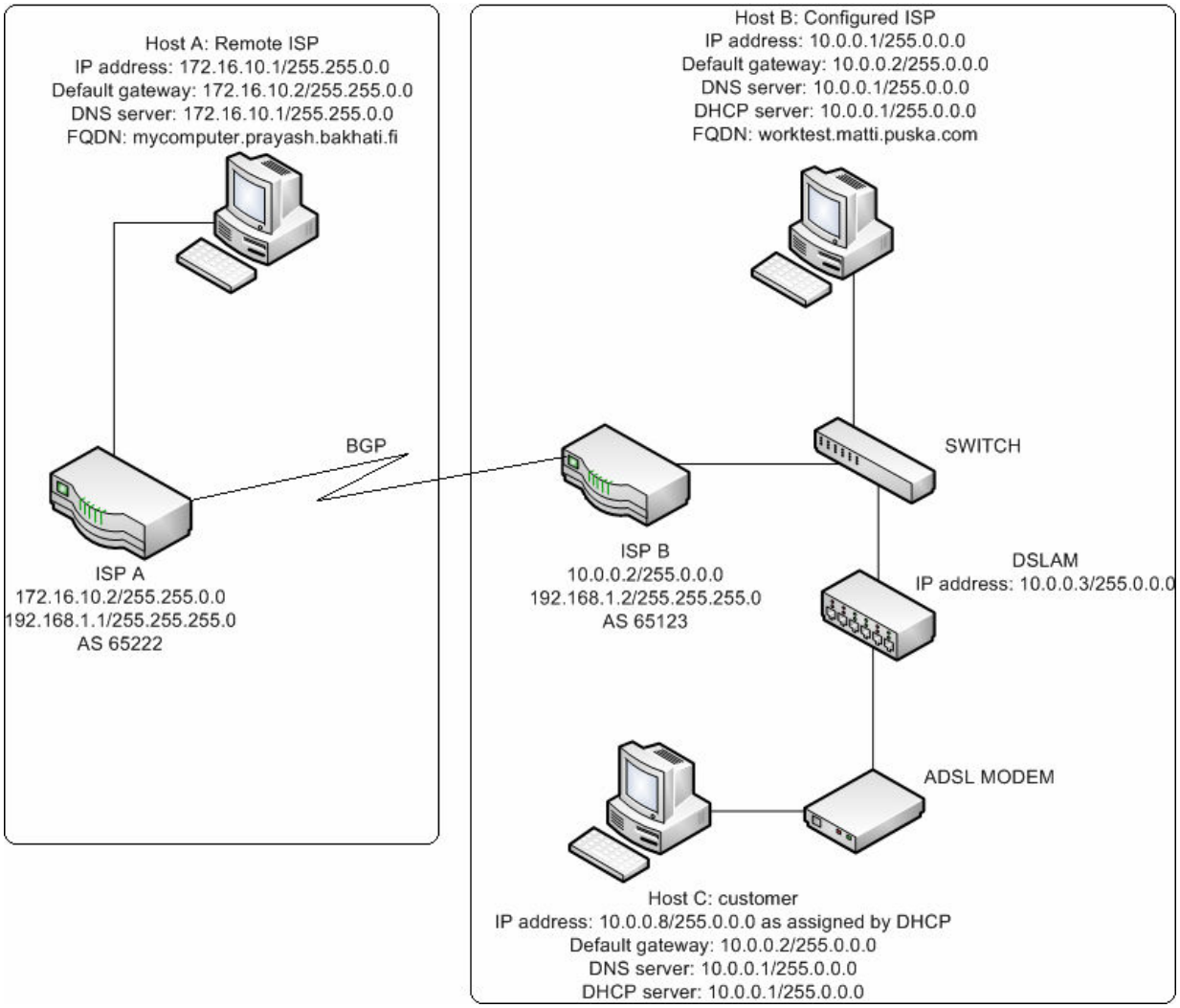

Figure1. Designed ISP Topology [Prayash Bakhati]

The figure above is the representation of simulated ISP environment, carried out during the project. The topology description is given below.

Topology Description

Real world ISP network topology is complex. An ISP network is connected to many other remote ISP networks in order to provide an Internet connection to customers. The customers are linked only with their own ISP network unaware about the facts how an ISP provides Internet connection to them. ISP is built with networking equipment and essential services on them, which are required to provide an Internet connection. The ISP maintains different servers for providing the essential services such as DHCP, DNS and Web servers.

The DNS server of the ISP is registered legally with a unique domain name and public IP address. ISP uses public IP addresses on DNS server since they have to be publicly available on the Internet for providing name resolution service to the customer and private IP addresses on the networking equipment, and customer workstations to provide security on the network [2;3,430;4]. Private IP addresses are only visible by ISP and their own customers. ISP uses different IP routing services for defining path to be followed by IP packets to reach its destination, providing IP connectivity between different hosts on the network to provide Internet connection to the customer [5;6]. In order to provide a good understanding of a small ISP environment, a topology was designed and implemented in the project.

The topology was a simulation of a small ISP environment. It was designed and implemented by using minimum resources and basic services such as DNS service, DHCP service, IP routing service and Web service in order to provide Internet connection to the customer. The topology was logically separated into two boundaries by Autonomous System (AS) 65222 comprising ISP A router and AS 65123 comprising ISP B router and its components of the network along with the fundamental services on it. The AS was used to exchange routing information between the ISP A and ISP B routers which were connected with different IP networks. The Autonomous System Numbers (ASNs) were used to identify the AS on the network and exchange the routing information [7;8].

The ASNs used in the project were private even they were supposed to be public in practice because the project was carried for studying purposes. In the real world, a private ASN is used if an AS is required to communicate with a single ISP through BGP. The routing policy between the AS and the ISP will be not visible over the Internet when a private ASN is used. A Private ASN is generally used to conserve the Autonomous Systems (ASes). A Public ASN is used when an AS is required to exchange routing information between ASes on the public Internet. All the routes which are originated from an AS will be visible on the Internet when a public ASN is used. A Public ASN has a single and clearly defined routing policy which is different from ISP routing policies. [7;9] The logical separation was done for the purpose of scalability and reliability of the entire network so that, as the demand of the Internetwork services grows, the administrator could easily upgrade the entire network without any constraints in a short period of time.

A host A was configured to be a DNS server and Web server by implementing DNS service and a Web service application on it. A Host B was configured to be a DNS server, DHCP server and Web server by implementing DNS service, DHCP service and Web service applications on it. The purpose of the DNS servers was to provide the name resolution service, the DHCP server to provide dynamic address allocation service and the Web server to provide Web service or Internet connection service to the customer. Microsoft Windows Server platform was used since it provided an easy and well-organized configuration procedure with detailed information for implementing DNS, DHCP and Web services using a Graphical User Interface (GUI).

The core part of the project lied on the AS 65123. The ISP B router being the edge router of AS 65123 was connected with ISP A using Border Gateway Protocol (BGP) in order to exchange all the prefixes that ISP B wanted and manage routing policy as needed by the real world ISP in practice. Host B was configured with all the services and was connected with the used networking equipment, which were switch, DSLAM and ADSL Modem. DSLAM and ADSL Modem were used to provide Internet connection to the customer using ADSL connection which was also part of the project.

Three different private IP addresses were used in the topology in order to understand the IP connectivity procedure between three different network subnets using the IP routing service. Since the DNS server on Host A and Host B were not registered legally, a private IP address was configured to represent them. The main aim was to provide an Internet connection to the customer through an ADSL connection using the services configured and the equipment used.

This project was designed to use three different private network subnets: 10.0.0.0/255.0.0.0 on Host B, 192.168.1.0/255.255.255.0 on ISP A and ISP B routers and 172.16.10.0/255.255.0.0 on Host A. The project was carried out for testing purposes so the large private subnets were used even though it was not feasible. In the real world ISP, large subnets are avoided in order to prevent the waste of IP addresses.

3 Access Technologies

Access technologies can be defined as the equipment used to transfer data over the network. It allows the customer to get access to the various services available on the Internet. Access technologies can be of different kinds depending on the services used by the customers and used by ISP, for example: routers, switches, ADSL modem, DSLAM.

3.1 Asymmetric Digital Subscriber Line

Internet popularity is getting higher and is increasing the number of customers. The ISPs are providing Internet to the customer via different means of connections such as wireless connection, Digital Subscriber Line (DSL), such as ADSL and Symmetric Digital Subscriber Line (SDSL) connection, and cable connection. An ADSL connection among them is more preferred, since it tends to provide a good solution for a cost effective, fast and permanent Internet connection with traditional telephone service operating alongside [13,14]. An ADSL connection generally aims at residential consumer market and Small Office Home Office (SOHO) [10;13].

ADSL stands for Asymmetric Digital Subscriber line. Asymmetric meaning that the data speed is not same during downloading and uploading. The downstream rate is higher than the upstream rate, which enables large transfer of data in the downstream direction even though the requests from the customer are small. The data transfer rate in this kind of connection heavily relies on the connection distance between ISP and customer, and quality of subscriber line. If the distance of connection is short, the transfer rate is fast and vice versa. [11;13] ADSL provides cheap installation and a cost-effective Internet connection to the customer. ISP can configure ADSL connection bandwidth as required by the customer for Internet connection and charge accordingly. The main required device for an ADSL connection is the modem [12].

3.2 Customer Premises Equipment

CPE are the equipment placed at the customer's end for getting connected to the Internet. In the real world this equipment is generally provided by the ISP supporting its network infrastructure. It is also one of the essential services provided by an ISP to the customer. Depending on the customer necessity, this equipment might be of different kinds. Some common examples are: wireless routers, ADSL 2 modem and ADSL routers. The common device that a customer uses to get connected to the internet is modem. Modem is an electronic device that converts the digital signals sent by a computer into specific frequencies to travel over the telephone or cable lines. At the destination, the receiving modem demodulates the frequencies back into the digital data. Modems can be of different kinds depending on the vendors. Modems supporting the Internet and telephone access at the same time are ADSL modem.

3.3 Service Level Agreement

A contract between an ISP and a customer which specifies about the kind of services the ISP will furnish is Service Level Agreement (SLA). Generally the contract is specified in measurable terms. Many ISPs provides SLAs to the customer. Below are some metrics that SLAs may specify include:

a. Availability of services based on the percentage of the time.
b. Number of users that can be served simultaneously.
c. Periodic comparison of the specific performance benchmarks and actual performance.
d. Schedule Notification in advance to the users in case of sudden network changes.
e. Response time of helpdesk for various classes of problems.
f. Usage statistics that will be provided. [15]

3.4 Digital Subscriber Line Access Multiplexer

DSLAM is a piece of networking equipment, usually located in the telephone central office, used for connecting multiple customer Internet connections simultaneously. It is placed centrally between the ISP and customer. The ISP uses the DSLAM to broaden its service area where high-speed Internet connectivity can be offered. It functions as a conduit that allows a number of customers to establish a high-speed gateway to the Internet using a single connection. The customer can access the Internet fast, after getting a connection from the DSLAM. [16,17] The connection rate depends on the maximum available bandwidth allocated by the ISP.

The DSLAM operates by receiving signals from multiple customer DSL connections and putting the signals on the high-speed backbone line using the multiplexing techniques. Depending on the product, DSLAM multiplexers uses some combination of Asynchronous Transfer Mode (ATM), Frame Relay (FR), or IP to connect the DSL lines [17]. ADSL CPE connects them together allowing the Internet access to the customer. ADSL splitter equipment can be used in between the ADSL Modem and the DLSAM, which allows customer to use both telephone service and Internet service at the same time, if both services are made available to the customer by ISP.

In this project ZyXEL, IES-1000 DSLAM was used. It was placed centrally in between the customer and Host B. It used Multiprotocol encapsulation over ATM Adaptation Layer 5 (RFC 1483) for operation purposes [18]. The DSLAM was configured with the following parameters in order to provide an Internet connection to the customer.

a. IP address: To identify the particular networking equipment on the network topology and for remote maintenance purpose it was configured. In this project it was assigned to be 10.0.0.3/255.0.0.0 and could be used for maintenance purpose using its Web interface.

b. DHCP relay: In order to forward an IP configuration requested by the customer to the DHCP server, it was configured in this device. It was configured to forward the IP configuration request from the customer work station to the DHCP server on Host A and vice versa.

c. Static route: For defining the specific one way path for the customer to get connected over the Internet it was configured. The static route was: 0.0.0.0 0.0.0.0 10.0.0.2 which allowed any customer IP address to use 10.0.0.2 as its path.

d. Profile: This was created to identify the particular customer of ISP on specific port of DSLAM. This option provided the maintenance support to the customer in case of necessity.

e. Bandwidth: This option was defined to provide the ADSL connection to the customer as per the need. The default value on the DSLAM was changed to 256 Kbps for Upstream and 512 Kbps for Downstream to provide the configured bandwidth Internet connection to the customer.

This project included an ADSL connection for providing an Internet connection to the customer and also for testing purposes. The reason behind using an ADSL connection for testing purposes was to study what kind of services can be given to the customer and what kind of support and maintenance services are available to this kind of connection. The statistics observed after configuring all the parameters on the DSLAM about the ADSL connection and the bandwidth configuration according to the customer needs yields that ADSL CPE are needed to support ADSL connection.

4 DHCP Services

4.1 Theoretical Background

The DHCP is a TCP/IP service protocol that offers dynamic leased configuration of host IP addresses and distributes other IP configuration parameters to eligible network clients. It provides safe, reliable, and simple TCP/IP network configurations, prevents IP address conflicts, and helps to conserve the use of client IP addresses on the network. The DHCP uses client/server architecture where the DHCP server maintains centralized management of IP addresses that are used on the network. The DHCP supporting client requests and obtains a Lease of an IP address from a DHCP server as part of their network boot process.

The DHCP proves to be useful and convenient for a network administrator to add new clients to the local network. The DHCP server is able to manage a pool of IP addresses and information about the client configuration parameters such as lease length specification, default gateway, DNS server IP address and many other service parameters configured by the network administrator. DHCP clients and DHCP servers communicates by exchanging DHCP messages.

There is always a DHCP server in a managed network. When a DHCP enabled client connects to the network, it goes to the INITIALIZATION state immediately where it does not have any IP address and is unaware of DHCP server. Therefore, to obtain the valid lease from the DHCP server it creates and broadcasts DHCPDISCOVER Message and goes to the SELECTING state and waits for the replies from the server. The DHCP server receives the message, examines, creates DHCPOFFER Message including the IP address to be offered and forwards the created message to the client. After receiving the DHCPOFFER Message, the client decides whether to accept the offer or not and, creates DHCPREQUEST Message only if the client is ready to accept. If the client does not accept,

it enters a retransmission mode and tries sending the DHCPDISCOVER Message again for a period of time. [3, 1021-1024]

DHCPREQUEST Message created is sent to the server by the client staying in the REQUESTING state where it waits for a reply from the server. After receiving the DHCPREQUEST Message, the DHCP server sends DHCPACK Message to the client if the offered IP address is available on the lease with all the pertinent configuration parameters or DHCPNAK Message is sent if the IP address is unavailable. The client receives either DHCPACK Message or DHCPNAK Message. If the message is DHCPNAK the whole process of obtaining lease repeats from the beginning. If the message is DHCPACK the client reads the IP address and records the lease length and all other parameters from the message. The query is typically initiated immediately after the client starts booting and must complete before it can initiate IP-based communication with other hosts. [3,1021-1024]

The client will try to renew the lease after 50% of the lease time has passed, with the original DHCP server from which the lease was released. The client tries to renew the lease every time when it boots or the lease length is 50% or more passed. At 87.5% of the lease completion the client will attempt to contact any DHCP server on the network for a new lease release. If the lease expires, the client transits to the INITIALIZATION state to get the lease again. [3,1031;19]

The lease contains information about IP address and various parameters configured by the administrator. Each lease provided by DHCP server contains a duration explaining when the lease is going to expire. In general, the lease duration is equal to the average time the client on the subnet is active. Longer leases are efficient for the client that is active on the network for a longer period without getting disconnected from the network, since it provides stability of IP addresses on the devices. Generally, administrators prefer to use shorter leases because they force the client to renew the IP address continually as long as it needs it. When the client stops asking for permission for the renewal of the IP address, it is

pulled back to the DHCP pool and conserved. Shorter leases are normally used where the number of IP addresses is limited. [3,1003-1004]

The DHCP relay agent is needed to relay DHCP messages between clients and servers for DHCP on different IP networks. It can be a host or an IP router that listens to the DHCP client messages being broadcast on the subnet and relays them to the configured DHCP server. The DHCP server sends the responses again using the DHCP relay agent back to the DHCP client. DHCP relay agents eliminate the necessity of having a server running DHCP on each physical network segment.

From the customer perspective, DHCP server reduces the task of TCP/IP configuration on their computers and chance of creating the IP addresses conflicts on the network by the customer if they are given to assign it manually. DHCP offers automatic address allocation to the customer meaning that it tries to provide the same IP address every time to the customer by keeping the customer computer name on its cache database. The functionality of automatic address allocation allow customers to remember the IP address of their computer making them successful to use remote application such as remote desktop in the case of necessity.

All the networking devices on the network are identified by their own IP addresses. Networking devices such as routers and switches are easy and safer to configure by using the manual IP address since they have to be used frequently for maintenance and network upgrade purpose. DHCP mainly targets for the end user or customer. DCHP server can be configured on router or server operating system. The operating system such as Microsoft Windows Server families proves to be more convenient because of its capability to provide security layer, Graphical User Interface (GUI) to check the status of customer and upgrade the DHCP server in case of the growth of the network efficiently.

4.2 Practical Implementation

In this project, the DHCP server was configured in Host B on which Windows Server 2003 was installed. The Microsoft Windows Server 2003 was chosen because of its enrich features availability to the administrator such as integration of DHCP with DNS, enhanced monitoring and statistical reporting, multicast address allocation, unauthorized DHCP server detection, automatic and alternate client configuration, command-line management and most importantly GUI availability. [20]

DHCP server configured Host B was assigned to provide a dynamic IP address to the customer within the range of subnet 10.0.0.0/255.0.0.0. An exclusion range of IP address was defined excluding the IP addresses of the DSLAM (10.0.0.3/255.0.0.0), ISP B router (10.0.0.2/255.0.0.0) and DHCP server (10.0.0.1/255.0.0.0), since they were configured statically for maintenance purpose. The other additional parameters such as default gateway, DNS server IP address, DNS domain name and lease period were configured. The default gateway identified the IP address of the ISP B router that the customer used to communicate with the clients on the other subnets on the topology i.e. ISP A router and Host A. The DNS server IP address that the customer should contact to resolve the name of another computer on the topology i.e. Host A. The DNS domain name identified the DNS domain that the customer belonged and the lease duration until which period the lease was available. The IP address released by the DHCP server to the customer workstation is illustrated in figure 2.

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\PrayashBakhati>ipconfig /all
Windows IP Configuration
        Host Name . . . . . . . . . . . . : NEW
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : matti.puska.com
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . : matti.puska.com
        Description . . . . . . . . . . . : Realtek RTL8102E Family PCI-E Fast Ethernet NIC
        Physical Address. . . . . . . . . : 00-23-8B-44-49-8A
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.0.0.8
        Subnet Mask . . . . . . . . . . . : 255.0.0.0
        Default Gateway . . . . . . . . . : 10.0.0.2
        DHCP Server . . . . . . . . . . . : 10.0.0.1
        DNS Servers . . . . . . . . . . . : 10.0.0.1
        NetBIOS over Tcpip. . . . . . . . : Disabled
        Lease Obtained. . . . . . . . . . : 20. huhtikuuta 2010 3:48:04
        Lease Expires . . . . . . . . . . : 28. huhtikuuta 2010 3:48:04
```

Figure 2. Remote user TCP/IP configuration provided by DHCP
[Prayash Bakhati]

Figure 2 shows the details of TCP/IP configuration allocated by the DHCP server to the customer after the parameters were configured. The lease duration of eight days in the figure was the default parameter provided by the operating system and the same was used in the DHCP server configuration.

5 IP Routing

5.1 Theoretical Background

IP routing defines a set of protocols which determines the path that data follows in order to travel across multiple networks from its source to its destination. Packets sent are routed from source to ultimate destination through a series of routers and across multiple networks. IP routing protocols enable routers to build up a forwarding table which correlates the final destinations with the next hop addresses.

An IP packet contains the destination IP address in the packet header. When an IP packet is forwarded, the router uses its forwarding table built by the protocols or uses series of routes assigned manually by the administrator to determine the next hop address for the packet's destination and forwards it appropriately. The same process is repeated by the next router using its own forwarding table until the packet reaches its destination. Some common protocols included in IP routing are BGP, Intermediate System to Intermediate System (IS-IS), Open Shortest Path First (OSPF) and Routing Information Protocol (RIP). [5]

An AS can be defined as a group of routers that exchange routing information using common routing policies and are under the control of a single administration. In other words, it can also be defined as one network or a set of networks under a single administrative control [8]. An AS is needed when the network is scalable. An AS is used with a number also called the Autonomous System Number. The American Registry for Internet Numbers (ARIN) defines Autonomous System Numbers as follows:

> *Autonomous System Numbers (ASNs) are globally unique numbers that are used to identify autonomous systems (ASs) and which enable an AS to exchange exterior routing information between neighboring ASs. An AS is a connected group of IP networks that adhere to a single and clearly defined routing policy.* [8]

Depending on the network structure Interior Gateway Protocol (IGP) and Exterior Gateway Protocol (EGP) are used precisely for IP routing purpose. IGP is used to exchange routing information between gateways within an AS. The routing information can then be used by the IP or any other network protocols to specify how to route transmissions. For example: OSPF, RIP etc. EGP is used to exchange routing information between ASes. Each AS must use the same exterior protocol to ensure the communicability.

The BGP is the most recent form of Exterior Gateway Protocol (EGP) which uses TCP as the transport protocol on port 179 to establish a connection between the routers [21]. The BGP is the most used protocol between gateway hosts on the Internet. It is a path vector routing protocol. Its BGP table contains a list of the nearest reachable routers, the addresses they can reach, and a cost metric associated with the path to each routers so that the best available route is chosen. BGP used between ASes is called External BGP (eBGP) and when it used to exchange route within an AS it is called Internal BGP (iBGP) which is widely used whenever the peer connection has to be created even though there is no physical connectivity directly. [22]

ISP combines many networks together from different AS. So there are multiple routes that can be used to reach from source to the particular destination. All the routes which are learned by BGP have associated properties also called BGP attributes, which helps to determine the best route to that destination. Some of the common attributes include Weight, Local preference, Multi-exit discriminator, Origin, AS_ path, Next hop and Community. [22]

5.2 Practical Implementation

In this project it was not completely necessary to implement BGP for routing between the two ASes. Statically configured routes would be just perfect for the smooth communication between the ASes. The use of BGP in project is the simulation of real world ISP in practice. EBGP session was created with ISP A and ISP B allowing the way to transfer BGP table of ISP A to ISP B and vice versa. No further complex configuration was made due to the simplicity of the designed topology. The result of the configurations made for IP routing on the routers during the project can be seen in figure 4 and figure 5.

```
ISPA#sh bgp

BGP table version is 3, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.0.0.0         192.168.1.2              0             0 65123 i
*> 172.16.0.0       0.0.0.0                  0         32768 i
```

Figure 4. BGP table of ISP A router

Figure 4 was the result of the configurations made on the ISP A router, which shows the neighbour route to ISP B was AS 65123.

```
ISPB#sh bgp
BGP table version is 3, local router ID is 192.168.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.0.0.0         0.0.0.0                  0         32768 i
*> 172.16.0.0       192.168.1.1              0             0 65222 i
```

Figure 5. BGP table of ISP B router

Figure 5 was the result of the configurations made on the ISP B router which shows the neighbour route to ISP A was AS 65222. The other attributes metric, local preference, path were not configured since the topology was designed to use only one route to exchange information.

```
C:\Documents and Settings\PrayashBakhati>ping 172.16.10.1

Pinging 172.16.10.1 with 32 bytes of data:

Reply from 172.16.10.1: bytes=32 time=63ms TTL=126
Reply from 172.16.10.1: bytes=32 time=39ms TTL=126
Reply from 172.16.10.1: bytes=32 time=42ms TTL=126
Reply from 172.16.10.1: bytes=32 time=39ms TTL=126

Ping statistics for 172.16.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 39ms, Maximum = 63ms, Average = 45ms

C:\Documents and Settings\PrayashBakhati>
```

Figure 6. IP connectivity test output using ping command

Figure 6 shows the IP address connectivity over the whole network after the Routing Information Base (RIB) is updated in BGP table. It was tested by using the ping command from Disk Operating System (DOS) mode to the Remote ISP IP address from the customer.

6 Domain Name System Services

6.1 Theoretical Background

DNS is a name resolution service which resolves human readable addresses into IP addresses. For example: www.microsoft.com into 207.46.10.123 and vice versa. It is a hierarchical, distributed database containing mappings of DNS host names to IP addresses and uses alphanumeric names to locate the hosts, which are easy to remember.

DNS has played a crucial part in the modern networking technology and over the Internet. Since it uses alphanumeric names to locate and access the networking resources, it has removed the difficulty of locating the resources using the IP addresses. In this current world, there are billions of hosts with different IP addresses all over the Internet which are completely impossible to remember. It has solved the problem using the alphanumeric names which are friendly to Internet users and easier to remember. DNS has also helped to distribute the host names residing in the database among the multiple servers, by decreasing the load on any server.

The DNS is based on a conceptual naming system which is a hierarchical and logical tree structure called domain namespace. The Internet Network Information Center (InterNIC) is responsible for managing the root or the highest level of the domain namespace and registering the domain names and delegating administrative responsibility for portions of domain namespace. [23]

6.1.1 Domain Namespace

The domain namespace defines hierarchical naming system tree, which the DNS uses to identify and locate a particular host in a particular domain relative to the root of the tree. It includes root domain, top-level domains, second-level domains and sometime subdomains.

a. Domain: In DNS, a domain is any tree or subtree within the overall domain namespace.

b. Root domain: It is the node of the DNS tree and it is unnamed. It is represented by a trailing period (.) to designate that the name is at the highest level of the domain hierarchy or root.

c. Top-level domain: It is the rightmost portion of a domain name which is stated usually with a two or three-character name code that identifies either organizational or geographical status of the domain name. For example: .com, .org, .net, .edu, .mil etc.

d. Second-level domain: It is a unique name of varying length that is registered formally by InterNIC to an individual or organization that connects to the Internet.

e. Subdomain: In addition to the second-level domain name that is registered with InterNIC, a large business company and organization can further divide the registered domain name using the name of their different departments. Each department is then represented by separate name portion. [23]

A host name and DNS namespace combines together to form the Fully Qualified Domain Name (FQDN). The FQDN is the complete DNS name. The DNS namespace makes it easier the user to understand the display name of resources by organizing the name in a logical structure. The valid DNS naming of the tree structure is done by using a trailing period (.) after each domain level.

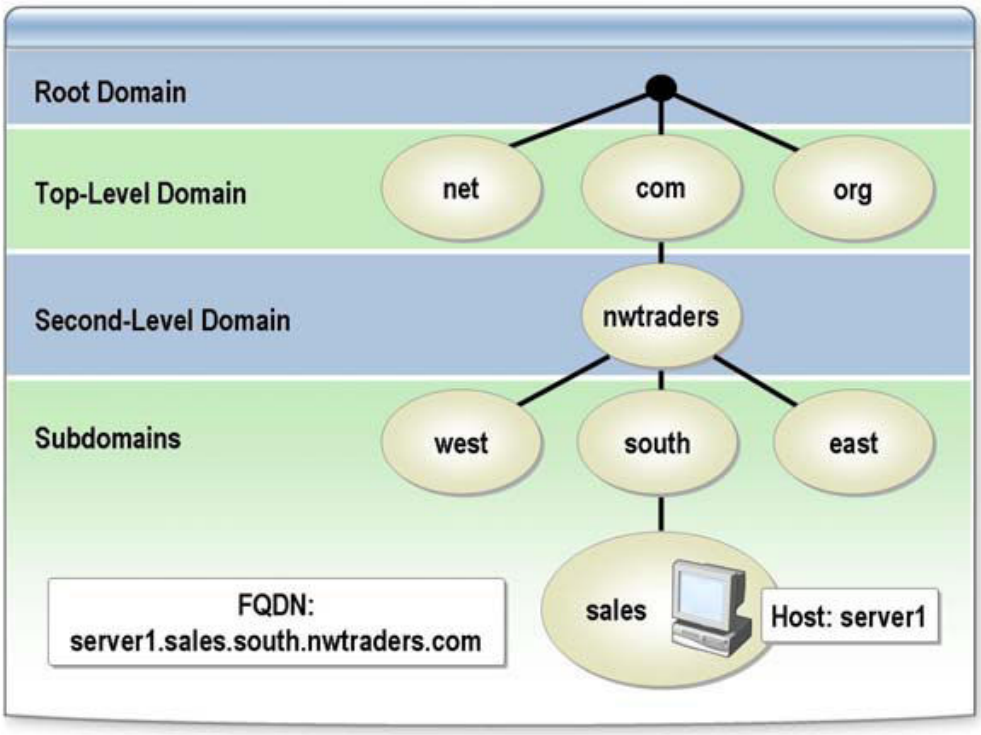

Figure 6. Tree structure of Domain namespace of Nwtraders Company [23]

Figure 6 shows the complete tree structure view of the domain namespace of a company named nwtraders.

6.1.2 DNS Server

The DNS server hosts records of a distributed DNS database and uses the records they host to resolve DNS name queries sent by DNS client computers, such as queries for the names of the Web sites or computers in a network or on the Internet. In order to establish the link between the domain names and IP addresses on a network, Domain Name Servers are needed. Every domain has its own domain name server, also called as primary domain name server, and secondary domain name server, which is used when primary domain

name server is unavailable. Primary and secondary domain name servers can be configured to use Forwarders and Root servers. [16,17]

a. Forwarders: Forwarders are the DNS servers which are used by the server to resolve DNS queries for records when the server cannot resolve. It helps to manage the name resolution for the names outside the network, such as the names on the Internet or names in other domains.

b. Root servers: Root server helps to find other DNS servers on the network. It resolves queries for zones that do not exist on the local DNS server. They are only used when Forwarders fail to respond and are not configured.

In the DNS, a DNS namespace can be divided into zones. The zones store name information about one or more DNS domains. The zone is the authoritative source of information for each DNS domain name included in a zone. A zone starts with a single DNS domain name. If other domains are added below the initial domain, these domains can either be part of the same zone or belong to another zone. Forward lookup zones provide name-to-address resolution service while reverse lookup zones they provide address-to-name resolution service. There are three DNS server services for zones. [23;27]

a. Primary zone: When a DNS server hosts a primary zone, it becomes the primary source of information about the zone. A master copy of the zone data in a local file is stored in the server.

b. Secondary zone: When a DNS server hosts a secondary zone, it becomes the secondary source of information about the zone. The zone at this server must be obtained from another remote DNS server computer that also hosts the same zone.

c. Stub zone: When a DNS server hosts a stub zone, it becomes the source only for information about the authoritative server for this zone. The zone for this server

must be obtained from another DNS server that hosts the zone. Generally, this DNS server has network access to the remote DNS server to copy authoritative name server information about the zone.

6.1.3 Resource Records

DNS is a distributed database containing records known as Resource Records (RR). RR contains the data associated with the domain names and their respective zones. Each RR specifies information about a particular object. For example: address mapping (A) records maps a host name to an IP address, and reverse-lookup pointer (PTR) records map an IP address to a host name. These records are used by the server to answer the queries for hosts in its zone. General RR information includes Domain name, Type (A, CNAME, HINFO, MX, NS, PTR, and SOA), Class and RDATA. [3,892;25]

6.1.4 Zone Delegation

When a portion of DNS namespace is designated for another zone, it is called Delegation. It provides the administrator a way to divide a namespace among multiple zones. For example: an administrator might place the goal.com domain in one zone and place example.goal.com subdomain in another delegated zone. If example.goal.com is not delegated, then goal.com will contain all the records for example subdomain. So through delegating, the goal.com zone contains only information for goal.com, as well as records to the authoritative name servers for example.goal.com zone. Any host entries for any machines in example.goal.com are contained only on the delegated server. The key benefits of zone delegation include the following: [28]

a. Zone delegation helps to delegate management part of the DNS namespace to other departments of locations.
b. Zone delegation helps to distribute a large DNS database across multiple servers for load balancing, faster name resolution, and increased performance.

c. Zone delegation is scalable with business needs. It helps to extend the name space for business expansion.

6.2 Practical Implementation

The project was carried without getting connected to the real world Internet and registering the domain name legally. For this project Microsoft Windows Server platform was used, which provided simple and detail stepwise information to configure the DNS server on the implemented network. The DNS server was installed on Host A and Host B on the topology. Simulating precisely with the real world ISP environment, where they are connected with many ISPs with different top level domains to provide Internet connection, two top-level domains, .fi on Host A and .com on Host B were used to provide Internet connection to the customer within those top level domains.

Forward lookup zones and Reverse lookup zones were configured to provide name-to-address resolution and address-to-name resolution on Host A and Host B respectively. Primary zones were configured with prayash.bakhati.fi and matti.puska.com domain names for providing primary source of information relating to the zone to the respective DNS server on Host A and Host B. FQDN was created on Host A and Host B DNS server to specify the exact location of the configured domain in the tree hierarchy of DNS. RR type A was created to match domain names to IP address on Host A and Host B DNS server.

For testing the name resolution under the same top-level domain but different second- level domain, a zone named testzone.fi was added under the forward lookup zone of Host A. RR type A was created to match the domain names to IP address.

In order to bind Host A and Host B DNS server together, Forwarder was configured. FQDN of Host A was placed on Host B and FQDN of Host B on Host A. Forwarder provided the DNS name resolution by forwarding queries to the DNS server on Host A and

Host B which were simulated on different network. Binding can also be done using Root server and forwarder.

```
C:\Users\Administrator.MYCOMPUTER.000>nslookup
Default Server:  mycomputer.prayash.bakhati.fi
Address:  172.16.10.1

> 172.16.10.13
Server:  mycomputer.prayash.bakhati.fi
Address:  172.16.10.1
Name:    www.testzone.fi
Address:  172.16.10.13

> 10.0.0.1
Server:  mycomputer.prayash.bakhati.fi
Address:  172.16.10.1
Name:    worktest.matti.puska.com
Address:  10.0.0.1

> www.matti.puska.com.
Server:  mycomputer.prayash.bakhati.fi
Address:  172.16.10.1
Name:    www.matti.puska.com
Address:  10.0.0.17

> www.testzone.fi.
Server:  mycomputer.prayash.bakhati.fi
Address:  172.16.10.1
Name:    www.testzone.fi
Address:  172.16.10.13

> worktest.matti.puska.com.
Server:  mycomputer.prayash.bakhati.fi
Address:  172.16.10.1
Name:    worktest.matti.puska.com
Address:  10.0.0.1
```

Figure 7. Nslookup output [Prayash Bakhati]

Figure 7 shows the result of Nslookup output. Nslookup helps to determine the corresponding IP address after entering the host name and vice versa.

7 Web Services

7.1 Theoretical Background

The Web Server is a computer program or computer running the program which uses Hypertext Transfer Protocol (HTTP) communication protocol, to deliver the content, such as web pages, over the Internet, intranets and extranets. The primary function of a web server is to deliver the web pages to the requesting clients. It includes the delivery of an HTML document and any other additional content such as images, style sheets and JavaScripts which are included in the document. A client's web browser initiates communication by making a request for a specific resource using HTTP and the server responds with the content of that resource or with an error message in case of unavailability. [29] The Web server uses different web server applications depending on the platforms to provide web services to Internet users such as Apache HTTP server and IIS.

The Web server has a huge impact over the Internet. It provides information to the users on the Internet, let the users download and upload their various contents with FTP or WWW, and helps to distribute the applications over the Internet easily instead of using physical media, such as floppy disks or CDs. It also proves to be significant for different customers in order to fulfill their different needs. For example:

a. Small business owners can provide information about their service and company by using a simple Web site.
b. Owners of a big or medium-size business can offer their goods and services through an online ordering system composed of various applications on a site.
c. Enterprise businesses can develop and provide business applications to employees over corporate intranets.
d. Hosting companies can provide individual customers with server space and services to host different online content and applications. [30]

IIS is web server application for Microsoft Windows server families. It provides integrated, reliable, scalable, secure and manageable web server capabilities over the Internet, intranets and extranets. It helps to create strong communication platform of dynamic network applications. Business companies and organizations of all sizes can use IIS to host and manage Web pages, FTP sites and route news or mail by using Network News Transport Protocol (NNTP) and the Simple Mail Transfer Protocol (SMTP) on the Internet or on their intranet. [30]

The Apache HTTP server and IIS are the two most used web servers. Apache server is more popular since it is freely available and supports multiple operating systems. The IIS is developed by Microsoft to provide their Windows operating system the ability to host Internet services, and supports only Microsoft Windows Operating System. Since the Windows operating system is prone to security risks because of its popularity, the IIS is not considered a secured web server. The IIS is popular only among Windows user. [31]

7.2 Practical Implementation

In this project, the Microsoft Windows Server platform was used to configure the Web server in Host A and Host B respectively. Since Microsoft Windows Server families used IIS as web server application to provide web service, the IIS was installed on both Hosts. A simple web page was created and was placed under domain name www.testzone.fi with the IP address of 172.16.10.13/16 to test the web service connection. The domain name was configured on the DNS server on Host A as RR type A under testzone.fi zone. The customer's workstation was used to browse and check the status of the configured web server since the project aimed to provide web service to the customer. Figure 8 was the result obtained using Internet Explorer browser to browse the webpage content using the domain name.

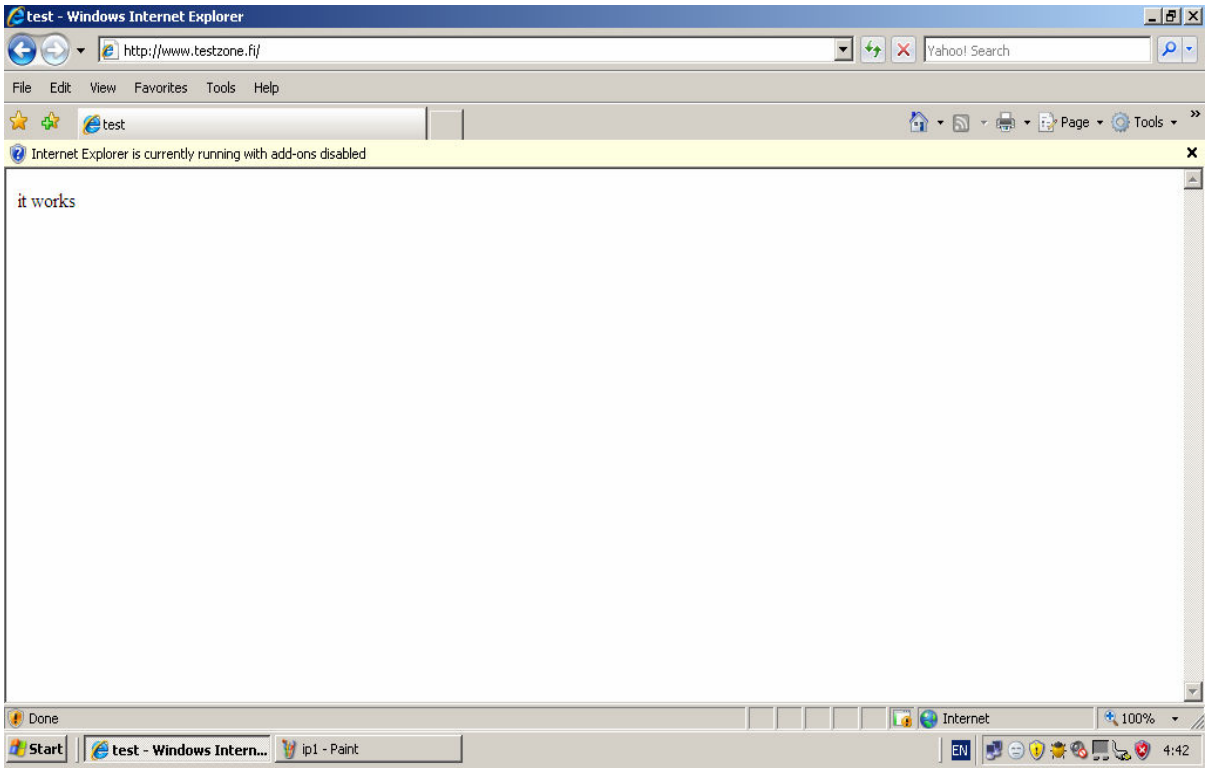

Figure 8. Using the domain name to browse the web page content

The figure 8 was the result of the successful configuration of the Web server on Host A which is being accessed from Host C (customer).

8 Support and Maintenance

Customers are the key elements to the ISP. In order to build a good relationship with the customer, ISP try to provide all possible support relating to any issues concerning the Internet connection, services and any new ISP products. Due to this reason all ISPs have their helpdesk for consulting and supporting customer issues. In the following are the typical helpdesk supports provided by an ISP to their customers:

a. Call support
b. Home support
c. Email support
d. CPE support
e. Online support
f. Helpdesk forum
g. Billing support

An ISP is built with networking equipment and services on it. A failure on any of them can cause interference on the whole network. In order to avoid any of those, ISP use different monitoring tools and services for maintenance and managing purposes. Those monitoring tools help an ISP to identify the malfunctioning equipment in ISP topology. All the equipment can be provided with different access services for maintenance purposes such as Telnet and Web interface. Since the networking equipment might reside on a different location, the ISP can easily perform maintenance on them using the access services remotely. From customers' prospective, the ISP can provide maintenance service to them by using the monitoring tools since they are capable of observing the customers' activities on the network.

There are various network monitoring tools which are used by the ISP, for example; NetDB, Net Detective, Network Bones, Network Management Software, StealthWatch and Castle Rock. The preferred and the most popular monitoring tools for the ISP is SNMP-supported monitoring tools, such as Castle Rock and NMS.

The Simple Network Management Protocol is an application-layer protocol and part of the TCP/IP suite used for exchanging management information between network devices. It helps the network administrators to manage network performance, find and solve network problems, and plan for network growth. [32] Managed devices, agents and Network Management Systems (NMSs) are the three key components of the SNMP managed network.

A managed device is a network node that contains an SNMP agent and resides on a managed network. It collects and stores management information and makes it available to NMSs using SNMP, for example; routers, switches or hubs. An agent is a network-management software module that resides on a managed device. An NMS executes applications that monitor and control managed devices. It provides the bulk of the processing and memory resources required for network management. It must exist on any managed network. In an SNMP-managed network, each management station or agent maintains a local database of information relevant to network management, known as MIB. [32]

An MIB is essentially a type of database which is used to manage devices in a communication networks. It contains a collection of objects in a database which are used to manage entities in a network, such as routers and switches. An MIB contains definitions and information regarding the properties of managed resources and the services which are supported by the agents. [32]

In this project, for maintenance and monitoring purposes, remote access services within the implemented network and a monitoring tool for observing the network and customer activity were used. The Remote access service included Telnet and Web interface. An ISP B router was configured to use the Telnet service and DSLAM to use the Web service for remote maintenance. The monitoring tool was Castle Rock, SNMPc Network Monitor evaluation version, which was downloaded from the Internet and implemented for testing

purposes. In order to analyze the generated and captured packets, software downloaded from Internet called Wireshark was used.

Castle Rock was installed and configured on Host B, and DSLAM was configured as an agent to provide information concerning the remote user. The basic configurations for forwarding the SNMP packets were configured on the ISP B router and switch respectively. The DSLAM supported MIB II RFC-1213 and RFC-1215 [11,16]. Despite flexibilities and features provided by SNMP, the project was bound to use only the features supported by the module of DSLAM, which consists of the basic features of SNMP such as Cold Start trap, Authentication Failure trap, Linkup trap, Link Down trap and Overheat trap. Figure 9 shows the MIB database about the Linkup trap supported by the DSLAM.

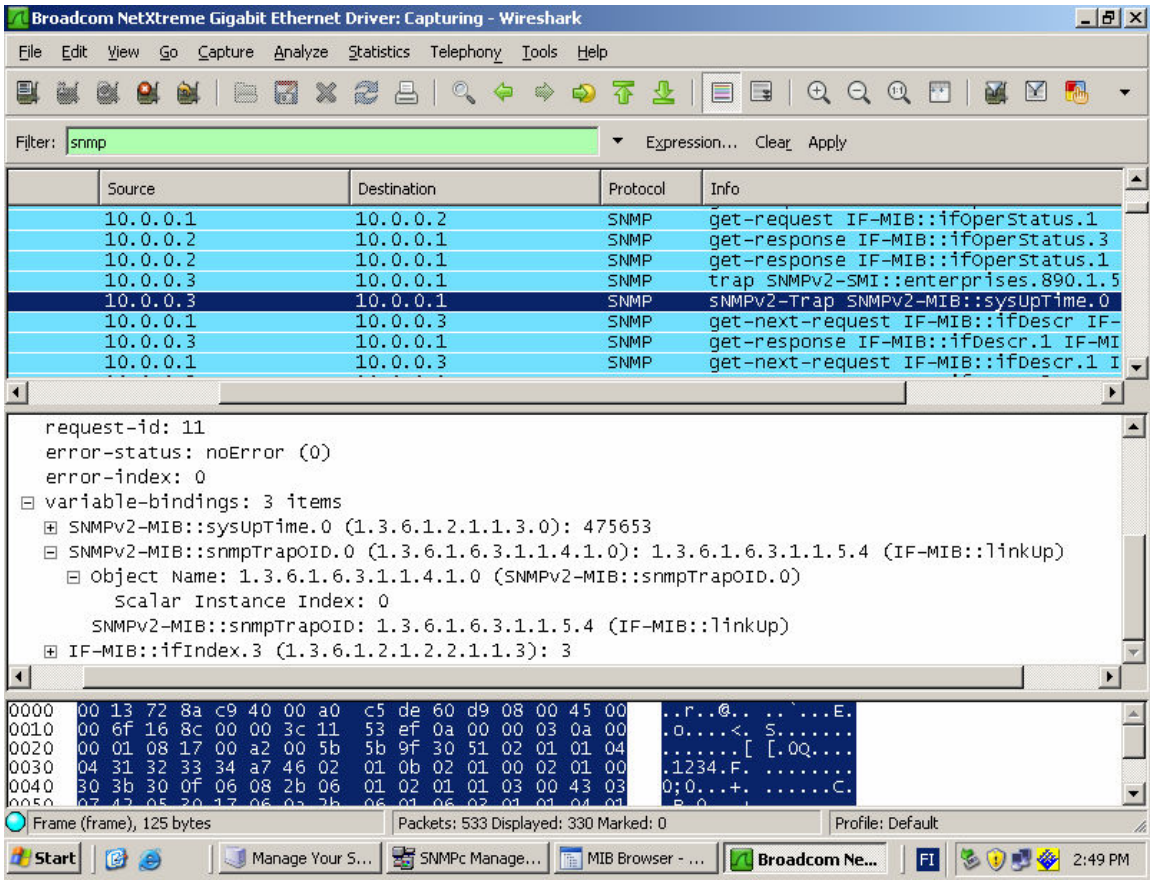

Figure 9. Linkup trap MIB database

ADSL Monitoring

The ADSL line connected from the ISP exchange equipment, i.e. DSLAM to ADSL CPE, can be monitored to obtain the line statistics. The line statistics can be a useful tool to aid troubleshooting ADSL problems and line faults. Generally DSLAM and ADSL CPE are responsible for providing the line statistics to the ISP and customer respectively. The measures from the line statistics can vary from the equipment vendors of DSLAM and ADSL CPE. However, the following are the typical measures which are provided by any vendors of the DSLAM and ADSL CPE. [33]

a. Bandwidth/synchronization rate: Shows the synchronization speed in which the ADSL CPE is connected to the DSLAM and vice versa. The rate can be defined by the ISP depending on the customer requirements.

b. Attenuation: Describes the reduction of the ADSL strength, which occurs over the distance and is measured in decibels (dB). The lower the figure the faster the connection, and vice versa. True line attenuation is measured by DSLAM at ISP. The ADSL CPE provides information about the attenuation, which is an average against all the frequencies that the CPE uses.

c. Signal to Noise Ratio (SNR): Is also measured in dB, which provides measurement concerning the signal strength to the level of noise on the line. The less the noise level is, the better the connection. The noise level can vary during any time of the day depending on the number of users over the line and the length of line.

d. Output Power: The amount of power transmitted from the DSLAM and ADSL CPE. The output power increases depending on the length of the line.

e. Line up time: Provides information concerning the time ADSL CPE has been connected to the DSLAM.

Line Mode	G.dmt	**Line State**	Show Time
Latency Type	Fast	**Line Up Time**	12:05:30:18
Line Coding	Trellis On	**Line Up Count**	1

Statistics	**Downstream**	**Upstream**
Line Rate	8128	832
Noise Margin	11.9 dB	9.0 dB
Line Attenuation	7.0 dB	7.0 dB
Output Power	11.9 dBm	15.8 dBm
K (number of bytes in DMT frame)	255	27
R (number of check bytes in RS code word)	0	0
S (RS code word size in DMT frame)	1	1
D (interleaver depth)	1	1
Super Frames	62152696	62152694
Super Frame Errors	99	177
RS Words	0	0
RS Correctable Errors	0	0
RS Uncorrectable Errors	0	0
HEC Errors	54	0
OCD Errors	4	0
LCD Errors	0	0
ES Errors	0	0

Figure 10. ADSL line statistics status using the voyager router [33]

Figure 10 shows a detailed view of the ADSL line statistics from the Voyager router, which is an ADSL CPE.

9 Conclusion

The use of Internet is indispensible in the modern society without which it can not move further. The role of the ISP is significant and unavoidable. The goals of the project were to deploy a small technical ISP environment with the basic services, solutions, equipment needed and obtain information about ADSL connection used by the customer to get the Internet connectivity.

The ISP infrastructure was built with minimum resources. The resources included networking equipment and the basics services such as DHCP, DNS, Web and IP routing which provided the required results needed by a small ISP to provided Internet service connection to the customer. ADSL bandwidth can be configured according to the customer need and ADSL CPE are needed to support the ADSL connection was the huge outcome concerned with the customer necessity. The ADSL line statistics can be obtained using the ADSL CPE which provided information needed for consistent performance of the line.

The project was carried just for educational purpose. Scalable solution, additional ISP services such as VoIP, Wireless connectivity, Billing and telephony services, business plan and any other commercial aspects were excluded from the project.

The outcome of the project was the demonstration of the real world ISP Environment for the general users about the internal structure of the ISP and working mechanism. The thesis is helpful for networking students and to all those who want to know about how the Internet Service Provider provides the Internet Service. Moreover, it helps to all administrators who have configured their DNS Server under Microsoft Windows Server to configure the DSLAM and speed of the connection of the Internet including the monitoring mechanism of the entire network.

References

1 Computer Network Hierarchy [online].
URL: http://computer.howstuffworks.com/Internet/basics/Internet-infrastructure1.htm. Accessed 1 June 2010

2 Private IP address [online].
URL: http://www.homenethelp.com/sharing/private-ip-address.asp.
Accessed 1 June 2010

3 Charles M.Kozierok. TCP/IP GUIDE. San Francisco, No Starch Press, Inc; 2005

4 Private and Public IP Addresses Explained [online].
URL: http://www.debianadmin.com/private-and-public-ip-addressesexplained.html.
Accessed 1 June 2010

5 What is IP routing? [online].
URL: http://www.metaswitch.com/ip-routing-unicast/what-is-ip-routing.aspx.
Accessed 18 March 2010

6 Problem: Directly Connected External BGP Neighbors Not Initializing [online].
URL: http://cisco.iphelp.ru/faq/5/ch15lev2sec2.html.
Accessed 6 June 2010

7 Autonomous System numbers - FAQs [online].
URL: http://www.apnic.net/services/services-apnic-provides/helpdesk/faqs/asn-faqs [online]. Accessed 3 June 2010

8 InetDaemon. Autonomous System [online].
URL: http://www.inetdaemon.com/tutorials/Internet/ip/routing/bgp/operation/autonomous_system.shtml. Accessed 16 March 2010

9 Removing Private Autonomous System Numbers in BGP [online].
URL: http://cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f27.shtml. Accessed 6 June 2010

10 ADSL Basics (DMT) [online].
URL: http://home.pacbell.net/bitrider/tb1000.pdf. Accessed 3 June 2010

11 Difference between DSL and ADSL [online].
URL: http://www.buzzle.com/articles/difference-between-dsl-and-adsl.html.
Accessed 4 March 2010

12 Networking Tips [online].
URL: http://www.computerfreetips.com/networking_tips/adsl.html.
Accessed 4 March 2010

13 ADSL_Tutorial.pdf [online].
URL: http://www.iol.unh.edu/services/testing/dsl/training/ADSL_Tutorial.pdf
Accessed 5 March 2010

14 ADSL [online].
URL: http://www.tradepage.co.za/adsl-faq.asp.
Accessed 6th March 2010

15 Service Level Agreement [online].
URL: http://searchitchannel.techtarget.com/sDefinition/0,,sid96_gci213586,00.html
Accessed 2 June 2010

16 Mr. Malcolm Tatum. What is DSLAM? [online].
URL: http://www.wisegeek.com/what-is-dslam.htm. Accessed 6th March 2010

17 DSLAM [online].
URL: http://searchtelecom.techtarget.com/sDefinition/0,,sid103_gci213916,00.html
Accessed 6 March 2010

18 ZyXel Communications Corp. IP Express User's Guide. Version 2.05 (DN.1), (DJ.1), (DD.0), 2004

19 DHCP [online].
URL: http://www.comptechdoc.org/independent/networking/guide/netdhcp.html.
Accessed 10 March 2010

20 DHCP [online].
URL: http://www.broadviewnetworks.ca/product-Microsoft+Windows+Server+
2003+Dynamic+Host+Configuration+Protocol.asp.
Accessed 11 March 2010

21 BGP [online].
URL: http://freesoft.org/CIE/Topics/88.htm. Accessed 18 March 2010

22 Cisco System. Border Gateway Protocol (BGP) [online].
URL:http://www.cisco.com/en/US/docs/Internetworking/technology/handbook/bgp.
html. Accessed 18 March 2010

23 Microsoft Training & Certification. Resolving Host Name by Using Domain Name System (DNS) [online].
URL: http://www.scribd.com/doc/6356625/DNS. Accessed 5April 2010

24 Kioskea Network. Domain Name System [online].
URL:http://en.kioskea.net/contents/Internet/dns.php3. Accessed 2 April 2010

25 DNS resource records [online].
URL:http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=/rzakk/rzakkconceptresourcerec.htm. Accessed 5 April 2010

26 DNS [online].
URL: http://www.preplogic.com/products/megaguides/samples/12413_83640_sample.pdf. Accessed 5 April 2010

27 Microsoft TechNet. Understanding Zones [online].
URL: http://technet.microsoft.com/en-us/library/cc725590.aspx.
Accessed 10 April 2010

28 Managing DNS [online].
URL: http://www.informit.com/articles/article.aspx?p=102158&seqNum=2.
Accessed 2 June 2010

29 Web server [online].
URL: http://en.wikipedia.org/wiki/Web_server. Accessed 20 May 2010

30 Microsoft Windows server 2008 x86 [Help and Support on DVD]. Enterprise edition .Washington USA, Microsoft Corporation, 2008

31 Difference-between-iis-and-apache [online].
URL: http://www.differencebetween.net/technology/difference-between-iis-an-apache/. Accessed 1 June 2010

32 SNMP_basics [online].
URL: http://www.pulsewan.com/data101/snmp_basics.htm, Accessed 2 June 2010

33 How to interpret your adsl Line Stats [online].
URL: http://www.kitz.co.uk/adsl/linestats.htm. Accessed 3 June 2010

Appendix 1: ISP A router configuration

ISP A Router

```
sh run
Building configuration...


Current configuration : 1106 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISPA
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
!
no ipv6 cef
multilink bundle-name authenticated
!
voice-card 0
 no dspfarm
!
!
archive
 log config
  hidekeys
!
!
!
```

```
interface FastEthernet0/0
 ip address 172.16.10.2 255.255.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.0.2 255.0.0.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.1.1 255.255.255.0
 clock rate 64000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router bgp 65222
 no synchronization
 bgp log-neighbor-changes
 network 172.16.0.0
 neighbor 192.168.1.2 remote-as 65123
 no auto-summary
!
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
line con 0
password cisco
login
line aux 0
line vty 0 4
password cisco
login

scheduler allocate 20000 1000
end


ISPA#sh bgp
BGP table version is 3, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```

```
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.0.0.0         192.168.1.2              0             0  65123i
*> 172.16.0.0       0.0.0.0                  0         32768 i

ISPA#sh ip int brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            172.16.10.2     YES NVRAM  up                    up

Serial0/0/0                192.168.1.1     YES NVRAM  up                    up

Serial0/0/1                unassigned      YES NVRAM  administratively down down

ISPA#
```

Appendix 2: DNS zone files

Workstation A

Forward lookup zone

```
;
;  Database file prayash.bakhati.fi.dns for prayash.bakhati.fi zone.
;      Zone version:  5
;

@                       IN  SOA mycomputer.prayash.bakhati.fi.
hostmaster.prayash.bakhati.fi. (
                              5            ; serial number
                              900          ; refresh
                              600          ; retry
                              86400        ; expire
                              3600       ) ; default TTL

;
;  Zone NS records
;

@                       NS    mycomputer.prayash.bakhati.fi.

;
;  Zone records
;

mycomputer              A     172.16.10.1
www                     A     172.16.10.15



;
;  Database file testzone.fi.dns for testzone.fi zone.
;      Zone version:  2
;

@                       IN  SOA mycomputer.prayash.bakhati.fi.
hostmaster.prayash.bakhati.fi. (
                              2            ; serial number
                              900          ; refresh
                              600          ; retry
                              86400        ; expire
                              3600       ) ; default TTL

;
;  Zone NS records
;

@                       NS    mycomputer.prayash.bakhati.fi.

;
;  Zone records
;

www                     A     172.16.10.13
```

Reverse lookup zone

```
;
;  Database file 10.16.172.in-addr.arpa.dns for 10.16.172.in-addr.arpa zone.
;      Zone version:  7
;

@                       IN  SOA mycomputer.prayash.bakhati.fi.
hostmaster.prayash.bakhati.fi. (
                            7           ; serial number
                            900         ; refresh
                            600         ; retry
                            86400       ; expire
                            3600      ) ; default TTL

;
;  Zone NS records
;

@                       NS    mycomputer.prayash.bakhati.fi.

;
;  Zone records
;

1                       PTR   mycomputer.prayash.bakhati.fi.
13                      PTR   www.testzone.fi.
15                      PTR   www.prayash.bakhati.fi.
```

Workstation B

Forward lookup zone

```
;
;  Database file matti.puska.com.dns for matti.puska.com zone.
;      Zone version:  6
;

@                         IN  SOA worktest.matti.puska.com.  hostmaster.matti.puska.com.
(
                            6           ; serial number
                            900         ; refresh
                            600         ; retry
                            86400       ; expire
                            3600      ) ; default TTL

;
;  Zone NS records
;

@                       NS    worktest.matti.puska.com.

;
;  Zone records
;

@                       A     10.0.0.13
worktest                A     10.0.0.1
www                     A     10.0.0.17
```

Reverse lookup zone

```
;
;  Database file 0.0.10.in-addr.arpa.dns for 0.0.10.in-addr.arpa zone.
;      Zone version:  4
;

@                       IN  SOA worktest.matti.puska.com.  hostmaster.matti.puska.com. (
                              4            ; serial number
                              900          ; refresh
                              600          ; retry
                              86400        ; expire
                              3600       ) ; default TTL

;
;  Zone NS records
;

@                       NS    worktest.matti.puska.com.

;
;  Zone records
;

1                       PTR   worktest.matti.puska.com.
13                      PTR   matti.puska.com.
17                      PTR   www.matti.puska.com.
```