American Journal of Networks and Communications
2013; 2(1) : 1-8
Published online February 20, 2013 (http://www.sciencepublishinggroup.com/j/ajnc)
doi: 10.11648/j.ajnc.20130201.11

Optimization of core network router for telecommunication exchange

Diponkar Paul*, Subrata Kumar Sarkar, Rajib Mondal

World University of Bangladesh

Email address:
dipo0001@ntu.edu.sg (D. Paul)

To cite this article:
Diponkar Paul, Subrata Kumar Sarkar, Rajib Mondal. Optimization of Core Network Router for Telecommunication Exchange, *American Journal of Networks and Communications*. Vol. 2, No. 1, 2013, pp. 1-8. doi: 10.11648/j.ajnc.20130201.11

Abstract: The operation of Core Router is to restrict Network Broadcast to the LAN, to act as default gateway, to move data between different networks and to advertise loop free Path. The technology of Wifi, WiMAX (Worldwide Interoperability for Microwave Access), GPRS (General Packet Radio Services), EDGE (Enhanced Data Rates For GSM Evolution), EV-DO (Evolution Data Optimized) which are used for remote data access. A Router must be able to support multiple telecommunications interfaces of the highest speed in use in the core Internet and must be able to forward IP packets at full speed on all of them. It must also support the routing protocols being used in the core. In telephone system, Core Routers installed on the network are used as carriers to carry data from traffic sources to sinks. The optimization formulation based on Telecommunication network to obtain an optimal decision for the Core Router on whether to accept packets from a traffic source. This decision is made to maximize the reward of data delivery while the quality-of-service performance is guaranteed. From the performance evaluation, a Core Router with network optimization can achieve the highest reward while the maximum packet-blocking probability requirements met. The Core Router is a cell-site access platform specifically designed to optimize, aggregate and transport mixed-generation Radio Access Network (RAN) traffic. It is used at a cell site as part of an IP-RAN or Cell Site DCN solution. An IP RAN solution in which the Core Router extends IP connectivity to the cell site and Base Transceiver Station (BTS), through a Fast Ethernet interface to the BTS, the router provides bandwidth-efficient IP transport of voice and data bearer traffic, as well as maintenance, control and signaling traffic over the IP using traditional circuits.

Keywords: IIG, DNS, Router

1. Introduction

A router is a device that forwards data packets between computer networks, creating an overlay internet work. A router is connected to two or more data lines from different networks. When a data packet comes in on one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table or routing policy, it directs the packets to the next network on its journey .Routers perform the "traffic directing" functions on the internet. A data packet is typically forwarded form one router to another through the networks that constitute the internet work until it gets to its destination node. The most familiar type of routers are home and small office routers that simply pass data, such as web pages and email, between the home computers and the owner's cable or DSL modem, which connects to the internet through an ISP. More sophisticated routers, such as enterprise routers, connect large business or ISP networks up to the powerful core routers that forward data at high speed along the optical fiber lines of the internet backbone. When multiple routers are used in interconnected network, the exchange information about destination addresses, using a dynamic routing protocol. Each router builds up a table listing the preferred routes between any two systems on the interconnected networks. A router has interfaces for different physical types of network connections (such as copper cables, fiber optic, or wireless transmission).It also contains firmware for different networking protocol standards. Each network interface uses this specialized computer software to enable data packets to be forwarded form one protocol transmission system to another. Routers may also be used connect two or more logical groups of computer devices known as subnets, each with a different subnetwork address. The subnets address recorded in the router do not necessarily map directly to the physical interface

connections. A router has to stages of operation called planes. A router records a routing table listing what routes should be used to forward a data packet, and through which physical interface connection. It does this using internal pre-configured address, called static routes. A typical home or small office router showing the ADSL telephone line and Ethernet network cable connections. The router forwards data packets between incoming and outgoing interface connections. It routes it to the correct network type using information that the packets header contains. It uses data recorded in the routing table control plane. Routers may provide connectivity within enterprises, between enterprises and the internet, and between internet service providers (ISP) networks. Smaller routers usually provide connectivity for typical home and office networks. Other networking solutions may be provided by a backbone wireless system (WDS), which avoids the costs of introducing networking cables into buildings. A screenshot of the luCI web interface used by open wrt. Access routers, including 'small office/home office'(SOHO) models, are located at customer sites such as branch offices that do not need hierarchical routing of there own. Typically, they are optimized for low cost. Some SOHO routers are capable of routing alternative free Linux-based firmwares like Tomato, Open Wrt or DD-WRT. Distribution routers aggregate traffic from multiple access routers, either at the same site, or to collect the data streams from multiple sites to a major enterprise location. Distribution routers are open responsible for enforcing quality of service across a WAN interface connections, and substantial onboard data processing routines [1]. They may also provide connectivity to groups of file servers or other external networks. External networks must be carefully considered as part of the overall security strategy. Separate from the router may be a firewall or VPN handling device, or the router may including Cisco systems 'PIX and ASA5500 series, junipers Net screen, Watch guard's Firebox, Barracuda's variety of mail-oriented devices, and many others. In enterprises, a core router may be provided a "collapsed backbone" interconnecting the distribution tier routers buildings of a campus, or large enterprise locations. They tend to be optimized for high bandwidth. Routers intended for ISP and major enterprise connectivity usually exchange routing information using the border gateway protocol (BGP).RFC 4098 standard defines the types of BGP-protocol routers according to the routers functions. Edge router also called a provider Edge router is placed at the edge of an ISP network. The router uses external BGP to EBGP protocol routers in other ISPs, or a large enterprise autonomous system. Subscriber edge router also called a customer Edge router, is located at the edge of the subscriber's network, it also uses EBGP protocol to its provider's autonomous system. It is typically used in an organization. Inter-provider border router. Interconnecting ISPs is a BGP-protocol router that maitains BGP session with other BGP protocol routers in ISP autonomous systems. A core router resides within an Autonomous System as a back bone to carry traffic between edge routers. In the ISPs Autonomous system, a router uses internal BGP protocol to communicate with other ISP edge routers, or the ISPs internet provider border routers. The internet no longer has a clearly identifiable backbone, unlike its predecessor networks. The major ISPs system routers make up what could be considered to be the current internet backbone core. ISPs operate all four types of the BGP-protocol routers described here. An ISP "core" router is used to interconnect its edge and border routers. Core routers may also have specialized functions in virtual private networks based on a combination of BGP and Multi protocol Label Switching protocols. Port forwarding Routers are also used for port forwarding between private internet connected servers [2]. Voice/Data/Fax/Video processing Routers Commonly referred to as access servers or gateways, these devices are used to route and process voice, data, video, and fax traffic on the internet .Since 2005,most long distance phone calls have been processed as IP traffic (VOIP) through a voice gateway. Voice traffic that the traditional cable networks once carried. Use of access server type routers expanded with the advent of the internet, first with dial up access, and another resurgence with voice phone service. Router is a kind of network equipment that connects many networks or network segments. A mobile network is composed of one or more routers and mobile or fixed nodes. All packets destined to or out of the mobile network should pass through the mobile router which manages the connectivity of the network. The mobile router can translate data and information between different networks or segments to make them understand each other[3]. The mobile router has the responsibility to manage the mobility of the whole network. While the mobile network moves, the mobile router has to find out the point of attachment and update the location information of every node which is attached to the mobile network. Generally connections of heterogeneous networks .The MWR 1941-DC Mobile Wireless Edge Router is a networking platform optimized for being used in mobile wireless networks. It is specifically designed to be used at the cell site edge as a part of an IP Radio Access Network (IPRAN) or Cell Site Data Communications Network (DCN).It offers high performance at a low cost while meeting the critical requirements for deployment in cell sites, including small size, high availability, and DC input power flexibility. Further more it can generate revenue from new cell-site IP-based services and enable rapid deployment of next-generation mobile services. The router comprises high-performance architecture, driven by a powerful MIPS RISC processor coupled with an optional ATM network processing engine. The Cisco MWR-1941-DC- provides Abis Optimization as part of CDMA 1xRTT IP RAN or Cell Site DCN solution. In an IP RAN solution, the MWR 1941-DC extends IP connectivity to the cell site and Base Transceiver Station (BTS). Through a Fast Ethernet interface to the BTS, the router provides bandwidth-efficient IP transport of voice and data bearer traffic, as well as main-

tenance, control, and signaling traffic over IP using the leased line or backhaul network. The router also supports standards-based Internet Engineering Task Force (IETF) Internet protocols over the RAN transport network. In computer networking, a gateway is a router on a TCP/IP network that serves as an access point to another network. A default gateway is the node on the computer network that the network software uses when an IP address does not match any other routes in the routing table. In home computing configurations, an ISP often provides a physical device which both connects local hardware to the Internet and serves as a gateway. In organizational systems a gateway is a node that routes the traffic from a workstation to another network segment. The default gateway commonly connects the internal networks and the outside network (Internet). In such a situation, the gateway node could also act as a proxy server and a firewall. The gateway is also associated with both a router, which uses headers and forwarding tables to determine where packets are sent, and a switch, which provides the actual path for the packet in and out of the gateway. In other words, a default gateway provides an entry point and an exit point in a network.

2. Methodology

The Internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail.

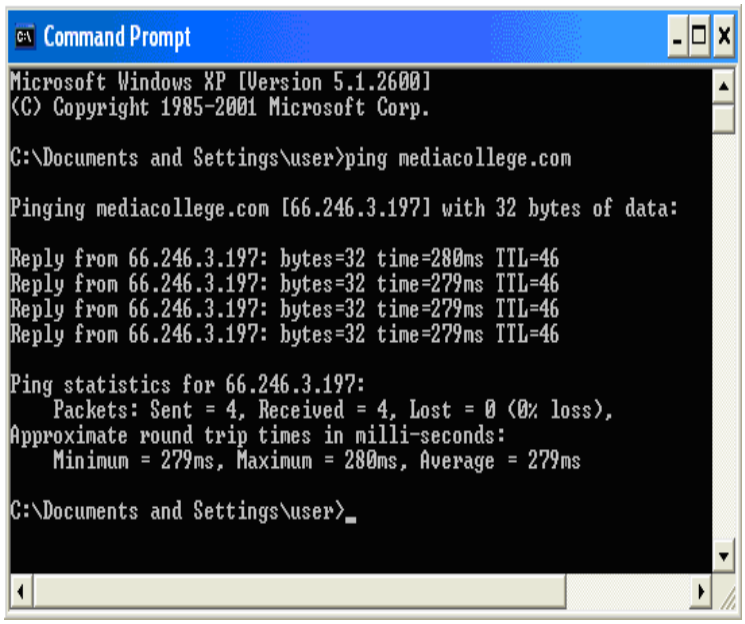
A firewall can either be software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A network's firewall builds a brigade between an internal network that is assumed to be secure and trusted, and another network, usually an external (inter)network, such as the Internet, that is not assumed to be secure and trusted. A fiber media converter is a simple networking device that makes it possible to connect two dissimilar media types such as twisted pair with fiber optic cabling. MRTG is free software for monitoring and measuring the traffic load on networks links [3] It allows the user to see traffic load on a network over time in graphical form. MRTG uses the Simple Network Management Protocol (SNMP) to send requests with two object identifiers (OIDs) to a device. The device, which must be SNMP-enabled, will have a management information base (MIB) to look up the OIDs specified. After collecting the information it will send back the raw data encapsulated in an SNMP protocol. MRTG records this data in a log on the client along with previously recorded data for the device. The software then creates an HTML document from the logs, containing a list of graphs detailing traffic for the selected device.

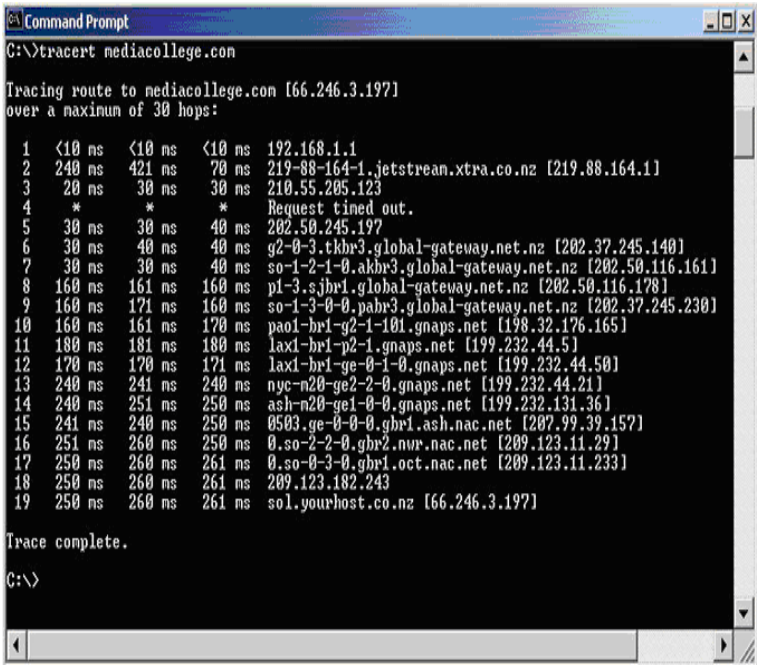
Ping is a computer network administration utility used to test the reach ability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer. Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response. In the process it measures the time from transmission to reception (round-trip time) and records any packet loss [4]. The results of the test are printed in the form of a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times, and sometimes the standard deviation of the mean. The Ping process are given bellow the source host generates an ICMP protocol data unit. The ICMP PDU is encapsulated in an IP datagram, with the source and destination IP addresses in the IP header. At this point the datagram is most properly referred to as an ICMP ECHO datagram, but we will call it an IP datagram from here on since that's what it looks like to the networks it is sent over. The source host notes the local time on its clock as it transmits the IP datagram towards the destination. Each host that receives the IP datagram checks the destination address to see if it matches their own address or is the all hosts address (all 1's in the host field of the IP address).If the destination IP address in the IP datagram does not match the local host's address, the IP datagram is forwarded to the network where the IP address resides. The destination host receives the IP datagram, finds a match between itself and the destination address in the IP datagram. The destination host notes the ICMP ECHO information in the IP datagram performs any necessary work then destroys the original IP/ICMP ECHO datagram. The destination host creates an ICMP ECHO REPLY, encapsulates it in an IP datagram placing it's own IP.

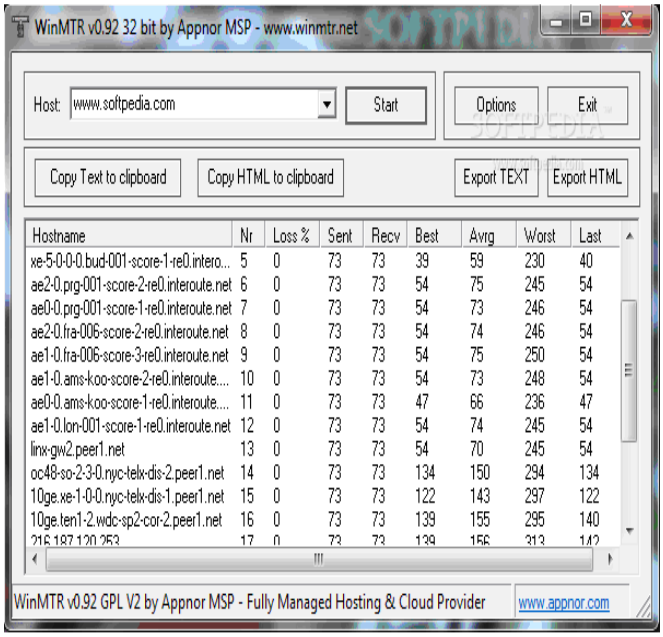
Address in the source IP address field, and the original sender's IP address in the destination field of the IP datagram. The new IP datagram is routed back to the originator of the PING. The host receives it, notes the time on the clock and finally prints PING output information, including the elapsed time. The process above is repeated until all requested ICMP ECHO packets have been sent and their responses have been received or the default 2-second timeout expired. The default 2-second timeout is local to the host initiating the PING and is NOT the Time-To-Live value in the datagram. This error message indicates that the requested host name cannot be resolved to its IP address; check that the name is entered correctly and that the DNS servers can resolve it.

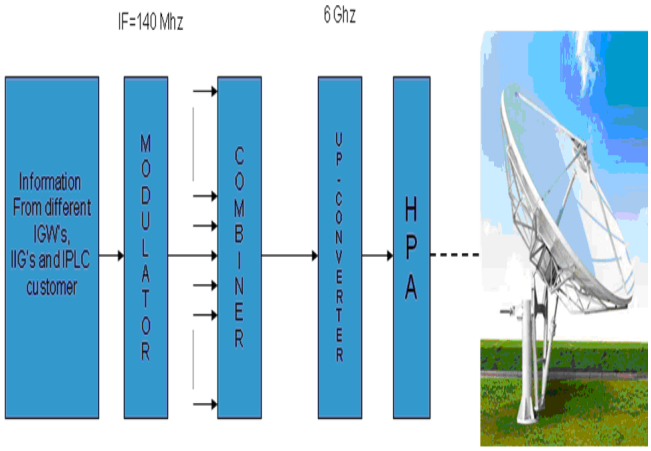
Trace route is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. MTR (My

trace route, originally called Matt's trace route) is computer software which combines the functionality of the trace route and ping programs in a single network diagnostic tool. MTR probes routers on the route path by limiting the number of hops individual packets may traverse, and listening to responses of their expiry. It will regularly repeat this process, usually once per second, and keep track of the response times of the hops along the path.







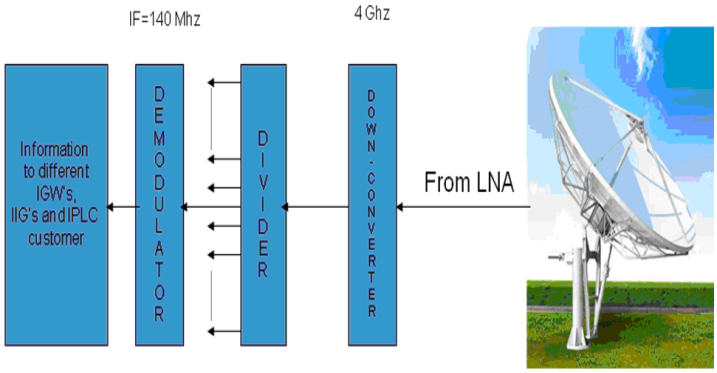


The Internet work Protocol identifies hosts with a 32-bit number called IP address or a host address. To avoid confusion with MAC addresses, which are machine or station addresses, the term IP address, will be used to designate this kind of address. IP addresses are written as four dot-separated decimal numbers between 0-255.IP addresses must be unique among all connected machines (are any hosts that you can get over a network or connected set of networks, including your local area network, remote offices joined by the company's wide-area network, or even the entire Internet community).The Internet Protocol moves data between the hosts in the form of datagram's. Each datagram is delivered to the address contained in the destination address of the datagram's header. The Destination Address is a standard 32-bit IP address that contains sufficient information to uniquely identify a network and a specific host on that network [8]. If your network is connected to the Internet, you have to get a range of IP addresses assigned to your machines through a central network administration authority. The IP address uniqueness requirement differs from the MAC addresses. IP addresses are unique only on connected networks, but machine MAC addresses are unique in the world, independent of any connectivity. Part of the reason for the difference in the uniqueness requirement is that IP addresses are 32-bits, while MAC addresses are 48-bits, so mapping every possible MAC address into an IP address requires some overlap. Of course, not every machine on an Ethernet is running IP protocols, so the many-to-one mapping isn't as bad as the numbers might indicate. There are a variety of reasons why the IP address is only 32 bits, while the MAC address is 48 bits, most of which are historical. Since the network and data link layer use different addressing schemes, some system is needed to convert or map the IP addresses to the MAC addresses.[9] Transport-layer services and user processes use IP addresses to identify hosts, but packets that go out on the network need MAC addresses. The Address Resolution Protocol (ARP) is used to convert the 32-bit IP address of a host into its 48-bit MAC address. When a host wants to map an IP address to a MAC address, it broadcasts an ARP request on the network, asking for the host using the IP address to respond. The host that sees its own IP addresses

in the request returns its MAC address to the sender. With a MAC address, the sending host can transmit a packet on the Ethernet and know that the receiving host will recognize it. The standard structure of an IP address can be locally modified by using host address bits as additional network address bits. Essentially, the dividing line between network address bits and host bits is moved, creating additional networks [5], but reducing the maximum number of hosts that can belong to each network. These newly designed network bits define a network within the larger network, called a subnet. Sub netting allows decentralized management of host addressing. With the standard addressing scheme, a single administrator is responsible for managing host addresses for the entire network. By sub netting, the administrator can delegate address assignment to smaller organizations within the overall organization. Sub netting can also be used to overcome hardware differences and distance limitations. IP routers can link dissimilar physical networks together, but only if each physical network has its own unique network address. Sub netting divides a single network address into many unique subnet addresses, so that each physical network can have its own unique address. A subnet is defined by applying a bit mask, the subnet mask, to the IP address. If a bit is on the mask, that equivalent bit in the address is interpreted as a network bit. If the bit in the mask is off, the bit belongs to the host part of the address. The subnet is only known locally. To the rest of the Internet, the address is still interpreted as a standard IP address. The IP address and the routing table direct a datagram to a specific physical network, but when the data travels across a network, it must obey the physical layer protocol used by that network. The physical networks that underlay the TCP/IP network do not understand IP addressing. Physical networks have their own addressing schemes and there are as many different addressing schemes as there are different types of physical networks. One task of the network access protocols is to map IP addresses to physical network addresses. In figure, when an ARP request is sent, all fields in the layout are used except the Recipient Hardware Address (which the request is trying to identify). In an ARP reply, all the fields are used. The fields in the ARP request and reply can have several values. The ARP software maintains a table of translations between IP addresses and Ethernet addresses. This table is built dynamically. When ARP receives a request to translate an IP address, it checks for the address in its table. If the address is found, it returns the Ethernet address in its table. If the address is not found in the table, ARP broadcast a packet to every host on the Ethernet. The packet contains the IP address for which an Ethernet address is sought. If a receiving host identifies the IP address as its own, it responds by sending its Ethernet address back to the requesting host. The response is then cached in the ARP table [7]. The arp -a command display all the contents of the ARP table. It is a distributed database system that doesn't bog down as the database grows. It guarantees that new host information will be disseminated to the rest of the network as it is needed to those who are interested. If a DNS server receives a request for information about a host for which it has no information, it passes on the request to an authoritative server (is any server responsible for maintaining accurate information about the domain which is being queried). When the authoritative server answers, the local server saves (caches) the answer for future use. The next time the local server receives a request for this information, it answers the request itself [6]. The ability to control host information from an authoritative source and to automatically disseminate accurate information makes DNS superior to the host table, even for small networks not connected to the Internet. We see that at first telephone call from user Telephone set gp to the Local Exchange (LE). Local Exchange than pass to the call TANDEM.TANDEM is the central switch of all Local Exchange. TANDEM than just pass to the call TAX. TAX is located in the big city. If the call is local tax than pass to the call to the TANDEM and if the call is international TAX than pass to the call International Gateway (IGW).The international call from IGW is passed by Satellite Earth Station or Submarine Cable. The bellow Figure illustrated how to International call exchange by Submarine Cable: As defined in the national telecommunications policy 1998 and international long distance telecommunications services (ILDTS) policy 2007, all mobile operators is to interconnect through Interconnection Exchange (ICX) s and all international calls to be handled by International Gateway (IGW) which is to be connected to the mobile and fixed operators through the ICXs. The Interconnection Exchange (ICX) will receive all calls from the mobile and fixed operators whenever the call is made to other network and will pass it to the destination network if the call is local, and will pass to the IGWs if the call is international. ICX will also deliver calls received from IGWs where the call is destined. Below illustrate the structure of interconnection between different interfaces. South East Asia –Middle East – Western Europe (SEA-ME –WE 4) is an optical fiber submarine communications cable system that carries telecommunications between Singapore , Malaysia, Thailand, Bangladesh ,India , Sri Lanka , Pakistan, United Arab Emirates, Saudi Arabia, Sudan, Egypt, Italy, Tunisia, Algeria and France. The cable is approximately 18,800Km long, and provides the primary internet backbone between South East Asia, the Indian subcontinent, the Middle East and Europe. SEA-ME-WE 4 are used to carry telephone, internet, multimedia and various broadband data applications. The SEA-ME-WE 3 and the SEA-ME-WE 4 cable systems are intended to provide redundancy for each other .The two cable systems are complementary, but separate , and 4 is not intended to replace 3. SEA-ME-WE 3 are far longer at 39,000 km (compare to SEA-ME –WE 4's 18,800km) and extend from Japan and Australia along the bottom of the Eurasian landmass to Ireland and Germany. SEA-ME-WE 4 has a faster rate of data transmission at 1.28 Tbit/s against SEA-ME-WE 3'S 0.96 Tbit/s. SEA-ME-WE 3 provides

connectivity to a greater number of countries over a greater distance, but SEA-ME-WE 4 provides far higher data transmission speeds intended to accommodate increasing demand for high speed internet access in developing countries. The cable uses dense wavelength – division multiplexing (DWDM), allowing for increased communications capacity per fiber and also facilitates bidirectional communication within a single fiber. DWDM does this by multiplexing different wavelengths of laser light on a single optical fiber. Two fiber pair able to carry 64 carriers at 10 Gbit/s each. This enables Terabit per second speeds along the SEA-ME-WE 4 cable, with a total capacity of 1.28 Tbit/s. While the ISDN TDM switching feature can switch any type of traffic, the main application for the feature is video traffic. This scenario, which was tested for this document, uses ISDN video endpoints for TDM switching. The ISDN PRI to the ISDN network uses E1 interface 0/0/0 with the configuration of 10 B channels. The video endpoints use EM-4BRI-NT/TE BRI interfaces on an EVM-HD-8FXS/DID, slots 2/0/16, 2/0/17, and 2/0/18.The EVM-HD has a 50-way amphenol Champ RJ-21 connector. The connector connects to a Black Box JPM2194A special patch panel. A male-to-female 50-way cable connects the EVM ports to the patch pane [6]. When we have to connect two switches then we make TG or TGs between them. TG contains 5E1s then there will be total of 160(32*5) circuits between these two switches. One more important thing, when we connect two switches then we have to make at least 2 Signaling Links between them. Signaling Link will be always made on a 16th circuit of an E1.In above example we have total 5 E1s, so we will use 16th circuit of any two E1s for making two Signaling Links. In these two E1s we will be able to use 30 circuits of each E1 for voice & data. But in remaining 3 E1s we won't use 16th circuit for Signaling & we will have 31 circuits for carrying voice & data. Synchronization will be done for each E1 so 0th interval will be used in all the 5E1s.Maximum 16 Signaling Links can be made between two switches. Digital Circuit Multiplication Equipment (DCME) performs voice compression over TDM and IP networks to reduce bandwidth requirements for microwave, wire line and costly satellite links by up to 16:1, without causing degradation in voice quality. DCME voice trunking gateways employ voice detection and silence suppression techniques to enable enterprises, cellular operators and carriers to cut operating costs and open up more lines of communications using existing bandwidth capacity.

3. Receive Path



3.1. Compression Equipment

- Digital circuit multiplication equipment (DCME).
- Low Rate Encoder (LRE).

3.2. Advantages

The advantages of satellite communication over terrestrial communication are:

- The coverage area of a satellite greatly exceeds that of a terrestrial system.
- Transmission cost of a satellite is independent of the distance from the center of the coverage area.
- Satellite to Satellite communication is very precise.
- Higher Bandwidths are available for use.

3.3. Disadvantages

The disadvantages of satellite communication:

- Launching satellites into orbit is costly.
- Satellite bandwidth is gradually becoming used up.
- There is a larger propagation delay in satellite communication than in terrestrial communication. A network with three Routers and three hosts, connected to the Internet through Router1.

Hosts and addresses:

- PC1 10.1.1.100, default gateway 10.1.1.1
- PC2 172.16.1.100, default gateway 172.16.1.1
- PC3 192.168.1.100, default gateway 192.168.1.96

Router1:

Interface 1 5.5.5.2 (public ip)

- Interface 2 10.1.1.1

Router2:

- Interface 1 10.1.1.2
- Interface 2 172.16.1.1

Router3:

- Interface 1 10.1.1.3
- Interface 2 192.168.1.96

Network mask in all networks: 255.255.255.0 (/24 in CIDR notation).

If the routers do not use a Routing Information Protocol to discover which network each router is connected to, then the routing table of each router must be set up.

Router 1

Network ID	Network mask	Gateway	Interface (examples; may vary)	Cost (decreases the TTL)
0.0.0.0 (default route)	0.0.0.0	Assigned by ISP (e.g. 5.5.5.1)	eth0 (Ethernet 1st adapter)	10
10.1.1.0	255.255.255.0	10.1.1.1	eth1 (Ethernet 2nd adapter)	10
172.16.1.0	255.255.255.0	10.1.1.2	eth1 (Ethernet 2nd adapter)	10
192.168.1.0	255.255.255.0	10.1.1.3	eth1 (Ethernet 2nd adapter)	10

Router 2

Network ID	Network mask	Gateway	Interface (examples; may vary)	Cost (decreases the TTL)
0.0.0.0 (default route)	0.0.0.0	10.1.1.1	eth0 (Ethernet 1st adapter)	10
172.16.1.0	255.255.255.0	172.16.1.1	eth1 (Ethernet 2nd adapter)	10

Router 3

Network ID	Network mask	Gateway	Interface (examples; may vary)	Cost (decreases the TTL)
0.0.0.0 (default route)	0.0.0.0	10.1.1.1	eth0 (Ethernet 1st adapter)	10
192.168.1.0	255.255.255.0	192.168.1.96	eth1 (Ethernet 2nd adapter)	10

Router2 manages its attached networks and default gateway, router 3 does the same, router 1 manages all routes within the internal networks. Accessing internal resources If PC2 (172.16.1.100) needs to access PC3 (192.168.1.100), since PC2 has no route to 192.168.1.100 it will send packets for PC3 to its default gateway (router2). Router2 also has no route to PC3, and it will forward the packets to its default gateway (router1). Router1 has a route for this network (192.168.1.0/24) so router1 will forward the packets to router3, which will deliver the packets to PC3; reply packets will follow the same route to PC2.Accessing external resources If any of the computers try to access a webpage on the Internet, like http://en.wikipedia.org/, the destination will first be resolved to an IP address by using DNS-resolving. The IP-address could be 91.198.174.2. Here none of the internal routers know the route to that host, so they will forward the packet through router1's gateway or default route. Every router on the packet's way to the destination will check whether the packet's destination IP-address matches any known network routes. If a router finds a match, it will forward the packet through that route but if not, it will send the packet to its own default gateway. Each router encountered on the way will store the packet ID and where it came from so that it can pass the request back to previous sender. The packet contains source and destination, not all router hops. At last the packet will arrive back to router1, which will check for matching packet ID and route it accordingly through router2 or router3 or directly to PC1 (which was connected in the same network segment as router1.

4. Conclusion

The Core Network Router is very essential for maintenance of Telephone Exchange System. Routing information is exchanged only upon the establishment of new neighbor adjacencies. To find a solution to the simultaneous routing, frequency planning and power allocation problem in a telecommunication network with fixed relay infrastructure and conclude that the major benefit of relays is to make the system more equitable while extending coverage. By using the Core Router, operators can simplify and optimize their current network with a compact, high-performance, and modular cell-site access platform, reduce operating costs and enhance profit opportunities. This report can be a guideline for proper operation, maintenance, monitoring and troubleshooting of Telecommunication Network System.

References

[1] I. Mohammad, and M. Imad, Handbook of Sensor Networks, CRC Press, London, 2005.

[2] Jun-Zhao, "Mobile ad hoc networking: an essential technology for pervasive computing", International Conferences on Info-tech and Info-net, Proceedings, 2001, pp. 316-321.

[3] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy- efficient communication protocol for wireless microsensor networks", Proc. 33rd Hawaii Int. Conf. Syst. Sci. (HICSS'00), 2000. http://wwl.microchip.com/downloads/en/devicedoc/41211b.pdf, Microchip Technology Incorporated, 2006. http://www.labcenter.co.uk, Labcenter electronics, 2006.

[4] Suri, S., Waldvogel, M., Warkhede, P.R.: Profile-Based Routing: A New Framework for MPLS Traffic Engineering. In: Quality of Future Internet Services. LNCS, vol. 2156, Springer Verlag, Heidelberg (2001).

[5] Yilmaz, S., Matta, I.: On the Scalability-Performance Tradeoffs in MPLS and IP Routing. In: Proceedings of SPIE ITCOM (May (2002).

[6] Ott, T., Bogovic, T., Carpenter, T., Krishnan, K.R., Shallcross, D.: Algorithms for Flow Allocation for Multi Protocol Label Switching. MPLS International Conference (October 2000).

American Journal of Networks and Communications
2013; 2(1) : 1-8
Published online February 20, 2013 (http://www.sciencepublishinggroup.com/j/ajnc)
doi: 10.11648/j.ajnc.20130201.11