

**Table of Contents**

Table of Contents .....	1
Task 1 .....	7
Introduction .....	7
WAN Technologies .....	8
Dialup .....	8
Benefits .....	9
Demerits .....	9
Broadband .....	9
DSL (Digital Subscriber Line) .....	10
ADSL (Asymmetric Digital Subscriber Line) .....	10
Benefits .....	10
Drawbacks .....	11
SDSL (Symmetric Digital Subscriber Line) .....	11
Benefits of Broadband WAN technology .....	12
Drawbacks of Broadband WAN technology .....	12
Frame Relay .....	12
Benefits .....	13
Drawbacks .....	13
ISDN (Integrated Services Digital Network) .....	13
Benefits of ISDN .....	14
Drawbacks of ISDN .....	14
MPLS (Multiprotocol Layer Switching) .....	14
Benefits of MPLS .....	15
Drawbacks .....	15
Routing Protocols .....	15
Dynamic Routing .....	16

Interior Routing Protocols.....	16
RIP.....	17
OSPF .....	17
Exterior Routing.....	17
EGP (Exterior Gateway Protocol).....	18
BGP (Border Gateway Protocol) .....	18
Benefits of Dynamic Routing.....	19
Drawbacks of Dynamic Routing.....	19
Static Routing.....	19
Benefits.....	19
Drawbacks.....	19
Summary .....	19
References.....	21
Task 2.....	23
Introduction.....	23
Quality of Service Management .....	23
QoS Concepts.....	23
Benefits of QoS .....	24
Type of Service (TOS).....	24
IP precedence .....	25
DSCP (Differentiated Services Code Point) .....	25
Queues.....	26
First in First out (FIFO) mechanism .....	26
Benefits.....	27
Drawbacks.....	27
WFQ queuing mechanism.....	27
Benefits.....	27

Drawbacks .....	27
Rules Base .....	27
Congestion Management.....	28
Quality of Service Need.....	28
Voice over IP (VoIP).....	28
Video .....	29
Interactive Video .....	29
Streaming Video.....	29
Conclusion .....	29
References.....	30
Task 3 [1.3] .....	31
Introduction.....	31
MD5 (Message Digest Algorithm 5) .....	31
Authentication Protocol.....	32
PAP (Password Authentication Protocol) .....	32
CHAP (Challenge Handshake Authentication Protocol) .....	33
Broadcast Reduction .....	33
Firewalls.....	34
Access Control Lists .....	35
Tunneling .....	36
Recommendation .....	36
Task 4.....	37
Introduction.....	37
Trust of Intermediary System .....	37
Trust of Remote System.....	37
Trust of Network WAN .....	37
Authentication, Authorization and Accounting (AAA) Protocol.....	38

Secure Sockets Layer (SSL) Certificate .....	38
Point-to-Point Protocol (PPP) Authentication.....	38
Conclusion .....	39
References .....	40
Task 5.....	41
Introduction.....	41
WAN Infrastructure Design .....	41
Technologies .....	42
DHCP .....	42
Role in Proposed System.....	42
VLANs .....	42
Connection .....	43
Routing Concepts .....	43
Frame Relay .....	43
Device Selection .....	44
Router .....	44
Cisco 2951 Router.....	44
Features .....	44
Switch: Cisco WS-C2960X-24PD-L .....	45
Features .....	45
Firewall: Cisco 5505 .....	46
Features .....	46
Wireless Access Points: Aironet® 3600 Series Access Point.....	46
Cable Connection .....	47
IP Addressing Plan.....	47
Head Office .....	47
Branch Office Siraha.....	48

Branch Office Pokhara .....	48
Branch Office Hetauda .....	49
Branch Office Nepalgunj .....	49
Bandwidth .....	49
Speed Plan for User .....	49
User .....	50
Overall Justification of Proposed Design .....	50
References .....	51
Task 7 .....	52
Introduction .....	52
Body .....	52
Conclusion .....	53
Testing of WAN System .....	54
Test Log .....	54
Analyzing Test results .....	58
Task 8 .....	59
Introduction .....	59
Network monitoring .....	59
NetQoS .....	59
Latency Monitor .....	60
Performance Monitor .....	60
Solar wind Monitoring .....	60
All Details .....	61
Bandwidth monitor .....	61
Advanced IP Scanner .....	62
Resolving identified Issues .....	62
Packet Loss .....	62

Connection with HR VLAN broken.....	63
Task 9.....	64
Introduction.....	64
Network Monitoring Tools .....	64
Benefits of Network monitoring of Everest network .....	64
Traffic Analysis .....	65
Benefits of Traffic analysis of Everest network.....	65
Bandwidth Monitoring.....	66
WAN Optimization.....	66
Benefits of WAN optimization in Everest network .....	66
Checking Rules .....	67
Conclusion .....	67
References.....	68

**Task 1**

**Critically** evaluate different WAN Technologies. [1.1, M1]

**Introduction**

For the improvement of vast associations/workplaces, online administrations or other worldwide application, just LAN is not adequate to meet its business necessity, therefore WAN innovations are utilized as a part of huge business workplaces/association. Woodcock (n.d.) clarifies, WAN is fundamentally characterized as a system that covers substantial land zone to associate with LAN. According to Technopedia (n.d.) a wide range system (WAN) is a system that exists over a vast scale topographical region. A WAN join distinctive littler systems, including neighborhood (LAN) and metro zone systems (MAN). This guarantees PCs and clients in one area can speak with PCs and clients in different areas. WAN usage should be possible either with the assistance of the general population transmission framework or a private system. WAN (Wide Area Network) systems are often built up by looking for assistance from telecomm offices who give the facility of rented lines. The biggest WAN on the planet is the Internet, which can in some cases be alluded to as the cloud.

WANs can be utilized for any information sharing reason for which LANs can be utilized. In spite of the fact that WANs fill a need like that of neighborhood (LANs), WANs are organized and worked in a different way. The client of a WAN more often than not does not claim the correspondences lines that associate the remote PC frameworks; rather, the client subscribes to an administration through an information transfers supplier, INC (n.d.). Slower transmission speeds, be that as it may, may make a few applications less pragmatic for WANs. This document critically evaluates different WAN innovations over the year while signifying their importance and Drawbacks.

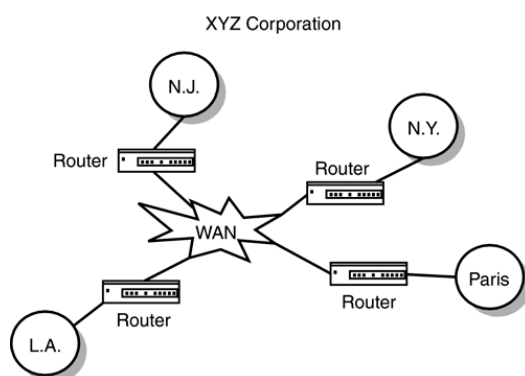


Figure 1 Basic WAN Structure (Source: <http://flylib.com/books/3/330/1/html/2/files/03fig04.gif>)

## WAN Technologies

WANs have existed for a considerable length of time, however new advances, administrations, and applications have created throughout the years to drastically expand their practicality for industry (REFERENCEFORBUSINESS, n.d.). WANs were initially produced for computerized rented line administrations conveying just voice, instead of information. In that capacity, they joined the private branch trades (PBXs) of remote workplaces of the same organization. WANs are still utilized for voice administrations, yet today they are utilized all the more often for information and picture transmission, (for example, video conferencing). These included applications have impelled noteworthy development in WAN use, essentially due to the surge in LAN associations with the more wide structures. Different WAN technologies along with their benefits and Drawbacks are evaluated beneath here.

### Dialup

Dial up is WAN innovation that denotes to the use of modem connected to **PSTN** (public switched telephone network) to transmit information, DOCWIKI (n.d.). An association that is built up utilizing a modem. To make the dial-up association the modem must be joined with a dynamic telephone line that is not being used. While uniting the modem will pick up the telephone and dial a number that is appended to another PC. Once an association has been made the two PCs will have the capacity to converse with one another and transmit information permitting the client to check his or her email, peruse the Internet, or offer documents.



Figure 2A 56K dialup modem (source: <http://www.technologyuk.net>)

KSI (n.d.) writes, Dial-up lines are normal phone lines. They are moderate, oblige clients to make an association for every correspondence session physically, and can be untrustworthy for transmitting information. Then again, for a few organizations it might be commonsense to briefly



utilize a dial-up correspondence connection between destinations for a sure measure of time every day to exchange records and overhaul databases. The essential employment of a dial-up modem is to take advanced data and proselyte it to an analog signal that can go over an ordinary phone telephone line. A modem at the ISP's side then takes the simple sign it gets and changes over it back to a computerized signal. Changing over the flag more than once causes corruption and can bring about diminished velocities. Dial up technology demonstrates following benefits and Drawbacks over other WAN technologies:

#### Benefits

- Dial up technology is cheapest amongst all WAN technologies
- Due to dynamic nature of IP addressing to client, it offers securer connection
- It allows connection to rural areas where telephone lines are accessible.

#### Demerits

- It is slowest of all WAN technologies as it offers bandwidth of 56kbps only.
- Due to its slow transmit capacity it is not suitable of video/audio transmission
- To provide dial-up service Telephone connection is required
- Another demerit dial up technology is when utilizing this technology, telephone line is engaged as only one service can be utilized at one time

#### Broadband

ISPVIEW (n.d.) describes broadband technology in general term for any telecoms innovation that can convey a great deal of information, utilizing a wide range (band) of frequencies, over altered phone lines or remote specialized systems. Broadband is regularly called rapid Internet, on the grounds that it for the most part has a high rate of information transmission with respect to dial-up access over a modem. Generally, any association with the client of 256 Kbit/s (0.256 Mbit/s) or more is viewed as broadband Internet, yet the low-end pace bar is consistently rising.

Broadband innovation, Telecommunications gadgets, lines, or advances that permit correspondence over a wide band of frequencies, and particularly over a scope of frequencies separated into various free stations for the synchronous transmission of distinctive signs. Broadband frameworks permit voice, information, and video to be telecast over the same medium in the meantime. They might likewise permit various information channels to be telecast at the same time. Broadband technology includes several transmission technologies such as DSL, Wireless, cable model, fiber, satellite and broadband over power line. This paper critically

evaluates technology such as ADSL which is based on broadband technology while briefly discussing other broadband technology.

### **DSL (Digital Subscriber Line)**

DSL is a wire line transmission innovation that transmits information quicker over conventional copper phone lines as of now introduced to homes and organization, FCC (n.d.). DSL-based broadband gives transmission rates extending from a few hundred Kbps to a large number of bits every second (Mbps). The accessibility and pace of your DSL administration may rely on upon the separation from your home or business to the nearest phone organization office. DSL offers two different technologies:

### **ADSL (Asymmetric Digital Subscriber Line)**

ADSL is short form for Asymmetric Digital Subscribers Line. ADSL is a sort of DSL innovation that gives more noteworthy data transfer capacity and gives higher-speed transmission over customary copper phone wires than dialup technology. DSL broadband innovation is a dependably on association innovation that uses existing phone lines to transport high-transfer speed information, and gives IP administrations to supporters. According to TECHTARGET (n.d.) unlike dialup technology, in ADSL phone line is not engaged and both service can be utilized together. This is achieved via use of micro filters, which is place just above phone and ADSL model.

ADSL is described by "high speeds" and "dependably on" availability. This is accomplished by utilizing the frequencies not being utilized by voice calls. For instance, an ADSL association may permit download rates of 1.5Mbps, while transfer capacity might just reach 256Kbps. Since most clients download significantly more information than they transfer, this distinction generally does not have a recognizable effect on Internet access speeds (TECHTERM, n.d.). In any case, for Web servers or different PCs that send a considerable measure of information upstream, ADSL would be a wasteful decision.

### **Benefits**

- One of the key improvement of ASDL over dial up is it offer better bandwidth
- Enables to utilize data and voice service together as both service uses separate bands



Figure 3 Basic ADSL Micro Filter to separate Phone and data line (Source: <http://www.pimfg.com>)

- It is more convenient than dial up as it provides reliable network connection than dial up
- It uses existing telephone line technology that is used in dial up technology

#### Drawbacks

- ADSL is expensive than Dialup technology
- Firewall is required to secure the network
- Not all telephone line provides DSL service
- Upstream speed is much lower than that of downstream speed which makes it unusable for organization that requires to send large information rather than receive information.
- Speed depends on the distance hence speed degrades over longer distance

#### SDSL (Symmetric Digital Subscriber Line)

Utilized ordinarily by organizations for administrations, for example, video conferencing, which require noteworthy transmission capacity both upstream and downstream. This means upstream speed and downstream speed capacity is similar unlike in ADSL where upstream speed is much lower than downstream.

Other broadband technologies are as follows:

- **Cable Modem:** Cable modem administration empowers cable service providers to give broadband utilizing the same coaxial links that convey pictures and sound to your TV set.
- **Fiber:** Fiber optic (fiber) innovation is a wire line innovation that transports information as light through straightforward glass strands. Fiber is fit for transmitting information at high speeds.
- **Wireless:** Wireless broadband unites a home or business to the Internet utilizing a radio connection between the client's area and the service supplier's office. Remote broadband can be versatile or fixed.
- **Satellite:** Generally as satellites circling the earth give important connections to phone and TV facilities, they can likewise give connections to broadband. Satellite broadband is another type of wireless broadband, and is additionally helpful for serving remote or meagerly populated regions.
- **Broadband over Power lines (BPL):** BPL can be given to homes utilizing existing electrical associations and outlets. BPL is a rising innovation that is accessible in exceptionally restricted territories. It has huge possible on the grounds that electrical chains

are presented basically all over, easing the necessity to build new broadband services for every client.

#### Benefits of Broadband WAN technology

- Broadband technology does not depend on phone line, though there are phone line based technology such as ADSL, there are also large number of technology that does not depend on phone line such as wireless, satellite, cable and BPL
- It is much faster than dial up technology
- Connection stays active hence reliable
- As discussed in ADSL, both voice and data service is available together
- Broadband technology consist of technology that is suitable for both download oriented client and upload oriented clients

#### Drawbacks of Broadband WAN technology

- Usually any broadband technology is expensive than dial up technology
- Requires firewall technology to secure connection
- Not all cable and phone lines are equipped with broadband service
- BPL is still very new technology and available on very few areas, hence it is not accessible from all rural areas which may force to use dial up technology

#### Frame Relay

Frame Relay is an elite WAN convention that works at the physical and Data Link layers of the OSI reference model. 9tut (2011) describes, it offers lower-cost information exchange when contrasted with average point-to-point applications, by utilizing virtual associations inside of the combining so as to case transfer system and those associations into a solitary physical association at every area. Casing hand-off suppliers utilize an edge transfer switch to course the information on each virtual circuit to the fitting destination.



Figure 4Frame relay structure (Source: <http://www.9tut.com/frame-relay-tutorial>)

By utilizing Frame Relay we just need one serial interface at the Headquarter to associate with all divisions as shown in figure 4. This is also genuine when we extend to 10 or 50 divisions. According to UAL (n.d.), it has turned into the most broadly utilized WAN innovation as a part of the world. Expansive ventures, governments, ISPs, and little organizations use Frame Relay, essentially on account of its cost and flexibility. This WAN technology is an illustration of a packet switched innovation. Bundle exchanged systems empower end stations to progressively share the system medium and the accessible data transmission. Variable-length bundles are utilized for more productive and adaptable exchanges. These parcels then are exchanged between the different system sections until the destination is come to. Factual multiplexing strategies control system access in a parcel exchanged system. The upside of this procedure is that it suits more adaptability and more effective utilization of data transfer capacity.

#### Benefits

- It offers greater flexibility while designing network
- It has less hardware requirement, as shown in figure 4, only one serial port is enough to connect with all branches rather than requiring extra serial port for each branch
- The information is sent over the system utilizing frame relay as a part of an extremely productive way, it works in a variable transmission capacities going from 56 Kbps and 45Mbps

#### Drawbacks

- Incorporate conceivable congested roads and transient disadvantages with viability
- It doesn't give the affirmation of got bundle

#### **ISDN (Integrated Services Digital Network)**

The condensing ISDN remains for the specialized term "Incorporated Services Digital Network" and alludes to a computerized standard for phone systems. As the name suggests, different sorts of correspondence services can be communicated through this sort of system. Apart from voice calls, ISDN permits bundle exchanged or circuit-exchanged information transmission and fax transmission. In a few nations, ISDN innovation has assumed control from simple phone systems, coordinating a wide range of administrations into a typical system interestingly. This digitization has additionally empowered advanced ISDN telephone lines to be made accessible to end clients. NFON (n.d.) explains, ISDN conveys the advanced circuits straightforwardly to the clients, empowering them to convey a wide assortment of activity over the system. Along these lines,

ISDN empowers clients to convey voice, video, information, and other movement over the current phone wiring.

According to Mitchell (n.d.) ISDN is a system innovation that backings digital exchange of synchronous voice and information movement. Like DSL in this technology, an ISDN Internet works over normal phone lines. ISDN Internet benefit by and large backings information rates of 128 Kbps. ISDN developed as a distinct option for conventional dialup systems administration amid the 1990s. The moderately high cost of ISDN service, however, constrained its prevalence with private clients at the start. One gigantic favorable position of ISDN is that one ISDN line has two telephone lines with two telephone numbers. You can surf and utilize the telephone in the meantime. For all intents and purposes all shopper ISDN equipment has a port for connecting to simple telephone hardware (phones, fax machines, and so on.) so you can utilize your simple gear over the advanced line. You can even connect your modem to for calling administrations that don't bolster ISDN.

#### Benefits of ISDN

- The core benefit of ISDN is to offer clients multiple digital channel, all working together in same copper wire
- It allowed faster connection with only two seconds while dial up required around 30-50 seconds.
- It offers higher speed rate of up to 128 kbps
- It provides better signal quality than older analog methods

#### Drawbacks of ISDN

- ISDN lines are expensive than traditional telephone lines
- It requires adapter for connection

#### **MPLS (Multiprotocol Layer Switching)**

According to METASWITCH (n.d.) Multiprotocol Label Switching (MPLS) is a convention for accelerating and forming network traffic streams. Multi-Protocol Label Switching (MPLS) gives a system to sending bundles for any system convention. It was initially created in the late 1990s to give speedier bundle sending to IP routers. From that point forward its abilities have extended enormously.

Multiprotocol Label Switching (MPLS) is a system that guides information starting with one system hub then onto the next taking into account short path distance instead of long network address, maintaining a strategic distance from complex lookups in a steering table. Multi-Protocol Label Switching (MPLS) was initially exhibited as a method for enhancing the sending pace of switches yet is presently developing as a critical standard innovation that offers new abilities for vast scale IP systems. Activity building, the capacity of system administrators to direct the way that movement takes through their system, and Virtual Private Network backing are illustrations of two key applications where MPLS is better than any as of now accessible IP innovation (Protocols, n.d.). MPLS moreover deliver the issue identified with adaptability and directing taking into account QoS controlling and service quality that can exist over existing frame relay systems.

According to Drake (n.d.) MPLS takes into account between availability developments of system with negligible expansion of equipment. A MPLS system utilizes correspondences by means of a cloud based system with every hub uniting with the system suppliers MPLS cloud. Not at all like the point to point network which requires a switch interface association on both closures of the association while MPLS considers including new remote associations without the prerequisites of including equipment at your essential site. This considers development at a lesser expense as you don't need to include any equipment interface at your essential site once the system is set up.

### Benefits of MPLS

- Offers great scalability with minimal addition of hardware
- Provides alternative paths to improve uptime
- Effectively utilize alternative paths to improve network congestion

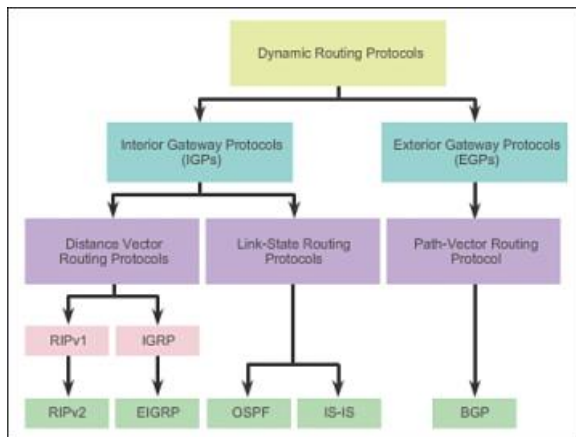
### Drawbacks

- User cannot be in total control as service provider has to play some role in network
- It does not offer any integral data protection

### Routing Protocols

LINFO (n.d.) defines routing protocols as an arrangement of principles utilized by routers to decide the most proper ways into which they ought to forward bundles towards their proposed destinations. The motivation behind routing conventions is to learn of accessible courses that exist on the network system, assemble routing tables and settle on routing choices.





**Figure 5** Internal and External Routing Protocols

Some portion of the occupation of the routing convention is to determine how router report changes and impart data to alternate routes in the system keeping in mind the end goal to redesign their routing tables, accordingly permitting systems to progressively conform to evolving conditions (e.g., changes in system topology and activity designs). There are two types of Routing; dynamic routing and static routing.

### **Dynamic Routing**

Dynamic Routing conventions are the applications which find system destinations progressively (CAREERRIDE, n.d.). Routers will impart the neighboring routers which educates the system to which every router is associated. These routers regulate automatically when variations in traffic occur. It consists of routing tables that are assembled and kept up consequently through a continuous correspondence between routers. This correspondence is encouraged by a routing convention, a progression of occasional or on-interest messages containing routing data that is traded between routers. Aside from their introductory configuration, dynamic routing require small continuous maintenance, and in this manner can scale to bigger internetworks. Dynamic routing protocol is further classified into two different groups as shown in figure 5; Interior Gateway protocol (IGP) and Exterior Gateway Protocol (EGP). This paper further evaluates these protocols.

### **Interior Routing Protocols**

An interior routing protocol (IGP) is a routing convention that is utilized to trade routing data among routers inside of a self-governing framework, for example, an undertaking's LAN. IGP's commonly bolster restricted geological regions. Interior Gateway Protocols (IGP) are utilized to course Internet interchanges inside of a LAN, for example, inside of an office building. Two most common IGP's, RIP and OSPF is discussed below.



### RIP

RIP (Routing Information Protocol) is a way for routers, which connect networks using the Internet Protocol (IP), to share information about how to route traffic among networks. RIP is a most established however broadly utilized routing convention. RIP is most usually utilized as a part of UNIX frameworks. It is a dynamic distance vector routing convention based upon the Berkley BSD application directed and was created for minor IP based systems. It uses step amount as a metric. NETWORKSORCERY (n.d.) notes that version 2 of RIP which is also known as RIPv2 limits network size to 15 hops. Which means RIP protocol is not suitable for larger network which has larger hop size.

### OSPF

OSPF routes IP bundles construct singularly in light of the destination IP location found in the IP bundle header. IP parcels are steered "as may be" - they are not exemplified in any further convention headers as they travel the Autonomous System. OSPF is a dynamic routing convention as it rapidly identifies topological changes in the AS, (for example, router interface disasters) and computes new loop free courses after a time of convergence. This period of convergence is little and implicates a least of routing traffic. Unlike in RIP, hop count does not exists in OSPF protocol. Each OSPF empowered router, when begun, will send hello bundles to all specifically associated OSPF routers. The hello bundles contain data, for example, subnet mask, router timer and router ID. When routers accept these data, they become OSPF neighbors and establish adjacencies.

### Exterior Routing

EGP is in charge of correspondence of system reachability data between neighboring routers, which might be in diverse self-ruling frameworks (TCPIPGUIDE, n.d.). EGP exists keeping in mind the end goal to pass on net-reachability data between neighboring doors, potentially in distinctive self-sufficient frameworks. The convention incorporates instruments to obtain neighbors, screen neighbor reachability and trade net-reachability data as Update messages. The convention depends on intermittent surveying utilizing Hello/I-Heard-You (I-H-U) message trades to screen neighbor reachability and Poll summons to request Update reactions. There are two types of Exterior Routing, EGP and BGP.

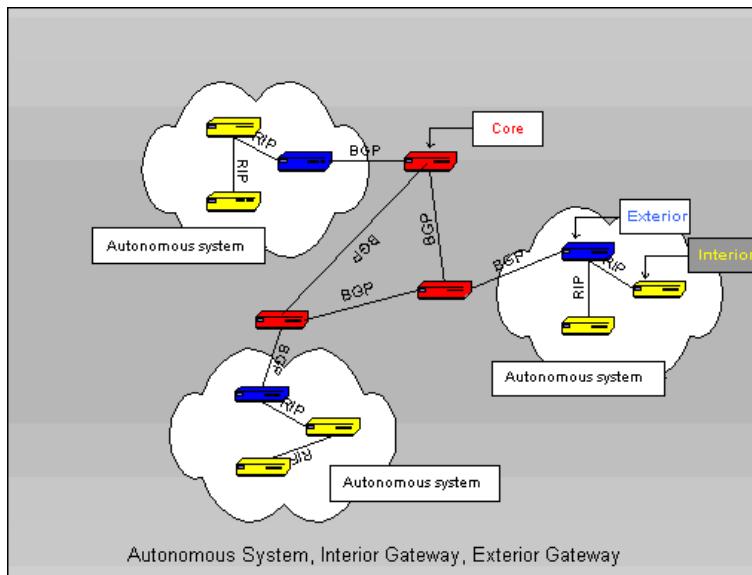


Figure 6 Internal and External Gateway protocol (Source: <http://www4.ncsu.edu>)

### EGP (Exterior Gateway Protocol)

According to Technopedia (n.d.) Preceding the presentation of BGP, Internet hosts utilized EGP for information table routing trades. The EGP routing table incorporates known switches, locations, cost measurements and each ideal course determination way. The EGP model is fabricated with limited occasion, activity and move mechanization. Exterior Gateway Protocol (EGP) is an out of date routing convention that was utilized for information trade between neighboring passages has in self-sufficient frameworks. EGP was habitually utilized by examination foundations, colleges, government offices and private associations, however was supplanted by Border Gateway Protocol (BGP). EGP includes:

- Gain neighbors
- Screen neighbors
- Trade information as redesign messages

### BGP (Border Gateway Protocol)

BGP is significant to network managers of vast associations which join with two or more ISPs, and also to Internet Service Providers (ISPs) who unite with other system suppliers. Schluting (2014) suggest, In the event that you are the administrator of a little network environment, or an end client, then you presumably don't have to think about BGP. BGP has developed its unique reason for conveying Internet reachability data, and can now convey courses for Multicast, IPv6, VPNs, and an assortment of other information. BGP utilizes numerous course parameters called as attributes to characterize directing arrangements and keep up a stable steering environment.

According to Wilkins (2010) The primary motivation behind BGP is to trade routing redesigns like other routing conventions, yet BGP commonly does not trade individual system routes (but rather in fact it can), it be able to trades rundowns of system routes. This is on the grounds that the run of the mill utilization of BGP is over vast systems including the Internet.

#### Benefits of Dynamic Routing

- Helps to determine best route and scalable
- Adapt to changes automatically
- If a route fails, it choose alternative route automatically

#### Drawbacks of Dynamic Routing

- It is complex to configure
- It requires extra CPU and memory

#### Static Routing

Static routing is a type of routing that happens when a router uses a manually designed routing passage, as opposed to data from a dynamic routing convention to exchange traffic. Technopedia (n.d.) Static routing achieves routing choices with preconfigured courses in the routing table, which can be changed manually. This method is typically executed in those circumstances where the decisions in course choice are restricted, or there is just a solitary default route accessible. Additionally, static routing can be utilized if only few routers need to be configured and routing routes are fixed.

#### Benefits

- Offers greater predictability as administrator knows the routing path
- This technology is easy to configure
- It has zero overhead

#### Drawbacks

- It offers lesser Scalability as configuring large network can be time consuming and complex
- No redundancy as alternative path is unavailable

#### Summary

This paper critically evaluated various WAN technologies. WAN is technology that covers large geographic land zone to connect with remote clients. There are various WAN based technologies available. From dial up connection to broadband connection, WAN has evolved a lot all these

years. Newer innovations has improvements over older technologies for example, dial up connection required telephone line and was able to provide only 56 Kbps whereas now it is possible to get Mbps of speed and does not required telephone line.

While evaluating various technologies, WAN supporting protocols are also critically evaluated which included frame relay, routing protocols etc. With frame relay two different corporate network would able to understand each other. Routing concept allows two different networks to understand each other. Finally, evaluation shows WAN has enabled the world to connect with each other, example being internet itself. It has provided ability to overcome limitations of LAN and explore more opportunities.

## **References**

- (TCPIPGUIDE, n.d.) TCP/IP Exterior Gateway Protocol (EGP)  
[http://www.tcpipguide.com/free/t\\_TCPIPEXteriorGatewayProtocolEGP.htm](http://www.tcpipguide.com/free/t_TCPIPEXteriorGatewayProtocolEGP.htm)
- 9tut (2011) Frame Relay Tutorial [Online] Available: <http://www.9tut.com/frame-relay-tutorial> Accessed [11/10/2015]
- CAREERRIDE (n.d.) what is static and dynamic routing? Explain their differences.  
[Online] Available: <http://www.careerride.com/Networking-what-is-static-and-dynamic-routing.aspx>
- DOCWIKI (n.d.) Dial-up Technology [http://docwiki.cisco.com/wiki/Dial-up\\_Technology](http://docwiki.cisco.com/wiki/Dial-up_Technology)  
Accessed [10/10/2015]
- Drake, K. (n.d.) Pros vs. Cons of an MPLS Network [Online] Available:  
<http://ongoingoperations.com/blog/2013/01/mpls-network-pros-cons/>
- FCC (n.d.) Types of Broadband Connections [Online] Available:  
<https://www.fcc.gov/general/types-broadband-connections>
- INC (n.d.) Wide Area Networks (WANs) <http://www.inc.com/encyclopedia/wide-area-networks-wans.html>
- ISPREVIEW (n.d.) Broadband ISP Technology  
<http://www.ispreview.co.uk/broadband.shtml> Accessed [10/10/2015]
- KSI (n.d.) Connection Services [Online] Available:  
<http://pluto.ksi.edu/~cyh/cis370/ebook/ch07c.htm> Accessed [10/10/2015]
- LINFO (n.d.) Routing Protocol Definition [Online] Available:  
[http://www.linfo.org/routing\\_protocol.html](http://www.linfo.org/routing_protocol.html)
- METASWITCH (n.d.) what is MPLS and GMPLS? [Online] Available:  
<http://www.metaswitch.com/resources/what-is-mpls-and-gmpls> Accessed [11/10/2015]
- Mitchell, B. (n.d.) ISDN - Integrated Services Digital Network [Online] Available:  
[http://compnetworking.about.com/od/internetaccessbestuses/g/bldef\\_isdn.htm](http://compnetworking.about.com/od/internetaccessbestuses/g/bldef_isdn.htm) Accessed [11/10/2015]
- NETWORKSORCERY (n.d.) RIP, Routing Information Protocol  
<http://www.networksorcery.com/enp/protocol/rip.htm> Accessed [11/10/2015]
- NFON (n.d.) ISDN <https://www.nfon.com/gb/solutions/resources/glossary/isdn/>
- PROTOCOLS (n.d.) Multi-Protocol Label Switching (MPLS)  
<http://www.protocols.com/papers/mps.htm>

- REFERENCEFORBUSINESS (n.d.) WIDE AREA NETWORKS (WANS)  
<http://www.referenceforbusiness.com/small/Sm-Z/Wide-Area-Networks-WANS.html>
- Schluting, C. (2014) Networking 101: Understanding BGP Routing  
<http://www.enterprisenetworkingplanet.com/netsp/article.php/3615896/Networking-101-Understanding-BGP-Routing.htm> Accessed [11/10/2015]
- Technopedia (n.d.) Exterior Gateway Protocol (EGP) [Online] Available:  
<https://www.techopedia.com/definition/6987/exterior-gateway-protocol-egp> Accessed [11/10/2015]
- Technopedia (n.d.) Wide Area Network (WAN) [Online] Available:  
<https://www.techopedia.com/definition/5409/wide-area-network-wan>
- TECHTARGET (n.d.) ADSL (Asymmetric Digital Subscriber Line) definition [Online] Available: <http://searchnetworking.techtarget.com/definition/ADSL>
- TECHTERM (n.d.) ADSL <http://techterms.com/definition/adsl>
- UAL (n.d.) Frame Relay  
[http://www.ual.es/~vruiz/Docencia/Apuntes/Networking/Technologies/Frame\\_Relay/index.html](http://www.ual.es/~vruiz/Docencia/Apuntes/Networking/Technologies/Frame_Relay/index.html) Accessed [11/10/2015]
- Wilkins, S. (2010) Cisco BGP (Border Gateway Protocol) Basics [Online] Available:  
<http://blog.pluralsight.com/bgp-border-gateway-protocol> Accessed [11/10/2015]
- Woodcock, J. (n.d.) WAN Technologies [Online] Available:  
<https://technet.microsoft.com/en-us/library/bb962087.aspx> Accessed [10/10/2015]

**Task 2**

**Critically analyze intensive services and their performance.** [1.2, D3]

**Introduction**

In many cases, distinctive system applications have diverse asset prerequisites. A few applications work progressively and require a higher offer of the accessible transfer speed, for example, VoIP interchanges. Other programming just requires little blasts of data transmission, for example, web programs. As utilization of the WAN develops more advanced and complex, so does the requirement for more prominent limit and quicker downloads. It is just fitting, then, that clients are agreeing to broadband at a rate that can be depicted as out and out rapid. Basically, this fast development speaks to a developing requirement for pace. Applications, for example, viewing online video, utilizing Internet convention based telephony benefits, and downloading music documents require much more noteworthy data transfer capacity.

The determination to coerce item expenses and power utilization places severe restrictions on system engineers, particularly with concerning peripheral memory bandwidth (Mace, n.d.). To improve quality, administrators/engineers must concentrate on effective usage of this system bandwidth to help in the organization of precious bandwidth resources.

**Quality of Service Management**

According to TechNet (n.d.) Quality of Service (QoS) is an all-inclusive arrangement of benchmarks and instruments for guaranteeing brilliant execution for intricate applications. By utilizing QoS components, administrators can utilize existing assets productively and guarantee the required level of administration without responsively growing or over-provisioning their systems. QoS lets system heads control when and how information is dropped when congestion occurs. Thusly, QoS is an essential device that ought to be empowered, alongside including transmission capacity, as a major aspect of an organized scope quantification process. TECHTARGET (n.d.) states, on the technology, QoS (Quality of Service) is the real trick that transmission rates, mistake rates, and different attributes can be measured, enhanced, and, to some degree, ensured ahead of time.

**QoS Concepts**

A traffic escalated application can bring about poor or unsuitable execution for all applications. These critical activities requires special handling. QoS turns into a key component in conveyance of administration in a guaranteed, strong, and exceptionally efficient way. The objective of QoS is

to give particular transmission service to the applications that need it by assuring adequate transmission capacity, governing Latency and jitter, and lessening information loss. The accompanying table depicts these system attributes.

- **Bandwidth:** Data traffic transfer rate
- **Latency:** The interruption in information communication from source to endpoint.
- **Jitter:** The discrepancy in latency.
- **Reliability:** The ratio of packages waste by a router.

### Benefits of QoS

- Ensures intensive applications such as video streaming, audio streaming, VoIP has required resources to function correctly
- QoS improves client experience by improving quality of intensive applications
- Utilizes existing system to satisfy business requirements

Various QoS technologies such as DSCP, IP precedence, Queue etc. are analyzed here.

### Type of Service (TOS)

IP parcels have a field called the Type of Service field (otherwise called the TOS byte). The first thought behind the TOS Byte was that we could determine a priority and demand a course for high throughput, low defer and high solid administration. The way it is utilized has changed consistently. This makes it confounding to comprehend subsequent to there is a considerable measure of phrasing and some of is not utilized any longer these days. This paper analyzes IP precedence and DSCP.

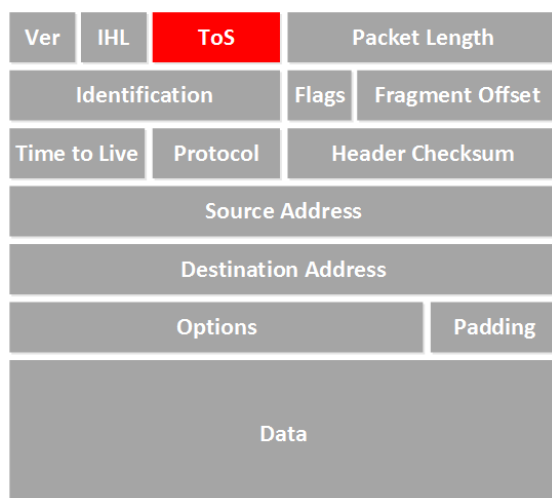


Figure 7 TOS byte



### IP precedence

According to NETWORKLESSONS (n.d.), during early days, TOS Bytes describes eight bits like as presented in figure 2. Here, first three bits described precedence (Figure 3) whereas other 5 bits described type of the service (Figure 4).

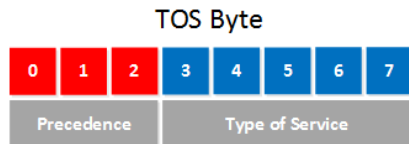


Figure 8 TOS Bytes in early days

000	Routine
001	Priority
010	Immediate
011	Flash
100	Flash Override
101	Critic/Critical
110	Internetwork Control
111	Network Control

Figure 9 Precedence

Bit 3:	0 = normal delay	1 = low delay
Bit 4:	0 = normal throughput	1 = high throughput
Bit 5:	0 = normal reliability	1 = high reliability
Bit 6-7:	Reserved for future use	

Figure 10 type of Service

### DSCP (Differentiated Services Code Point)

Differentiated Services (DiffServ, or DS) is a convention for indicating and controlling system movement by class so that definite type of activity get priority - for instance, voice traffic, which requires a moderately continuous stream of information, may get priority over different sorts of activity. It is most innovative method for handling traffic in terms of what is called Class of Service (CoS). The six utmost important bits of the DiffServ field is termed as the DSCP (figure 5).

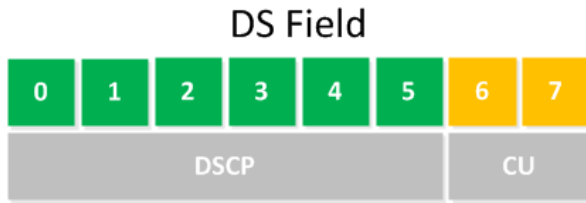



Figure 11 TOS Byte distribution

According to Fortinet (n.d.) Differentiated Services portrays an arrangement of end-to-end Quality of Service (QoS) abilities. End-to-end QoS is the capacity of a system to distribute facility required by particular system traffic starting with one end of the system then onto the next. By developing differentiated services, you arrange your system to convey specific levels of service for diverse packages in light of the QoS determined by every bundle. The DSCP 6-bit field in an IP parcel header empowers levels of administration to be allocated to network movement as per the field's binary value. This 6-bit field includes three IP Precedence MSBs with a minimum huge 3-bit extension field as characterized in RFC 2474.



DSCP Value	DSCP Description	Example Traffic Types
46	VoIP	VoIP
34	Interactive video	Video conferencing
26	Mission critical data	Database queries Database synchronizations Streaming media
0	Best effort	
10	Bulk data	E-mail Web browsing
8	Scavenger	Network backups Windows Update

Figure 12 Example of DSCP in Traffic priority (Source: <http://www.biztechmagazine.com/>)

### Queues

If someone goes to a band and he/she has to wait on a queue, because there are not cashiers available. Similarly, in networking environment, queues is formulates because output interface is jammed. For example, 15Mbps cannot fit on a 10Mbps interface. This makes router to queue packets rather than dropping traffic. Any new packet will go over the queuing line. There are two queuing algorithm available which are explained below.

#### First in First out (FIFO) mechanism

In this algorithm, the first packet is served first whereas last packet is served last. Packages are not classified based on their importance. FIFO is known for its fairest queuing algorithm. Some benefits FIFO algorithm are as follows:

### Benefits

- This algorithm is simple and fast
- It is supported on all platform
- It is supported by all version of cisco IOS

### Drawbacks

- Causes starvation
- Causes variation in delay-jitter

### WFQ queuing mechanism

Weighted Fair Queuing". A stream based lining calculation utilized as a part of Quality of Service (QoS) system applications that calendars low-volume movement to begin with, while letting high-volume activity share the remaining transfer speed. This is taken care of by relegating a weight to every stream, where lower weights are the first to be adjusted. Benefits and limitations of this algorithm is listed as follows:

### Benefits

- Supported in almost all platform and cisco IOS
- Simple to configure and manual classification is not required

### Drawbacks

- Most router does not allow to configure WFQ algorithm
- It is not available for high speed connection over 2.048 Mbps
- Significant increment in traffic can make this queuing system ineffective

### Rules Base

A Policy Package includes a few Rule Bases, contingent upon the arrangement sorts chose (checkpoint, n.d.). QoS strategy is actualized by characterizing a requested arrangement of principles in the Rule Base. The Rule Base is contained those tenets which you make as default guideline. The default standard is naturally made with the Rule Base. It can be adjusted however can't be erased. The major idea of the Rule Base is that unless different principles apply, the default tenet is connected to all information bundles. The Rule Base indicates what moves are to be made with the information parcels. It determines the source and destination of the correspondence, what administrations can be utilized, at what times, whether to log the association and the logging level.

A QoS Rule Base is connected to particular portals and interfaces. After you have made the Policy Package and characterized its QoS rules you must introduce it on the pertinent QoS entryways.

### Congestion Management

Congestion management is the procedure of dealing with a jam condition. It is a standout amongst the most vital instruments in QoS control. It uses lining hypothesis to take care of issues in the congested interfaces. As the information rate can be distinctive among diverse systems, blockage may happen to both wide range system (WAN) and neighborhood (LAN). Just when an interface is congested will the lining hypothesis start to work. Framework backings class-based weighted reasonable lining (CBWFQ) and low inertness lining (LLQ).

Congestion handling systems incorporate the utilization of supports that can be utilized to impermanent store information in one or more lines until the information can be sent through the interior transport or exchanging grid of a switch or switch or through an active port and over an interchanges join. As the supports fill to limit, data can be tossed, maybe precisely taking into account a need or nature of service (QoS) component. In the event that a system is arranged as a cross section, a segment switch may be able to distinguish and practice substitute ways if the essential way is enduring congestion levels that surpass quantifiable parameters set up in light of QoS goals. Congestion management, is utilized to oversee outlines before they leave a gadget. In switches this is known as yield lining in light of the fact that IP sending choices are made before the lining. Blockage evasion is a term for overseeing activity to choose if/when parcels will be dropped amid congestion periods.

### Quality of Service Need

This paper has already analyzed various technologies related to Quality of service management. As there are many traffic intensive applications (services), the need of quality of service is even greater. This paper now analyzes QoS need of VoIP, Video (interactive and streaming) and audio streaming.

### Voice over IP (VoIP)

Voice over IP also referred as VoIP is basically phone service through internet. If a person has access to internet, he can access to phone service via internet rather than local telephone organization. It has become popular choice due to low cost and added functionality. For VoIP to work efficiently and provide quality performance along with cost benefits, consistent high quality voice transmission is required. Packets should not be dropped and create jitter and high latency.

QoS ensures VoIP packets are treated in right way so that they are guaranteed with sufficient bandwidth, jitter and latency requirement. VoIP requires QoS assistance to achieve following features:

- Achieve required adequate bandwidth
- reduce loss and avoiding network congestion
- Determining system traffic
- Packet classification and place in reserve queue

### Video

There are two types of video traffics available. First being interactive video (video conferencing) and other being video streaming.

### Interactive Video

While managing this sort of video traffic following instruction is suggested:

- There should be maximum of 150 ms one-way latency
- There should be less than one percent of loss and less than 30 ms jitter
- There should be less than 30 ms jitter

### Streaming Video

Video streaming have more tolerant QoS requirements as they can take several second delay. But as it may contain valuable information such as e-learning content, service should be guaranteed.

While managing video streaming traffic following instruction is suggested:

- There should be less than 5 percent of loss
- Latency should be of less than 4-5 seconds

### Conclusion

This paper critically analyzed various technologies that enables the management of intensive services. These intensive services refers to bandwidth related services such as VoIP or audio/video streaming. Quality of Service management allows to ensure that these critical application/services operates correctly. To achieve this, QoS need for each of these services is evaluated while also analyzing queue management, base rules, congestion management, IP precedence etc. Technologies such as IP precedence and DSCP allows to prioritize certain intensive service. Special treatment for traffic intensive services is critically analyzed in this paper.

**References**

- Checkpoint (n.d.) Managing QoS [Online] Available:  
[https://sc1.checkpoint.com/documents/R76/CP\\_R76\\_QoS\\_AdminGuide/14871.htm](https://sc1.checkpoint.com/documents/R76/CP_R76_QoS_AdminGuide/14871.htm)  
Accessed [15/10/2015]
- Fortinet (n.d.) Differentiated Services Code Point (DSCP) behavior through an IPsec tunnel [Online] Available: <http://kb.fortinet.com/kb/documentLink.do?externalID=13588>  
Accessed [15/10/2015]
- Mace, T. (n.d.) Traffic Management for Optimizing Media-Intensive SoCs [PDF]  
Available: [https://www.arm.com/files/pdf/Traffic\\_Management\\_for\\_Optimizing\\_Media-Intensive\\_SoCs.pdf](https://www.arm.com/files/pdf/Traffic_Management_for_Optimizing_Media-Intensive_SoCs.pdf)
- NETWORKLESSONS (n.d.) IP Precedence and DSCP Values [Online] Available:  
<https://networklessons.com/quality-of-service/ip-precedence-dscp-values/> Accessed  
[15/10/2015]
- TechNet (n.d.) What Is QoS? [Online] Available: [https://technet.microsoft.com/en-us/library/cc757120%28v=ws.10%29.aspx#w2k3tr\\_qos\\_what\\_bsja](https://technet.microsoft.com/en-us/library/cc757120%28v=ws.10%29.aspx#w2k3tr_qos_what_bsja)
- TECHTARGET (n.d.) QoS (Quality of Service) definition [Online] Available:  
<http://searchunifiedcommunications.techtarget.com/definition/QoS-Quality-of-Service>  
Accessed [15/10/2015]

**Task 3 [1.3]**

**Discuss** WAN concerns and make recommendations to sustain network security, reliability and performance.

**Introduction**

Ensuring protection of data and corporate resources has dependably been a complicated task, and modern developments just adds to the complication. Remote workplaces and portable clients require the same amount of security, and perhaps more, than base camp representatives who sit behind precisely developed layers of guard. Number of clients working outside a main workplace from distant location like branch workplaces are growing building security and optimization challenges for administrators.

WAN is a network atmosphere that covers large topographical area. WAN environment has several concerns such as its reliability, performance and its security. Organization has make sure WAN network is reliable and give satisfying performance hence to achieve business goals. Yet, security can be biggest concern faced by WAN due to its critical nature. As WAN is large and complex network environment, there are various concerns related to the security that can be utilized as opportunity by attacker (intruders) to gain access of system or harm system. WAN tends to have security vulnerabilities if not managed properly and these vulnerabilities can be exploited by attackers. Hence, these security concerns need to be analyzed and managed properly before any disaster occur. The significance of addressing WAN concern is not limited to security but performance and reliability as well. This paper discusses various WAN security technologies **recommendation** that allows to build secure and reliable network.

**MD5 (Message Digest Algorithm 5)**

Cryptography is technology that allows to code and decode data to provide secure transfer of the data. It is process of converting plaintext data into cipher text. MD5 (Message Digest calculation 5) is extraordinary cryptographic has.

MD5 has hash capacity of 128bit and is utilized in data security. MD5 cryptography algorithm was developed in 1991 by Prof. Ronald L. Rivest. In this method normal message is provided as input and 128 coded message in taken as output. This algorithm allows to compare originality of a file by comparing checksums on two files.

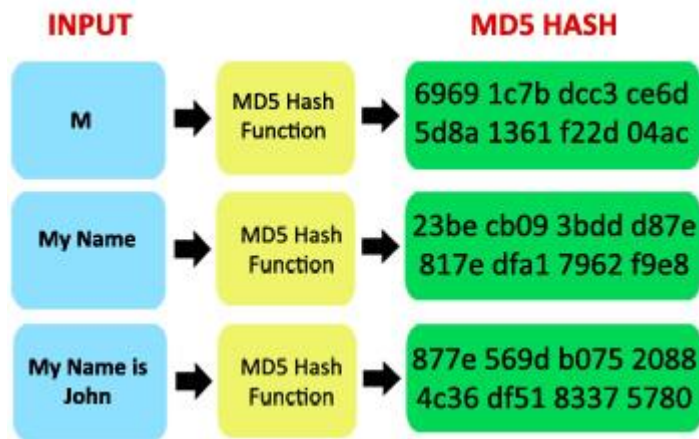


Figure 13 MD5 hashing (source: <http://www.gohacking.com/>)

In WAN environment, MD5 is utilized to authenticate routing. Router utilizes MD5 algorithm to secure the routing. Protocols that utilizes MD5 are, RIPv2, OSPF, BGP and EIGRP. For example, Administrator can arrange MD5 validation between two BGP companions, implying that every portion sent on the TCP association between the associates is confirmed. MD5 confirmation must be designed with the same secret word on both BGP peers; generally, the association between them won't be made. Designing MD5 verification causes the Cisco IOS programming to create and check the MD5 condensation of each section sent on the TCP association.

### Authentication Protocol

The procedure of distinguishing an individual, typically in view of a username and password. In security frameworks, verification is particular from approval, which is the procedure of giving people access to framework articles in view of their character. System validation affirms the client's recognizable proof to any system benefit that the client is endeavoring to get to. Validation is a totally key component of a regular security model which is the procedure of affirming the recognizable proof of a client or at times, a machine that is attempting to sign on or access assets. There are several authentication protocol and methods, this paper discusses two of the most popular authentication protocols.

### PAP (Password Authentication Protocol)

PAP is authentication mechanism that utilizes password to authenticate an individual. In point to point protocol, before authorizing access to a client authentication is done to verify the client. This authentication protocol is utilized by remote network server to authenticate client by checking username and password (as shown in figure 2) but as it generally uses unencrypted ASCII passwords, it is considered less secure technology. It is used on networking environments where



more secure authentication is not supported. In UNIX based remote system, PAP is utilized to authenticate the access as more secure protocol is not supported. PAP is popular due to its simple use and deployment.

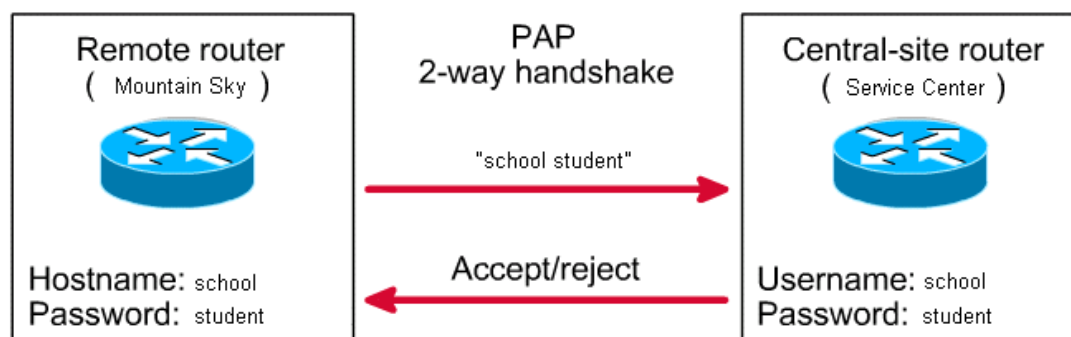


Figure 14 PAP Authentication (Source: <http://www.point.ro>)

### **CHAP (Challenge Handshake Authentication Protocol)**

The server sends a test message to requester once connection is made. Utilizing hash function, requestor replies with a value. Then the server checks the reply with the hash value it expects (shown in figure 3). Here if expected has value and hash value of reply from responder matches, authentication is accepted or else, connection is ended. CHAP provides better security mechanism than PAP and server may ask for new challenge message during connection as CHAP identifiers alters regularly. Unlike PAP, instead of password, representation of sent to server for authentication.

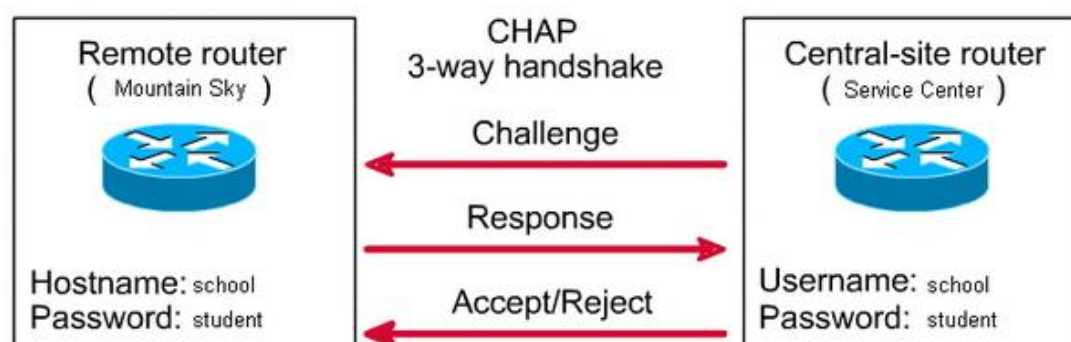


Figure 15 CHAP Authentication (Source: <http://www.examcollection.com>)

### **Broadcast Reduction**

In basic term, broadcasting intends to convey the message or an information to the distinctive people. It transmits a bundle which will be gotten by every last gadget on the system. Switches, switches, printers, servers, workstations and so on are the sorts of gadgets which are the wellsprings

of system show decrease. Reducing broadcast results reduction in unnecessary traffic in network. This results enhancement in data transmission. This enables increment in quality of service performance. This is a popular method to tackle performance concern on WAN. Along with increased traffic, broadcast can eat CPU hence it is better to reduce broadcast and match the requirement of the system.

To reduce broadcast, IP sub netting technology is utilized. It is basically method to divide single large network into smaller network. As broadcast is processed by every client in the network reducing size of the network allows to improve performance by limiting broadcast. Benefit of sub netting is it allows to control traffic and bandwidth use by reducing broadcast.

### **Firewalls**

Firewall is a great technology to prevent access that are not authorized. In WAN, security concern of unauthorized access to system is greatly tackled using firewall system. Corporate network consists of hardware, software of both firewalls combined together. Firewall provides network security by monitory every incoming or outgoing traffic flow and allow/block them based on the defined **traffic rule**. Hardware firewall is device utilized in similar manner to other network infrastructures. But modern routers tends to have firewall system integrated with them. On the other hand, software firewall is installed to operating system. To achieve optimal security, both hardware and software firewall should be implemented.

Firewall provides security basically by packet **filtering**. A method in which, each inbound and outbound packets are either allowed or blocked by firewall based on the traffic rule stored in firewall. Both hardware and software firewall functions similarly. Firewall is great tool to address security concern in WAN technology. Figure 4 demonstrates basic use of firewall to secure critical resources in the network.

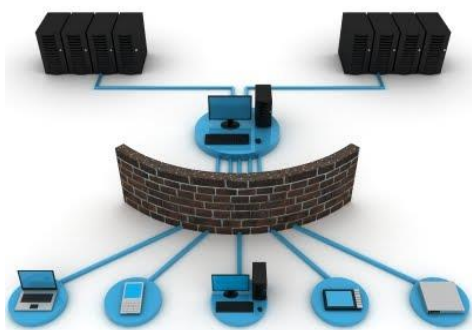


Figure 16 Demonstration of Firewall in Network ([www.tudopelanet.com.br](http://www.tudopelanet.com.br))

## Access Control Lists

Access control list is another great tool to filter/control traffic. Traffic control is done using defined set of traffic rules. ACL is cisco based mechanism that provides great security mean while addressing WAN security concerns. There are basically two types of ACL available. Standard and Extended.

1. Standard Access Control List ranges from 1-99 and allows to block connection from any specific IP address. This method is utilized if whole connection is need to be blocked from a system rather than any specific service as shown in figure 5. This is very basic type of access control mechanism and very easy to implement

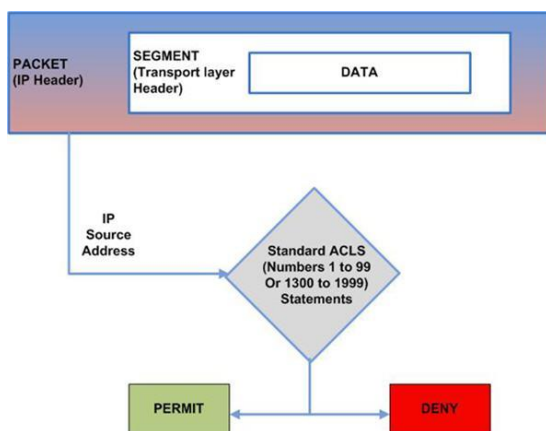


Figure 17 Standard Access Control (Source: <http://blog.pluralsight.com/>)

2. Extended Access control list on the other hand allows to control traffic based on source, destination and port. Extended access control list offers additional control to the administrator while defining traffic rules.

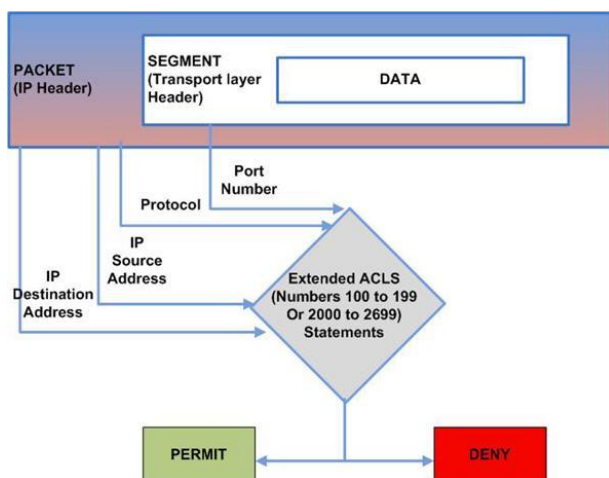


Figure 18 Extended Access Control (Source: <http://blog.pluralsight.com/>)

**Tunneling**

While addressing WAN concern of security and reliability, tunneling is great mean of ensuring secure data transmission. Tunneling allows to move data to private network through public network by encapsulating them. This means, client can access to remote network through public network securely. In WAN, branch offices can join with head office through tunneling to ensure security of data. In this method, public network is unaware of data being part of private network. With help of VPN (Virtual private network) user gains authorized access to data. Two most common tunneling protocol are PPTP and GRE. PPTP stands for point to point tunneling protocol developed by Microsoft whereas GRE stands for generic routing encapsulation and developed by Cisco systems. Tunneling utilizes various encrypting algorithm to enhance security outcome.

**Recommendation**

When developing WAN infrastructure for Everest networking, it is recommended to utilize Proper authentication method to ensure the identity of client. Here CHAP is recommended but in places where CHAP is not suitable, at least PAP should be utilized. It is recommended to use proper encryption methodology such as MD5 to encode information while transferring critical data. Furthermore, to address security concerns, proper firewall and ACL should be utilized and VPN should be used for connecting with branch offices. And finally, proper broadcast reduction should be done to enhance security and performance.

**Task 4**

**Critically evaluate** different trust systems on a WAN [1.4]

**Introduction**

WAN depends on trust, in one way or another among clients of the system. Basically, several forms of trust exist to tackle different sorts of issues and reduce risks in certain situation. In WAN security, there are three forms of trust than clients can understand: remote trust, intermediary trust and trust of network wan. This paper critically evaluates various trust systems on WAN.

**Trust of Intermediary System**

Intermediary is basically a third party service. In WAN environment, there are third party tools that filter, modifies and evaluates data between client and server. According to TECHTARGET (n.d.) an example of such tools is proxy server which in corporate networks is placed between public internet user and internal web users. Proxy is basically point to point association between remote network and client. Clients may use proxy to get into restricted websites, or get security and anonymity it breaks its own network traffic code. Which makes Network extremely vulnerable. Another drawback of using such intermediary system such as proxy is it slows down connection as it fundamentally transferring all information to another location before going out of internet.

**Trust of Remote System**

Different clients in WAN are associated with main server through cloud. These clients are described as remote system. When connecting to remote system, a trust need to be established between client and remote system. This trust is required to ensure system is trusted before data transmission. Trust in remote system is be certain of that the other party is credible and reliable. To build such trust connection between requires authentication and authorization which utilizes authentication protocols such as PAP or CHAP. In PAP method, client uses username and password to authenticate itself. If credentials are valid remote system permit user to access system creating trust between them. Meanwhile, In CHAP, encrypted message is used as CHAP. As functionalities of PAP and CHAP has already been analyzed in previous document, study of these authentication protocol provides idea of how trust is built between remote system and client.

**Trust of Network WAN**

Corporate networks often requires connection with other corporate networks. These connection is done through leased line (SOURCEDADDY, n.d.). For example, many organization utilizes leased line to connect with branch networks across the nation. Security of such environment is equivalent

to security level of weakest network. Here, for successful association, trust is required. To ensure security of the network resources, trust system enables to make sure only authorized clients gets access to system. Various technologies utilized in WAN to establish trust is discussed below.

#### Authentication, Authorization and Accounting (AAA) Protocol

According to Cisco (n.d.) AAA is technology framework that perceptively controls access to the system. First A is referred to Authentication which basically verifies the identity of client by utilizing verification tools such as username and password. Second A is referred to authentication which defines what user is allowed to do in the system. Client is able to perform only tasks that are authorized to them. And last A describes accounting which explains the measurement required by client to access the system such as resource use. This technology helps to build trust within WAN network connection.

#### Secure Sockets Layer (SSL) Certificate

SSL Certificates are little information records that digitally tie a cryptographic key to an association's subtle elements. At the point when introduced on a web server, it initiates the lock and the https convention (over port 443) and permits secure associations from a web server to a program. SSL is utilized to secure credit card transaction, information exchange and logins, and all the more as of late is turning into the standard when securing perusing of online networking destinations (Simard, 2014). SSL Certificates should be issued from a trusted Certificate Authority's Root. The Root Certificate must be available on the end client's machine all together for the Certificate to be trusted. On the off chance that it is not believed the program will exhibit untrusted blunder messages to the end use. This technology improves trust system of the WAN as any unauthorized access can be denied and any change in originality of document can be catch and warned.

#### Point-to-Point Protocol (PPP) Authentication

Point-to-Point Protocol is a Data Link layer convention that can be utilized over asynchronous serial (dial-up) and ISDN media and uses the LCP (Link Control Protocol) to manufacture and keep up information associations (TRIPOD, n.d.). The essential purpose of PPP is to transport layer-3 bundles over a Data Link layer point-to-point join. PPP comprises of two principle segments, LCP (Link Control Protocol - used to set up, arrange, test, keep up, and end the point-to-point association) and a group of NCPs (Network Control Protocols) for setting up and arranging distinctive Network layer conventions. With PPP authentication, it is ensured that only authenticated person access to the system enhancing the true level.

**Conclusion**

This paper critically evaluated several trust system on WAN. Trust system such as intermediary system, trust on networks on WAN and trust on remote system was evaluated. With trust system, various security risk can be mitigated. To develop trust between remote and head office, authentication mechanism should be utilized such as PAP or CHAP to ensure validity of client. In WAN network to develop trust authentication system such as PPP or AAA validates the identity of client. This evaluation of trust system on WAN signifies the importance trust system. Different type of trust is suitable for different situation. For Everest network WAN, suitable trust system should be utilized to ensure trust in the network.

**References**

- Cisco (n.d.) Network Authentication, Authorization, and Accounting: Part One  
[http://www.cisco.com/web/about/ac123/ac147/archived\\_issues/ipj\\_10-1/101\\_aaa-part1.html](http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-1/101_aaa-part1.html)
- Simard, E. (2014) the-importance-and-advantages-of-SSL-certificates [Online] Available:  
<http://www.gtcomm.net/blog/the-importance-and-advantages-of-ssl-certificates/Access>  
[10/13/2015]
- SOURCEDADDY, (n.d.) Network trust relationships [Online] Available:  
<http://sourcedaddy.com/networking/network-trust-relationships.html>
- TECHTARGET (n.d.) intermediary definition [Online] Available:  
<http://searchcio.techtarget.com/definition/intermediary> Access [10/13/2015]
- TRIPOD (n.d.) The PPP Model [Online] Available:  
<http://netcert.tripod.com/ccna/wan/ppp.html> Access [10/13/2015]



**Task 5**

**Design a WAN** infrastructure to meet the given requirement of Himalayan Networks and **critically** evaluates the suitability of WAN components. [2.1, 2.2 M2]

**Introduction**

Everest Network Pvt. Ltd. Is network service provider who wants to plant WAN infrastructure for head office and branch offices. To design WAN infrastructure for branches and connect branches with main office to provide Wi-Fi service to customers, various technologies needs to be analyzed. This paper design WAN infrastructure for Everest Network while evaluating supporting technologies, devices, routing solution and IP addressing plan.

**WAN Infrastructure Design**

Prepared design to satisfy requirement for Everest Networking is provided in page below.

## **Technologies**

Various Technologies utilized while designing WAN infrastructure is evaluated below. This includes DHCP roles, Planned VLANs, Routing Concepts utilized in network as well as other server technologies that supports implementation of network infrastructures.

### **DHCP**

Dynamic Host configuration protocol is protocol that enables automatic distribution of dynamic IP addresses to resources in Network, Indiana University (n.d.). Dynamic IP addresses are distributed using either DHCP server which is dedicated server that provides IP addresses or through Access point router itself. An IP scope is defined which is utilized by DHCP while distributing IP, this scope store information about IP ranges. One of the key benefit of DHCP is it not only provides IP addresses to clients but also provide DNS information and gateway information.

### **Role in Proposed System**

IP addresses in proposed system is assigned to resources using both static as well as dynamic method. As Himalayan network is service provider that provides service to very large clients, it is nearly impossible to provide static IP address to all clients. Also as dynamic IP addresses are not permanent, it is suitable method to provide IP to clients as Wi-Fi users are not permanent. Static IP addresses are distributed to more consistent resources like servers. Proposed design uses both server based DHCP to provide IP to resources within the network and access point DHCP to provide IP to Wi-Fi users.

### **VLANs**

According to Beal (n.d.) VLAN is short form of virtual local area network that allows resources to behave like if they are in same LAN even if they are physically in different segment LAN. VLANs are created and maintained using software instead of hardware itself. This makes VLAN a very flexible tool when it comes to WAN infrastructure design. Some of the advantages of VLANs in proposed design are as follows:

- One of the key advantages of VLAN is broadcast control. VLAN is utilized to create small segment of LAN from large LAN. This allows to reduce Broadcast and tackle WAN concern of performance and reliability
- As Large LAN behave as different LANs in VLAN, they cannot communicate with each other like they used to when they were in single network. This helps to improve security of the system.

- With single switch multiple network can be created which helps to reduce cost of design implementation.

In proposed WAN infrastructure plan, various VLANs are identified. Which includes VLANs for server, HR department, Account Department, Customer Care department. Planned VLANs for Everest network demonstrated below.

```
VLAN Name
-----
1    default

101  Servers
102  SalesMarketing
103  HR
104  Account
105  CustomerCare
```

### **Connection**

#### **Routing Concepts**

In proposed design dynamic routing is utilized. Enhanced Interior Gateway Routing Protocol is cisco based interior routing protocol which has been very popular due to its friendly and advanced features (TECHREPUBLIC, n.d.). This protocol is utilized to route data in internal network. It is advancement of older and less popular IGRP. One of the key benefit of this routing protocol is it requires very small network resources. Following are the benefits of EIGRP in designed system:

- It offers very rapid connection and loop free environment
- Requires very small network resources for routing update
- Requires very small CPU
- Usage load of link, bandwidth, reliability and delay as matrix
- Offers redundancy

#### **Frame Relay**

To connect head office with remote branches, designed network utilizes Frame relay technology. When connecting head office's private network with branch office's private network through **carrier's network** layer 2 protocol Framework is utilized. There are alternative methods are also available such as leased line but due to its cost efficiency, Frame relay technology is recommended. Implementation of frame relay in designed system is demonstrated in image below.

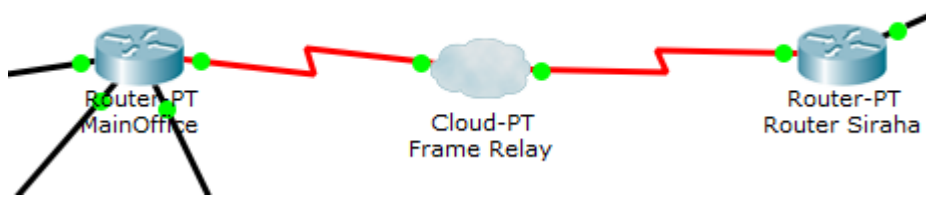


Figure 19 Use of Frame relay to connect Head office with branch office network

### **Device Selection**

To design a WAN infrastructure various devices are required. Devices identified for the designed network is evaluated below.

#### **Router**

To enable connection between two different networks, router is utilized. In Everest network, router is utilized to connected different internal network as well as connect private network with cloud. Router enables organization to provide services to its client using other network infrastructures. Router accomplishes traffic directing function. Additionally, routers are also utilized in Everest network to connect VLANs and subnets. This paper evaluates suitable router for the designed network.

#### **Cisco 2951 Router**

According to Cisco (n.d.) Cisco 2900 Series Integrated Services Routers (ISR) are intended to meet the application requests of today's medium-sized branches and to develop to cloud-based administrations. They convey virtualized applications and exceptionally secure coordinated effort through the most extensive exhibit of WAN availability at superior that offers simultaneous administrations at up to 75 Mbps. Features of this router that makes it suitable for selection is listed below here.

#### **Features**

- Large WAN connectivity option through copper, fiber, 4G, T1/E etc.
- Optimized WAN connectivity
- High Security
- High Performance
- Integrated threat control

Detailed information about features of Cisco 2900 Series Integrated Services Routers is provided below.

- 3 integrated 10/100/1000 Ethernet ports with 1 port capable of RJ-45 or SFP connectivity
- 2 service module slots
- 4 Enhanced High-Speed WAN Interface Card slots
- 3 onboard digital signal processor (DSP) slots
- 1 internal service module slot for application services
- Fully integrated power distribution to modules supporting 802.3af Power over Ethernet (PoE) and Cisco Enhanced PoE
- Security
  - Onboard hardware acceleration for VPN encryption
  - Secure collaborative communications with Group Encrypted Transport VPN, Dynamic Multipoint VPN, or Enhanced Easy VPN
  - Integrated threat control using Cisco IOS Firewall, Cisco IOS Zone-Based Firewall, Cisco IOS IPS, and Cisco IOS Content Filtering
  - Identity management using authentication, authorization, and accounting (AAA), and public key infrastructure
- Voice
  - High-density packet voice DSP module, optimized for voice and video support
  - Standards-certified VoiceXML browser services
  - Cisco Unified Border Element capabilities
  - Cisco Unity Express voicemail support.
  - Support for Cisco Communications Manager Express and Survivable Remote Site Telephony

Figure 20 Features of 2951 router (Source: [www.cisco.com](http://www.cisco.com))

#### Switch: Cisco WS-C2960X-24PD-L

Switch is used for connecting IP based resource in single LAN. Manageable switches allows to create VLANs inside switches that acts as separates LANs. For the designed network, Cisco Catalyst 2960-X model WS-C2960X-24PD-L switch is identified. Some of the key feature of this switch according to cisco (n.d.) are provide below.

#### Features

- It has 24 numbers of port that is suitable for the designed network size
- Allows to stack 8 other switches to create large switch as per requirement
- Extremely secure
- Green Energy that saves energy

Detailed feature of Cisco WS-C2960X-24PD-L switch is provided below.

**Networking**

Compliant Standards:	IEEE 802.1ae , IEEE 802.1AX , IEEE 802.1D , IEEE 802.1p , IEEE 802.1Q , IEEE 802.1w , IEEE 802.1x , IEEE 802.3 , IEEE 802.3ab , IEEE 802.3ad (LACP) , IEEE 802.3ae , IEEE 802.3af , IEEE 802.3at , IEEE 802.3az , IEEE 802.3u , IEEE 802.3x , IEEE 802.3z
Features:	Access Control List (ACL) support , ARP support , Auto-negotiation , Auto-uplink (auto MDI/MDI-X) , Cisco EnergyWise technology , DHCP support , Dynamic ARP Inspection (DAI) , Dynamic Trunking Protocol (DTP) support , Energy Efficient Ethernet , Hot Standby Router Protocol (HSRP) support , IPv4 support , IPv6 support , Jumbo Frames support , Layer 2 switching , Link Aggregation Control Protocol (LACP) , MLD snooping , Multiple Spanning Tree Protocol (MSTP) support , NetFlow , PoE+ , Port Aggregation Protocol (PAgP) support , Power over Ethernet (PoE) , RADIUS support , Rapid Per-VLAN Spanning Tree Plus (PVRST+) , Rapid Spanning Tree Protocol (RSTP) support , Remote Switch Port Analyzer (RSPAN) , Shaped Round Robin (SRR) , Trivial File Transfer Protocol (TFTP) support , Trunking , Uni-Directional Link Detection (UDLD) , Unicast Reverse Path Forwarding (URPF) , VLAN support
Form Factor:	Desktop , Rack-mountable
Jumbo Frame Support:	9216 bytes
Manageable:	Yes
Max Units In A Stack:	8
PoE Budget:	370 W
Ports Qty:	24
Power Over Ethernet (PoE):	PoE+
Remote Management Protocol:	CLI , HTTP , RMON 1 , RMON 2 , RMON 3 , RMON 9 , SNMP 1 , SNMP 2 , SNMP 2c , SNMP 3 , SSH , Telnet
Stackable:	Stackable
Status Indicators:	Link activity , Port duplex mode , Port status , Port transmission speed , System
Subcategory:	Network hubs and switches
Subtype:	Gigabit Ethernet
Type:	Switch

**Figure 21 Detailed feature of selected Cisco WS-C2960X-24PD-L switch (Source: <https://www.cdw.com/>)**

### Firewall: Cisco 5505

Firewall is technology which enables to block unauthorized access. It monitors and filter outgoing and incoming traffic based on the defined traffic rules. In developed system integrated firewall in router as well as dedicated cisco 5505 is utilized. Features of selected firewall system is provided below based on Cisco (n.d.):

#### Features

- Enhanced multilayered protection from threats
- High performance
- Robust next gen security
- Lowered power consumption

### Wireless Access Points: Aironet® 3600 Series Access Point

To provide Wi-Fi service to clients, Aironet® 3600 Series Access Point wireless access point has been selected. Cisco claims it gives up to three times data rate than market quality. Some of the features of selected wireless access points are:

- Enhanced Security module and performance
- Advanced Encryption Standard (AES)
- 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA

Cable Connection

Designed network utilizes wireless technology to provide service to its clients via Wi-Fi. But to implement network infrastructure and connect wireless access points with network switches, cable connection technology is utilized as it offers faster and secure connectivity option. **Category 6** cable which is also known as **CAT6** is utilized as its standard cable for wired connection.

IP Addressing Plan

As discussed above designed system utilizes both static and dynamic IP distribution model. IP addresses are required by network resources to recognize and understand each other. IPv4 is planned for the system. Planned IP addressing is provided in table below.

Head Office

Device/Server	IP address
Domain Controller	IP address: 192.168.1.101/24 DNS IP address: 192.168.1.102/24 Default gateway: 192.168.1.1/24
DNS server	IP address: 192.168.1.102/24 DNS IP address: 192.168.1.102/24 Default gateway: 192.168.1.1/24
DHCP	IP address: 192.168.1.103/24 DNS IP address: 192.168.1.102/24 Default gateway: 192.168.1.1/24
WEB & FTP server	IP address: 192.168.1.104/24 DNS IP address: 192.168.1.102/24 Default gateway: 192.168.1.1/24
Database	IP address: 192.168.1.105/24 DNS IP address: 192.168.1.102/24 Default gateway: 192.168.1.1/24
Application	IP address: 192.168.1.106/24 DNS IP address: 192.168.1.102/24 Default gateway: 192.168.1.1/24
Email	IP address: 192.168.1.107/24 DNS IP address: 192.168.1.102/24

	Default gateway: 192.168.1.1/24
Router Main office	Interface fa0/0 192.68.1.1/24 Interface fa1/0 192.68.2.1/24 Interface fa4/0 192.68.3.1/24 Interface fa5/0 192.68.4.1/24
Clients	Clients will receive dynamic IP from DHCP

Branch Office Siraha

Device/Server	IP address
Read Only Domain Controller	IP address: 10.10.10.11/24 Default gateway: 10.10.10.1/24
Read Only DNS server	IP address: 10.10.10.12/24 Default gateway: 10.10.10.1/24
DHCP	IP address: 10.10.10.13/24 Default gateway: 10.10.10.1/24
Router Siraha office	Interface fa0/0 10.10.11.1/24 Interface fa1/0 10.10.12.1/24 Interface fa4/0 10.10.13.1/24 Interface fa5/0 10.10.14.1/24
Clients	Clients will receive dynamic IP from DHCP

Branch Office Pokhara

Device/Server	IP address
Read Only Domain Controller	IP address: 172.16.10.11/24 Default gateway: 172.16.10.1/24
Read Only DNS server	IP address: 172.16.10.12/24 Default gateway: 172.16.10.1/24
DHCP	IP address: 172.16.10.13/24 Default gateway: 172.16.10.1/24
Router Pokhara office	Interface fa0/0 172.16.11.1/24 Interface fa1/0 172.16.12.1/24 Interface fa4/0 172.16.13.1/24 Interface fa5/0 172.16.14.1/24
Clients	Clients will receive dynamic IP from DHCP



Branch Office Hetauda

Device/Server	IP address
Read Only Domain Controller	IP address: 192.167.0.11/24 Default gateway: 192.167.0.11/24
Read Only DNS server	IP address: 192.167.0.12/24 Default gateway: 192.167.0.11/24
DHCP	IP address: 192.167.0.13/24 Default gateway: 192.167.0.11/24
Router Hetauda office	Interface fa0/0 192.167.0.1/24 Interface fa1/0 192.167.1.2/24 Interface fa4/0 192.167.2.3/24 Interface fa5/0 192.167.3.4/24
Clients	Clients will receive dynamic IP from DHCP

Branch Office Nepalgunj

Device/Server	IP address
Read Only Domain Controller	IP address: 172.31.0.1/24 Default gateway: 172.31.0.1/24
Read Only DNS server	IP address: 172.31.0.1/24 Default gateway: 172.31.0.1/24
DHCP	IP address: 172.31.0.1/24 Default gateway: 172.31.0.1/24
Router Nepalgunj office	Interface fa0/0 172.31.0.1/24 Interface fa1/0 172.31.1.1/24 Interface fa4/0 172.31.2.1/24 Interface fa5/0 172.31.3.1/24
Clients	Clients will receive dynamic IP from DHCP

BandwidthSpeed Plan for User

Designed WAN infrastructure is planned keeping business requirement in mind. Designed system will provide Wi-Fi service to its clients. Maximum capacity of 9.6 Mbps will be provided to corporate clients whereas maximum of 1.2 Mbps will be provided to end users.

**User**

Designed WAN infrastructure has utilized various technologies to ensure satisfaction of user expectation. Size of network, clients, and services can easily increase as designed system is very scalable. Selected wireless access points has ability provide quality service and support large number of clients.

**Overall Justification of Proposed Design**

While designing the system various server technologies is identified and utilized to support network infrastructure. These server technologies includes dc, DNS, email server etc. Additionally, designed system has VPN server to secure connection between head office and branch offices. This paper also designs for proper VLAN plan. To reduce to requirement of extra switches and improve security enhancements, each department is placed in different VLANs.

DHCP server is utilized to allocate IP addresses dynamically to its clients. Whereas wireless routers has inbuilt DHCP for its clients. With DHCP no manual IP configuration is required in each clients. As it is must for network resources to have proper IP address configuration to be able to understand by network infrastructures, this design prepares proper plan for the WAN infrastructure. Designed network has different networks that requires to understand each other to achieve business requirement, for this proper routing solution is identified and evaluated. Enhance interior gateway routing protocol helps to achieve routing requirement with minimal resource/bandwidth utilization. And finally, several devices requirements are identified and evaluated. Based on the features of each device which includes Router, Switches, firewall and wireless access point, appropriate device model has been selected which enhances the service and security quality of the system. Hence, justification for proposed design has been made.

**References**

- Beal, V. (n.d.) VLAN [Online] Available:  
<http://www.webopedia.com/TERM/V/VLAN.html>
- Cisco (n.d.) Cisco 2900 Series Integrated Services Routers [Online] Available:  
<http://www.cisco.com/c/en/us/products/routers/2900-series-integrated-services-routers-isr/index.html>
- Cisco (n.d.) Cisco ASA 5500-X Series Firewalls [Online] Available:  
<http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/index.html> Accessed [2/11/2015]
- Cisco (n.d.) Cisco Catalyst 2960-X Series Switches  
<http://www.cisco.com/c/en/us/products/switches/catalyst-2960-x-series-switches/index.html>
- Indiana University (n.d.) what is DHCP [Online] Available: <https://kb.iu.edu/d/adov>  
Accessed [2/11/2014]
- TECHREPUBLIC (n.d.) Select the right routing protocol for your network  
<http://www.techrepublic.com/article/select-the-right-routing-protocol-for-your-network/>  
Accessed [2/11/2015]

**Task 7**

**Critically** review and test the WAN [3.3, M3]

**Introduction**

Everest Network Pvt. Ltd is a growing network service provider organization that provides network services in capital city of the nation, Kathmandu. Along with service sell, organization also sells and support networking devices. To grow the business even further, company has identified need of branch offices in several other parts of Nepal. Growth plan includes Pokhara, Siraha, Nepalgunj, Hetauda city to distribute its services. Planned project includes network infrastructure design for each branches as well as design, plan, implement and evaluation of overall WAN solution. Company plans to provide Wi-Fi service of maximum capacity of 1.2 Mbps. Meanwhile, company also plans to provide fast internet service of maximum capacity of 9.6 Mbps to its corporate clients. It is also required to plan proper routing solution for the WAN infrastructure.

Various tools and technologies were identified while designing the WAN infrastructure before the implementation phase. Server technologies such as domain controller, web and ftp, email, application, VPN, DNS etc. is planned in design to support network infrastructure of the system. This enables organization to achieve basic networking needs. Developed system utilizes technologies such as DHCP, VPN to satisfy the business requirement. Appropriate routing device and routing protocol is utilized to implement routing solution in WAN infrastructure. Similarly, suitable cisco switch is implemented to support networking environment. Frame relay technology is utilized to connect head office with remote branch offices to provide centralized network.

**Body**

Developed system utilized DHCP technology to provide IP addresses to clients. This enables dynamic IP distribution which means no manual configuration is required. As company has large customer segment that uses Wi-Fi service, implementation of static IP can be really complicated hence, DHCP provides great mechanism to support large clients. Other technology utilized by develop system is VLANs. This allows to create smaller VLANs to allow single switch works as multiple networks. This enables administrator to separate departments for enhancing maintenance and security of the system. Even if two department is supported by single switch, due to VLANs, they behave as different network. Helps to increase performance by broadcast limitation.

Implemented system utilizes highly manageable router (Cisco 2951) and highly manageable cisco switch as well. These devices has features that improves the state of the implemented WAN

infrastructure. Another key strength of the system is it utilizes dedicated firewall device to secure server infrastructures. One of the other significance of this system is implementation of EIGRP as routing protocol. This provides fast and dependable routing solution to the system. As this protocol consumes very little bandwidth and CPU resources. High performance access point is utilized to provide Wi-Fi service to its clients. It is also worth talking that implemented system is highly scalable as it can support larger number of devices, clients, networks. As developed system has many positive aspects, it has few limitations as well. Table below demonstrates strengths and weakness of implemented system properly.

S.N.	Strengths	Weaknesses
1.	Use of EIGRP enables to design network not worrying about hop size.	Developed system utilizes EIGRP technology which is supported by Cisco brand only. This limits choices of device for the future.
2.	Very scalable network as switches support stacking, and very large clients are supported using DHCP	As system is designed and developed, only basic testing of the system is done. Critical testing of the system is not performed yet. Which
3.	Dedicated firewall to secure server department.	This project is conducted without any prior feasibility study which out allow to analyze viability of project based on economy, social, technology, schedule etc.
4.	High security and performance from high end device selection	Implemented system uses devices with very high specification which allows to provide service with very high quality. But these devices are expensive than alternative devices with lower specification.

### **Conclusion**

This paper critically reviewed implemented WAN infrastructure. Developed system utilizes various technologies to enhance to performance, security and reliability of the system. Frist of all network infrastructure for each branches and head office is designed and implemented. Server technologies such as dc, email, ism, web etc. are implemented to support basic requirement of the system. While reviewing the system, it is noted that use of high end devices has enhanced performance of the system. System uses high end dedicated firewall to secure critical resources.

Developed system is designed to be very scalable as additional clients are easily supported by the system. Additional computers, servers in office is also supported. Meanwhile, system does have few weaknesses. This includes, use of expensive devices, future choice being limited to cisco brand and absence of proper feasibility study to ensure viability of the system. Finally, critical review of the system showed absence of critical test and maintenance plan. It is recommended to perform test of the system to find misconfigurations and perform necessary maintenance procedure.

### **Testing of WAN System**

Testing of the WAN infrastructure is essential phase. It allows to find possible misconfiguration in system and enables administrator to fix them. Testing of the developed system includes testing of routing solution, VLANs configuration, DHCP IP distribution, connection between server and clients, Wi-Fi connectivity, etc. Performed test and test results are documented in table below in terms of test logs. This paper further analyze the test results to identify misconfigurations.

#### **Test Log**

<b>What was tested: <i>Internal Routing</i></b>		<b>Date: 10/18/2015</b>
<b>S.N.</b>	<b>Expected Output</b>	<b>Actual Output</b>
1.	Computer with IP address of 192.168.2.1/24 should not be able to ping 192.168.1.101/24 before routing configuration is done	Pinging 192.168.1.101 before routing configuration showed 100% loss with request time out message
<pre>PC&gt;ping 192.168.1.101  Pinging 192.168.1.101 with 32 bytes of data:  Request timed out. Request timed out. Request timed out. Request timed out.  Ping statistics for 192.168.1.101:     Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),</pre>		
2.	Computer with IP address of 192.168.2.1/24 should be able to ping 192.168.1.101/24 after routing configuration is done	Pinging different network of 192.168.1.101 from 192.168.2.1 showed successful ping result.

```

PC>ping 192.168.1.101

Pinging 192.168.1.101 with 32 bytes of data:

Reply from 192.168.1.101: bytes=32 time=3ms TTL=127
Reply from 192.168.1.101: bytes=32 time=1ms TTL=127
Reply from 192.168.1.101: bytes=32 time=0ms TTL=127
Reply from 192.168.1.101: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

```

**What was tested: VLAN configuration****Date: 10/18/2015****S.N.****Expected Output****Actual Output**

1.

Show VLAN command should display  
all VLANs

Showed VLAN table in switch

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/6, Fa0/10, Fa0/11 Fa0/12, Fa0/15, Fa0/16, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/24, Gig0/1, Gig0/2
101 Servers	active	Fa0/1, Fa0/2, Fa0/3, Fa0/5
102 SalesMarketing	active	Fa0/7, Fa0/13
103 HR	active	Fa0/8, Fa0/14
104 Account	active	Fa0/23
105 CustomerCare	active	Fa0/9, Fa0/17

2

PC1 from HR VLAN should not be  
able to ping PC2 from ACCOUNT  
VLAN

Member of one VLAN was not able to  
ping member of another VLAN

```

Pinging 192.168.1.104 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.104:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

**What was tested: DHCP Configuration****Date: 10/18/2015****S.N.****Expected Output****Actual Output**

1.

After Wi-Fi access, client should get  
dynamic IP address

Smartphone device dynamically  
received IP address from router

```

Wireless0 Connection:(default port)

Link-local IPv6 Address.....: FE80::290:CFF:FE32:6EED
IP Address.....: 192.168.0.102
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.0.10

3G/4G Cell1 Connection:

Link-local IPv6 Address.....: FE80::203:E4FF:FEA8:E6CE
Autoconfiguration IP Address.....: 169.254.230.206
Subnet Mask.....: 255.255.0.0
Default Gateway.....: 0.0.0.0

```

**Analysis:**

2	Resources should be able to get dynamic IP address from DHCP server
---	---

```

PC>ipconfig /renew

IP Address.....: 192.168.1.150
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DNS Server.....: 192.168.1.102

```

**What was tested: *Connectivity with Branch Office*****Date: 10/18/2015****S.N.****Expected Output****Actual Output**

1.

Should able to ping Siraha branch router from head office

Successfully pinged Siraha branch router

```
Router#ping 10.10.10.1
```

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

```

2.

Should able to ping Pokhara branch router from head office

Successfully pinged Pokhara branch router

```
Router#ping 172.16.11.1
```

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.11.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

```

3.

Should able to ping Hetauda branch router from head office

Successfully pinged Hetauda branch router



```
Router#ping 192.167.0.1
```

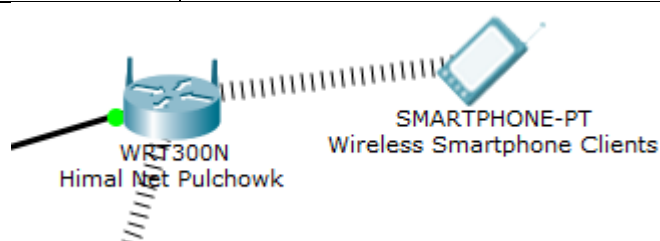
```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.167.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

4.	Should able to ping Nepalgunj branch router from head office	Successfully pinged Nepalgunj branch router
----	--	---

```
Router#ping 172.31.0.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

<b>What was tested: Wi-Fi configuration</b>		<b>Date: 10/18/2015</b>
<b>S.N.</b>	<b>Expected Output</b>	<b>Actual Output</b>
1.	Client should able to connect to Wi-Fi after authentication	After providing password, Wi-Fi access was successful



<b>What was tested: Web server Configuration</b>		<b>Date: 10/18/2015</b>
<b>S.N.</b>	<b>Expected Output</b>	<b>Actual Output</b>
1.	Clients should able to browse website	Browsing website from client computers was successful

## Web Browser

< > URL  Go St

# Welcome to Himalayan Network

## Join Himalayan Network Today for fast internet

<b>What was tested: Neighbor Search</b>		<b>Date: 10/18/2015</b>
<b>S.N.</b>	<b>Expected Output</b>	<b>Actual Output</b>

1.	Router should able to find all neighbors			Router was able to scan all neighbors	
Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
Switch	Fas 1/0	52	S	2960	Fas 0/1
Switch1P2	Fas 9/0	65	S	2960	Fas 0/1
KalimatiSwitch	Fas 1/0	172	S	2960	Fas 0/1
PulchowkSwitch	Fas 9/0	125	S	2960	Fas 0/1

### Analyzing Test results

Various tests were conducted on implemented WAN environment to check configuration of the system and find any possible misconfiguration. Routing solution, VLANs configuration, DHCP IP distribution, connection between server and clients, Wi-Fi connectivity etc. were tested and test result were documented as test logs. To test the routing configuration pinging from two different networks are tested before and after routing configuration. Test results shows after implementation of EIGRP routing configuration, different networks were able to understand each other. Similarly, test further checked the configuration of VLANs by trying to ping resources from different VLAN which was not successful, which indicates configuration is made correctly.

Test results showed that Wi-Fi clients and other resources with DHCP enabled was able to obtain IP address dynamically. Each branches was tested for connection with head office, all branch router was able to connect with head office. This ensures implementation of centralized network. Similarly, web server test and router neighbor scan test was performed which showed proper configuration is made. Hence testing of the system has be carried out, though no significant issue has been found, it is recommended to carry out more in-depth test to find any possible issue and take proper action to address them.

## **Task 8**

**Monitor and troubleshoot** the WAN and **Resolve** WAN issues to improve security, reliability and performance. [4.1, 4.2]

### **Introduction**

WAN infrastructure for Everest Network is already planned, designed and implemented. Implemented system has been passed through various test procedure and critical review. Newly developed system is able to fulfill business requirements. But, it is essential to monitor and maintain the system continuously to ensure optimal performance and security. This paper documents monitoring and troubleshoot process of the system. Monitoring of system includes analyzing traffics, bandwidths, resource usage etc.

### **Network monitoring**

Network monitoring is process of keeping close eye on continuous traffic status, bandwidth status, routing updates etc. It monitors resource usage to ensure optimal operation of network. In other words, it is process of fixing potential issue before it creates catastrophe. Another benefits of monitoring is it allows to identify issue if any problem arises. This paper documents various monitoring tools utilized in implemented system to track traffic bandwidths etc.

### **NetQoS**

NetQoS is network monitoring tools that is acquisitioned by CA technologies in 2009. It offers hundred percent traffic visibility with allowing to monitor which application is consuming most bandwidth. If current system can handle more video and voice traffic is analyzed with this tools. CA Network Flow Analysis is a system traffic observing arrangement that can offer you some assistance with optimizing your system foundation for better network performance. With improved deceivability into your system's applications, hosts, discussions and QoS data, you can proactively deal with your system to diminish blackouts, tackle issues quicker and guarantee proficient and savvy operations. CA Network Flow Analysis can offer you some assistance with aligning assets to bolster business results, pick up believability and backing with information driven choices and quit being the default focus for fault. NetQoS is utilized in current system to monitor latency and network performance. Some benefits of NetQoS is listed below.

- Quicker issue resolve
- Improved application performance
- Reduced structure expenses

## Latency Monitor

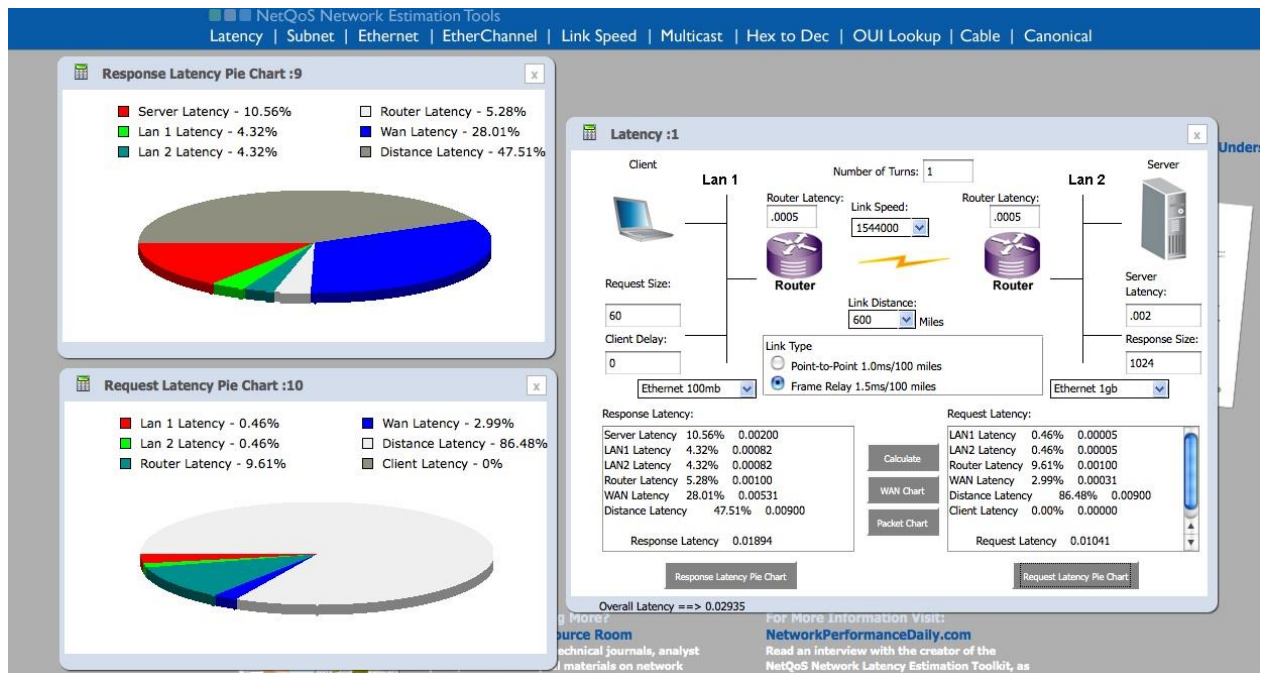


Figure 22 Latency Calculation using NetQoS

## Performance Monitor

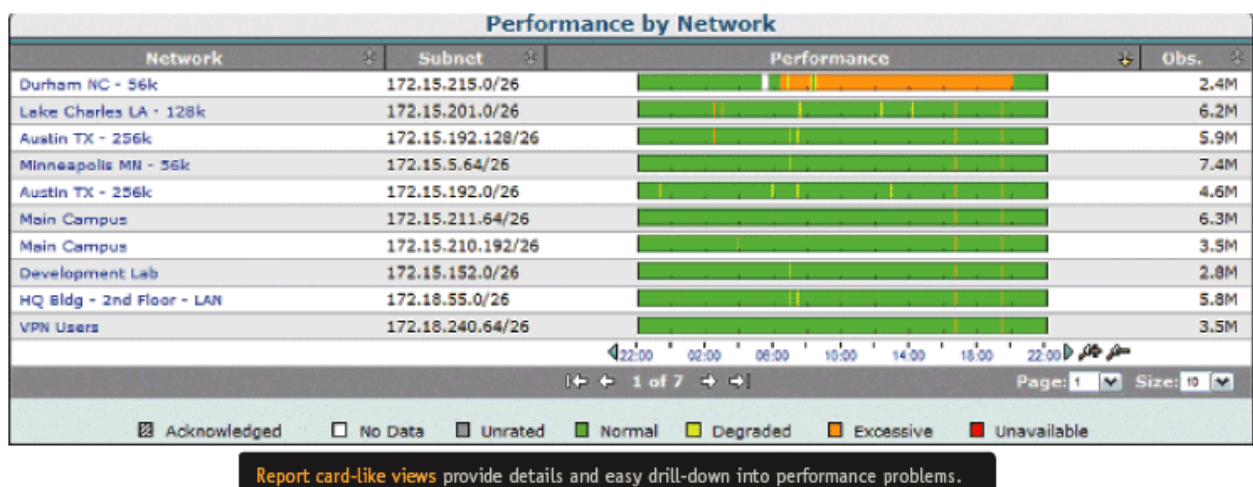


Figure 23 Performance Monitoring using NetQoS

## Solar wind Monitoring

This tool enables to Recognize, analyze and resolve traffic issues while studying Track reaction time, accessibility and uptime of switches, switches and other SNMP-empowered gadgets. This tool helps to examine and screen system transmission capacity execution and movement designs. With this tool administrators distinguish transmission capacity hoards and see which applications are utilizing the most transfer speed. One of the benefit of this tools is it graphically show system

traffic measurements continuously by means of dynamic maps. This tool is utilized in current system to monitor resources and bandwidth status.

### All Details

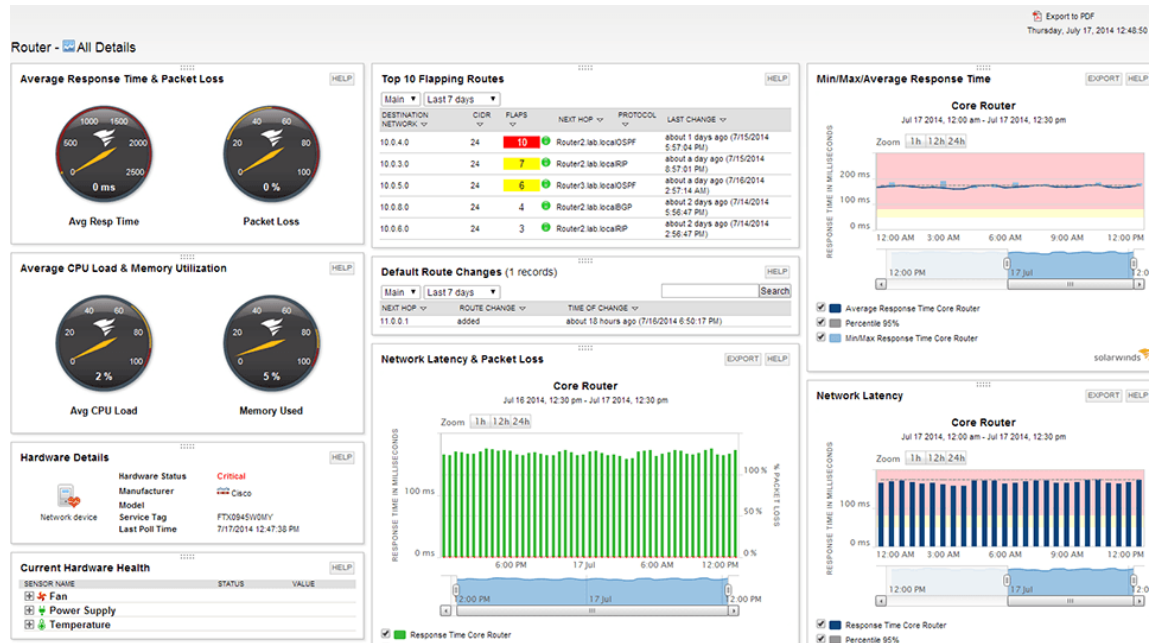


Figure 24 Network Monitoring using Solar Wind

### Bandwidth monitor

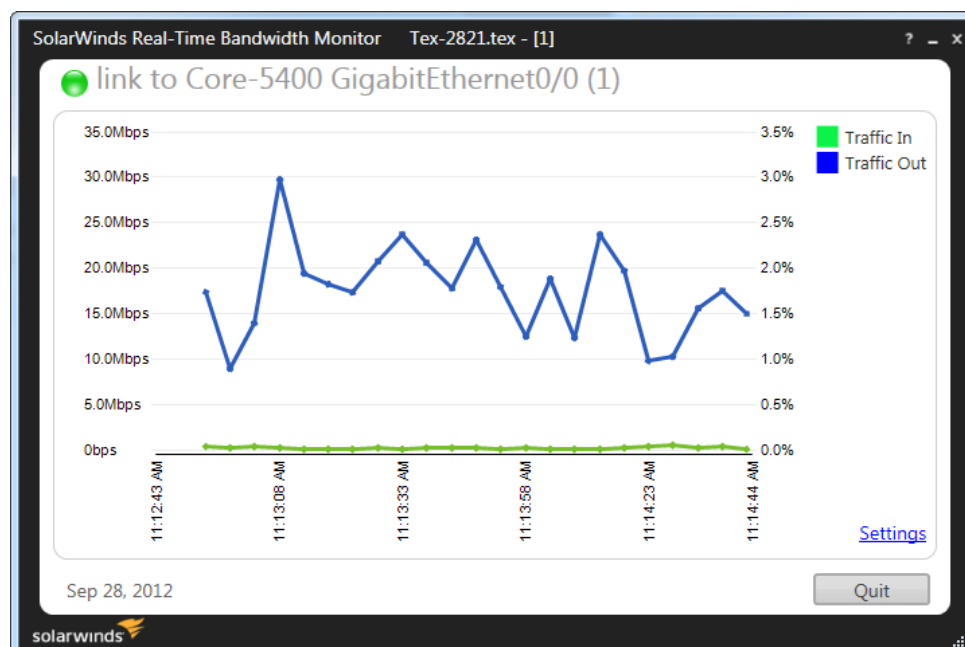
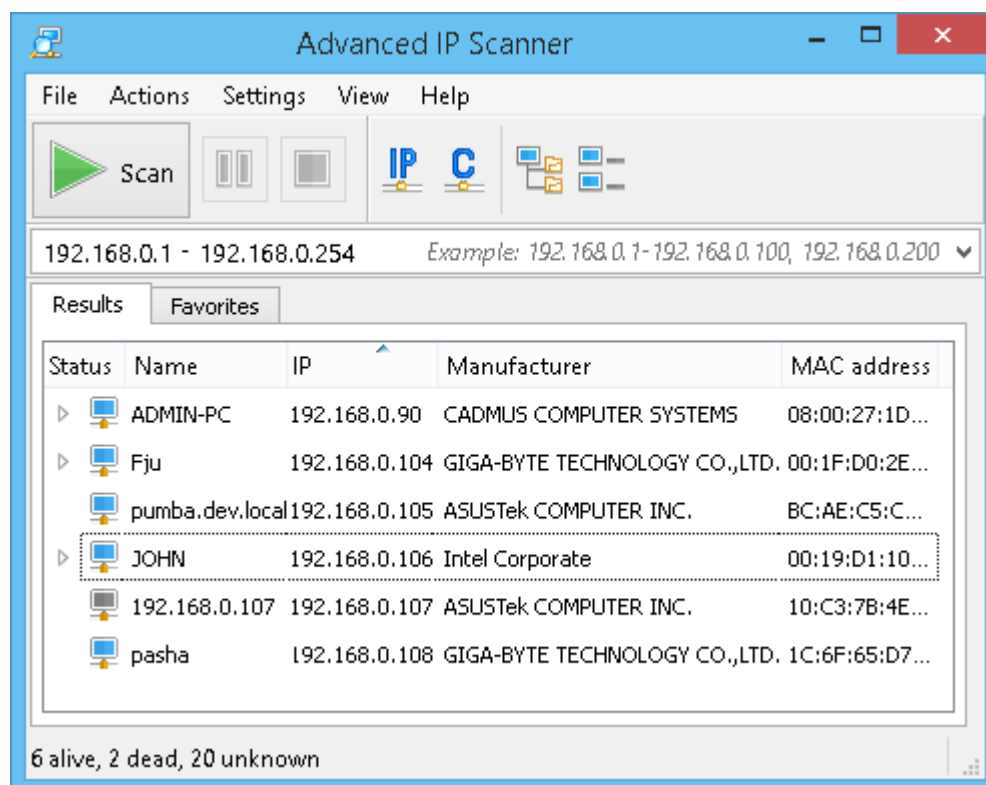


Figure 25 Bandwidth Monitoring Using Solar wind

### Advanced IP Scanner

Advanced IP scanner is Dependable network scanner. The application scans all resources available in the network. This tool allows to remotely turn off computer/resources. This tool very easy to use. This tool is utilized to scan all available resources in the system while troubleshooting network infrastructure of head office of branch.



### Resolving identified Issues

Various monitoring tools is utilized to monitor the network system and identify issues to resolve them. During monitoring few issuers are monitored.

#### Packet Loss

Possible cause	Solution and Recommendation
Duplex mismatch	When different duplex setting is applied in two end of the network it can cause packet loss, ensure all ends are using similar duplex setting.
Link congestion	This happens when large traffic is trying to pass through network line capacity. Ensure network line is large enough to support all traffic.

Firewall blocking specific traffic	Sometimes packet loss can be caused by firewall filtering. Make sure firewall is not blocking traffic to cause such issues
Bad/Broken cable/loose connect	Ensure cable is in good shape and connection is not loose

#### Connection with HR VLAN broken

Possible cause	Solution and Recommendation
Switch has no power	Make sure VLAN is in ON state and recheck connection
Cable unplugged	Make sure cable is plugged into right interface
Bad Cable	Make sure cable is in good state, replace it if necessary
Wrong Cable Type	Make sure correct cable type is used
Faulty interface	If problem persists change VLAN configuration to other interfaces as current ones may have faulty ones.

**Task 9**

**Critically evaluate** the performance of WAN. [4.3]

**Introduction**

Wide area network is becoming progressively significant component of accompanying businesses. It is essential for WAN to give maximum performance to increase productivity of the business as demand of WAN performance is ever growing. Wide Area Network (WAN) efficiency is one of the leading concerns for organizations. Application performance over the WAN are assailed by range of issues. These issues includes congestion, low bandwidth, packet loss, latency etc. This paper evaluates various components that helps to analyze and improve performance of WAN.

**Network Monitoring Tools**

It is very simple to understand the fact that WAN infrastructure helps to minimized functioning cost, take full advantage of employee productivity and generate more revenue but in the same time it is essential to ensure performance of WAN does not drop. According to INFOVISTA (n.d.) proactive management of WAN performance can be complicated but with constant monitoring and inclusive management plan, IT organizations are able to mitigate the effect of performance issues on the service quality. For this, consistent network system monitoring is a necessity.

According to HELPSYSTEMS (n.d.) network monitoring helps to monitor, optimize and secure complex IT infrastructure environments. It enables to ensure that all server technologies, resources are functioning correctly, to satisfy the business requirement. Any sort for WAN performance issue can disturb productivity, customer involvement and most significantly the status of organization.

**Benefits of Network monitoring of Everest network**

Developed WAN infrastructure for Everest networking utilizes network monitoring tool to constantly keeping tab on network resources for any component getting slow or fail. Such events are notified to system administrator via either alarm, SMS or emails. Benefits of utilizing such tools according to NAGIOS (n.d.) are noted below:

- With network monitoring, unresponsive resources are identified and system administrator/technical team is notified.
- Detailed reports that can be analyzed to plan troubleshoot
- Improved Service, application, server accessibility



- Quicker identification of network and protocol failure.

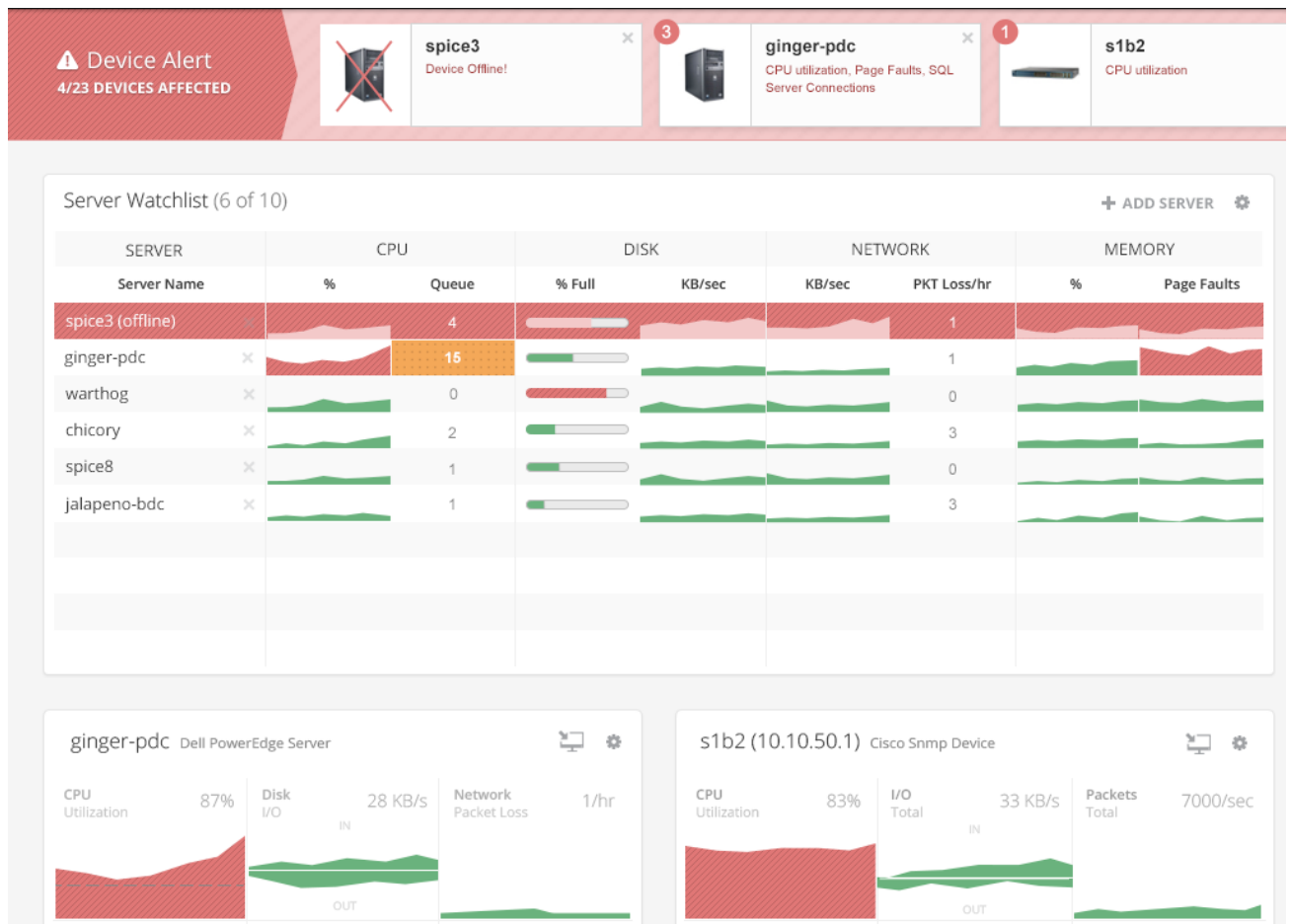


Figure 26 Network Monitoring

### Traffic Analysis

Traffic analysis is the procedure of recording, checking on and breaking down traffic movement with the end goal of security, performance and/or general system operations and administration, Technopedia (n.d.). It is the procedure of utilizing manual and mechanized methods to audit granular-level point of interest and measurements related to traffic of network. It is basically performed to gain detailed knowledge of traffic/network packets that are flowing over a network.

### Benefits of Traffic analysis of Everest network

To ensure performance of Everest Network WAN infrastructure various traffic analysis tools are implemented to understand traffic flow in the network. Following are the benefits of using traffic analysis in developed system:

- Studying and assessing the network utilization

- Identify malicious packets

### **Bandwidth Monitoring**

Monitoring bandwidth allows to keep track of bandwidth to provide instant report. Bandwidth monitoring is a system for breaking down the information streaming over a network. It is method of calculating and handling the data packets on the network. It includes keeping track of bandwidth utilization of leased line, network devices like switches, routers and network connection. It helps to identify application or protocol consuming the most of the bandwidths. This allows to ensure critical applications are prioritized to receive bandwidth. Bandwidth monitoring on developed WAN system for Everest network allow to have following benefits:

- Screen, log and investigate network bandwidth, SIMPLELIZE (n.d.).
- Study bandwidth consumption by application and protocol
- Alter administrator when predefined criteria is matched.

### **WAN Optimization**

An expression used to portray applications and items used to oversee and quicken the stream of information over a wide area network (WAN), Webopedia (n.d.). A percentage of the particular advances utilized as a part of WAN enhancement incorporate reduplication, information compression systems, reserving, and VPN tunneling, caching and different innovations.

A perfect WAN Optimization arrangement will permit administrator to organize traffic, and to ensure certain bandwidth availability to critical application. They can block undesirable (in and outbound) activity, permit it at certain time amid the day, offer need to specific has, and authorize numerous other related arrangements. They will enable lower latency and high throughput for the critical application. With WAN optimization package for implemented Everest network, very less manual monitoring and troubleshooting would be required.

### **Benefits of WAN optimization in Everest network**

- Quicker file access
- Increased speed between head office and branch office connection
- Improved WAN performance for all application including applications that are directly affected and applications that are not affected.

### **Checking Rules**

WAN infrastructure consist of various rules such as Access control list rules, firewall rules etc. These rules ensures performance of the WAN. These rules permits regulation of unrestrained traffic. Access control rule is used for controlling IP traffic, cisco (n.d.). Similarly firewall is also used for controlling traffics as well. Rechecking these rules helps to improve security performance of the WAN.

### **Conclusion**

This paper evaluated various technologies that allows to ensure optimal WAN performance. Utilization of proper network monitoring allows to ensure optimal bandwidth, resource configuration. **Monitoring** tools like traffic monitor, bandwidth monitoring helps in the Quality of service management. Traffic intensive services are prioritized for **bandwidth** utilization. Developed WAN infrastructure for Everest networking would benefitted from such WAN performances to ensure quality service to its clients. Furthermore technology like WAN optimization is also discussed and its potential benefit to WAN performance is evaluated. It is recommended that proper network monitoring tools should be utilized to ensure optimal performance from developed wan system while regular checking of **rules, configuration, user access** etc. guaranty the performance and security of the system. It is also recommended that if WAN required added level of performance, suitable WAN optimization package should be implemented which automatically enhances the quality of system.

**References**

- Cisco (n.d.) Configuring Access Rules [Online] Available:  
[http://www.cisco.com/c/en/us/td/docs/security/asa/asa83/asdm63/configuration\\_guide/config/access\\_rules.html](http://www.cisco.com/c/en/us/td/docs/security/asa/asa83/asdm63/configuration_guide/config/access_rules.html) Accessed [4/11/2015]
- HELPSYSTEMS (n.d.) Top Benefits of Network monitoring  
<http://www.helpsystems.com/intermapper/resources/articles/top-benefits-network>
- INFOVISTA (n.d.) Wide Area Network (WAN) Performance Management [Online] Available: <http://www.infovista.com/solutions/WAN-performance-management> Accessed [4/11/2015]
- NAGIOS (n.d.) Network Monitoring Tools from Nagios [Online] Available: <https://www.nagios.com/solutions/network-monitoring-tools/>
- SIMPLELIZE (n.d.) Understanding Real-time Bandwidth Monitoring & Its Benefits  
<http://simplelize.com/internet/understanding-real-time-bandwidth-monitoring-its-benefits>
- Technopedia (n.d.) Network Traffic Analysis  
<https://www.techopedia.com/definition/29976/network-traffic-analysis>
- Webopedia (n.d.) WAN optimization [Online] Available:  
[http://www.webopedia.com/TERM/W/WAN\\_optimization.html](http://www.webopedia.com/TERM/W/WAN_optimization.html) Accessed [4/11/2015]