International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Policy Based an Effective and Efficient Bandwidth Optimisation for Performance Enhancement of an Organisation

Ashok Kumar Tripathi[1], Ramesh Bharti [2]

[1]MTech Research Scholar, Department of Electronics and Communication Engineering, Jagannath University, Jaipur, India

[2]Associate Professor, Department of Electronics and Communication Engineering, Jagannath University, Jaipur, India

Abstract: ***Bandwidth management is a generic term that describes the various techniques, technologies, tools and policies employed by an organization to enable the most efficient use of its bandwidth resources 'Efficient use' means both the minimisation of unnecessary bandwidth consumption and the delivery of the best possible levels of service to users.' Bandwidth resources' refers to the bandwidth of a network, which might be a local campus network, a Regional Area Network. The IT managers of all organisations are very much concerned to make proper utilisation of available network bandwidth and to make it sure that sufficient bandwidth is available to every user/application for productive work. With the exponential growth of digitally rich contents and Intranet computing demands for the last few years, the users often perceive that there is insufficient bandwidth available to completely satisfy their needs whereas the problem lies at the end of management who fails to identify certain bandwidth eating unproductive applications. In this paper an attempt is made to analyse and implement a policy framework for optimal utilisation of Intranet bandwidth by considering Organisational Networking System (ONS) of Chanakya Organisation, as a case study. To implement Policy-Based bandwidth management we applied ACLs on: gateway routers; content filters on gateway routers; appropriate network nodes; proxy caches, Apply content filters to restrict prohibited content. To restrict applications and protocols and to priorities traffic, install various bandwidth shaping and priorisitation techniques. Monitor users and, where necessary, prevent their accessing prohibited Content. The findings of the study indicate that there is a need of good netiquette of all stakeholders as per IT policy. The IT policy must be framed and enforced for optimal utilisation of bandwidth in Chanakya***

Keywords: Bandwidth Management, Organisational Networking System (ONS), Netiquette, Intranet Usage Policy, Traffic Filtering, Mission Critical Application, Network Monitoring.

1. Introduction

The organisational networking system is one of the most essential assets for any organisation to support and deliver numerous key services. This is also an integral part of computing environment that supports organisanal business activity and official works [6]. It is not viable for any big organisation to operate if it is not connected to the entire offices spread across the country side. This means, the survival is dependent on good working access of Intranet. Effective Intranet Access requires an information delivery chain consisting of four essential links: (*i*) content, (*ii*) connection, (*iii*) local resources, and (*iv*) bandwidth management. The content must be in a form accessible by the user. The connectivity is essential to access the content. Furthermore, the resources are required to deliver the content to the end users. These include the local network, computers, necessary tools and skills of network administration team. But bandwidth management is the core issue that attracts attention to provide seamless flow of information. Without proactive management, network capacity fills with viruses and inappropriate traffic, and the connection becomes ineffective [12]. In that case, network management becomes essential. The network management is defined as the control, planning, acquisition, allocation, deployment, coordination and monitoring of the resources of the network [6]. In the current paper, one of the core issues of network management system, i.e. to make available adequate bandwidth is discussed in detail by considering case study of Chanakya Organisation. This organisation has various categories of users with varying network requirements and service utilisation trends. This paper has also tried to identify the major bottleneck applications which generally eat one of the most valuable and limited resources of the organisation's network, i.e. bandwidth followed by designing of policy framework by considering both technical and managerial possible solutions.

2. Necessity of Bandwidth Management

The bandwidth simply represents the capacity of the communication media to transfer data from source to destination. Wider the route/path for data transmission, more packets of information will be transmitted to the user's Intranet enabled devices. Bandwidth is a gross measurement, taking the total amount of data transferred in a given period of time at a particular rate, without taking into consideration the quality of the signal itself [10]. Furthermore, the bandwidth is responsible for data transfer speed and commonly used in Intranet connections. Bigger the bandwidth quota is, the higher the connection speed and hence quicker it will be to upload and download information. Various Intranet connections are offering different bandwidth standards. For instance, the traditional dial-up Intranet Connection provides a very narrow bandwidth limit of about 56 kbps, while the current broadband connections allow data transfer at much higher speed ranging from 128 kbps to 2 mbps. Bandwidth is both absolutely and relatively much more expensive for any organisation. Many organisations are finding that they still do not have reliable, usable Intranet Access for their offices and staffs despite considerable investment. Improving the

performance of the information delivery chain is urgent if organisation and staffs are to be benefited from the Intranet and take part in the organisational activity [9].

3. Background to the Problem

Chanakya is a virtual org having large network infrastructure. The network is spread across the country and headquarter is located in City [3]. The initial networks was functioning on 2 mbps for voice and file transfer purpose. Automation of org started on 2000 and by 2012 the various networks based application increased manifold . Networks was used for voice, data transfer, video, photo, emails, file transfer, websites and online database accesses activity. The Bandwidth has been increase up to 8 mbps by different via media like leased line, wireless, microwave links and VSAT. The network started facing congestion and mission critical applications were not accessible across the offices and field units of Chanakya. The maximum users were accessing the networks during day time from morning 8 am to 6 pm.

Chanakya were under pressure to provide their staff and offices with reliable Intranet access. As Intranet connectivity is increasingly becoming a strategic resource for firm management, a robust Branch office network with good connectivity to the Intranet is no longer a luxury to a Chanakya, in actual fact, it is now a basic necessity. The use of the Intranet can enhance the efficiency and capacity of Chanakya. Despite considerable investment in bandwidth, many of these Area offices are still finding themselves not having reliable, usable Intranet access for their staffs and offices.

The demand for bandwidth is constantly rising and the overall bandwidth usage continues its upward trend. A definite trend is continuing towards multimedia websites, which contain bandwidth-hungry images, video, animations, and interactive content. Staff uses the Intranet in many different ways, some of which are inappropriate or do not make the best use of the available bandwidth. Not all of these activities could be described as having much official worth and indeed some may be viewed as undesirable by any standards. Bandwidth is often consumed by low priority, bandwidth hungry uses for non-official purposes. However, restricting this altogether may not be the solution since this leads to frustration on the part of the users across the Chanakya.

As the popularity and usage of heavy bandwidth consuming applications grows and the number of network users multiplies, the need for a concerted and co-ordinate effort to monitor bandwidth utilisation and implementation of effective bandwidth management strategies becomes increasingly important to ensure excellent service provision. The absence of a bandwidth management strategy will leave a Chanakya's work at risk of being hopelessly bogged down, to the point where users are denied access to this valuable resource. Even in situations where high amounts of bandwidth are available, controls, monitoring and optimization are necessary because users will always find ways to fill the available amount of bandwidth. Since bandwidth is a strategic resource, the efficient usage and management of such a resource should always be a priority. Without bandwidth management, mission critical applications would be starved of bandwidth, disrupting services that impact the operational activities of Chanakya.

4. The Problem

The demand for bandwidth within Chanakya is on a constant rise. The available bandwidth is generally not enough to meet demands and to support optimal usage. If Area offices and field units are to participate in high-end quality works, then availability of required bandwidth is must. The major challenges experienced by Chanakya are:

(a) Staff' overuse of undesired applications.
(b) Violations of network due to peer–to-peer (P2P) file sharing.
(c) Poor application performance and Quality of Experience (QoE) during congestion.
(d) Mission critical application not able to access in last end office and field units.
(e) Experience of sluggish network speed during peak office hours.
(f) Sudden very less bandwidth availability at user end and non response of web enabled hosted applications.

Inappropriate use of existing bandwidth, due to absence of bandwidth management strategies promotes bandwidth wastage on unwanted traffic such as viruses, music and movie download by some users . The largely unrestricted access exposes the Intranet connectivity to bandwidth-hogging applications such as peer-to-peer (P2P) file sharing and media streaming. Audio and video streaming applications embedded in Web sites have grown in popularity among staffs. Although chanakya have increase their Intranet capacity by purchasing additional bandwidth from one or more Intranet Service Providers (ISPs), it is very expensive to do so because the price of bandwidth is still exorbitantly high. No matter how much more bandwidth is bought, a point will be reached when one can no longer buy more bandwidth and therefore the need to look to bandwidth management is necessary. Furthermore, increasing Intranet capacity cannot be done affordably considering the rate at which unmanaged applications consume it. It is therefore the duty of the Information Technology (IT) department to make sure that the available Intranet facility is effectively and optimally used to support the core business of a Chanakya. It is now recognized that one of the tasks that IT directors need to tackle is the management of bandwidth. The challenge of this problem is how to make more bandwidth available and how to manage the limited bandwidth in the best and most efficient way. Although there are technical issues relating to bandwidth management, the biggest challenge is to raise awareness of the importance of conserving and using bandwidth responsibly by the users. [4]

5. Objectives of Study

1) To identify unproductive network based applications responsible for eating valuable bandwidth of Organisation Network System (ONS).
2) To design a bandwidth management policy to enhance and optimise bandwidth for performance enhancement of an organisation network.

6. Research Methodology

To identify unproductive web applications responsible for eating valuable bandwidth of organisation network system, monitoring of network traffic was conducted by configuring 'Cyberoam'[2] as a gateway between organisation network system and outer world environment. A time period of 30 days was set to monitor the behaviour of Intranet Users and their bandwidth utilisation trends. The following tools were used to monitor network traffic: (*i*) Traffic reports provided by 'Cyberoam'—a product of Elite Core Technologies . The 'Cyberoam Identity-based UTM' (Unified Threat Management) appliances offer comprehensive protection against existing and emerging Intranet threats, including viruses, worms, Trojans, spyware, phishing and more. Cyberoam delivers the complete range of security features such as stateful inspection firewall, VPN (Virtual Private Network)—SSL (Secure Socket Layer), gateway anti-virus and anti-spyware, gateway anti-spam, intrusion prevention system, content filtering in addition to bandwidth management and multiple link management over a single platform[2] [3]. A detailed analysis of above reports was completed followed by categorization and classification of applications as productive and unproductive activities in addition to applications which are consuming high bandwidth. Thereafter a bandwidth utilisation policy framework was designed by throttling unproductive works and prioritising organisational relating activities.

The bandwidth management means to improve the performance of an Intranet Connection by removing unnecessary traffic. Bandwidth is like a pipe and if the flow of the material inside the pipe is not monitored and managed properly then it will clog up with unwanted traffic. Similar is the case for computer network bandwidth where it can be hijacked by viruses, spam, peer-to-peer file-sharing traffic, etc. Furthermore, the useful resource of any organisation will be eaten by unproductive applications and may be difficult to avail useful services by the needy ones [8]. Bandwidth management is a process of controlling and measuring communication (traffic, or packets) on a network link in order to avoid filling up the link either to its capacity or crossing the capacity which could result in network congestion and poor performance [3]. If the organisation has a much slower connection, Intranet Access will still function, however if the connection is increased and the management removed, useful access to the Intranet will decrease immediately and soon become impossible [8].

A bandwidth management functions by sorting network traffic into various classes according to service and application types. Traffic is then planned out accordingly to the minimum and maximum bandwidth that is configured for each of the traffic types [3]. Bandwidth management requires three activities: (*i*) Policy, (*ii*) Monitoring, and (*iii*) Implementation. If any one of these activities is missing then the management of bandwidth is significantly compromised. These activities inform and reinforce each other [9]. The Fig. 1 shows the relationship among bandwidth management activities.

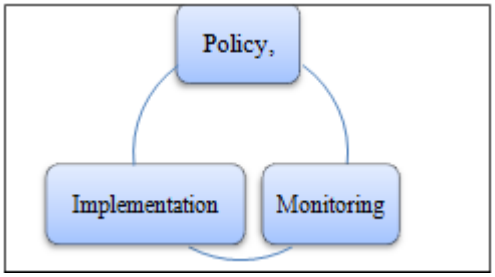


Figure 1: Bandwidth Management Process

- Monitoring is important for defining and enforcing policy. Network monitoring informs the process of creating an enforceable policy that reflects the actual needs of the user group. It is also the necessary part of enforcing policy. Furthermore, monitoring is also required to diagnose faults and troubleshooting of the network.
- Without an "Acceptable Intranet Usage Policy" no amount of bandwidth is enough to satisfy the demands of an unrestricted user community. Individuals downloading music and other files for their personal use can absorb an organisation's bandwidth. Frequently it is the minority that consumes the majority bandwidth. In this situation, user education is far more productive than technical solutions. The organisation's policy needs to be understood and enforced. It becomes the responsibility of the network administrators to find out which users are not adhering to the policy and to interact with them on a face-to-face level.
- There are number of tools and techniques that help network administrators to ensure that bandwidth is being managed properly and policy is adhered. The key components are: (*i*) Network Analyzers—for monitoring traffic; (*ii*) Firewalls—for blocking malicious and unwanted traffic; (*iii*) Anti-Virus-for protecting network; (*iv*) Caches—for efficiently using bandwidth, (*v*) Traffic Shapers—for prioritising and controlling traffic; and (*vi*) Quota Systems—for managing user behaviour. The above discussion has made it clear that network management is the core concern but bandwidth being a limited and valuable asset attracts immediate attention of the network managers to do efforts so that adequate network services may be provided to the genuine users.

7. Network Monitoring and Analysis

The bandwidth is one of the most expensive resources available in the present time which needs to be managed effectively and efficiently. Proactive network monitoring and analysis is an effective way to identify bottlenecks and sources of heaviest traffic. Monitoring and analysis tools do not physically enhance the network, but rather, offer an interface to the managers to gain a better understanding of what is happening on the network so that failures and bottlenecks can be prevented before they occur.

7.1 The Status of Intranet in Chanakya.

The status of network infrastructure, users and maximum bandwidth is shown in table.1.

Table 1: Status of Intranet in Chanakya

Factors	*Head quarters*	*Area offices*	*Sub area offices*	*Field/Mobile units*
No of PCs	1500	1200	650	460
No of users	8000	6000	5400	6500
Bandwidth	8 mbps	8 mbps	2 mbps	2 mbps
Via media	Leased line/fiber optics	Microwave link	VSAT/Microwave link	VSAT/Radio links

7.2 Network Usage Profile.

We have monitored nature of network traffic and the applications accessed and run by all users. In particular:

- We have monitored the network on a 24 hours a day, 7 days per week basis using a variety of network tools .
- We have recorded in-coming and out-going traffic levels, categorized by protocol and application type.
- We monitored all applications running on the network and all applications accessed by users over the network's external links.
- We monitored which applications are mission-critical, & which are very important or popular and which do not fall into these categories.
- We monitored sites, or types of sites, the users are not allowed to access.
- We know which applications the users are not allowed to run or access, both on the network and over any external links.
- We monitored critical network segments and critical links within the network;
- We got awareness of the organization's development strategy and how this is likely to affect the development of the network and network services.

7.3 Network Users in Chanakya

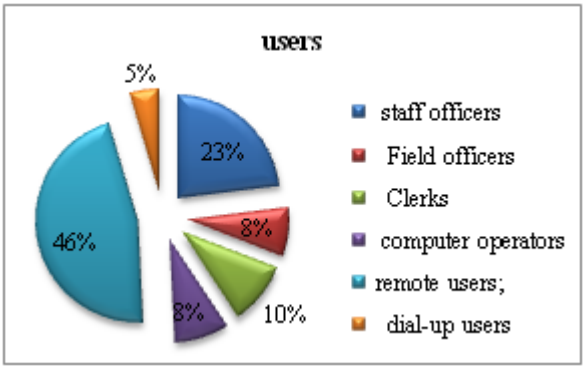


Figure 2: Network User Status

In Chanakya Organisation, a connectivity through line, microwave, VSAT (Virtual Satellite Aperture Terminal) was available from main headquarter to area headquarters, sub area HQ, field units and mobile units. The available bandwidth among the HQs and units is as shown in table 1. We can say every units/office was statically getting a bandwidth of around 2 mbps which is very low in present context especially when user wants to download digital contents containing images, graphics or heavy documents, etc. In addition to above, following facts are also related to bandwidth utilisation in offices:

a. IT Policy was not followed by 46% of users and maximum employee were using network during office time only.
b. Staffs were sending all correspondence file, data from their office to others in office time and also using network for chatting, video download, social activity, music and p2p file due to which sudden chock up of network was occurring.
c. Employee experiment with their computing knowledge and connect to exposed computer systems elsewhere in the network to invite viruses, worms, spyware, etc. which in turn chock the whole network bandwidth.

From the above, it has become very clear that users and mission critical applications of organisation need sufficient amount of bandwidth to do productive work and some of them are using unproductive applications which need to be discouraged. To provide adequate bandwidth is the prime responsibility of IT manager of organisation . To solve this problem, following two options were available:
a. Technology based Bandwidth management
b. Policy based Bandwidth Management.

8. Technology Based Bandwidth Management

There are various technologies available in the market, which can be applied to enhance bandwidth of network which is as under:

- Compression techniques
- Cashing techniques
- QoS and network management techniques.

In this we need to go for procurement of hardware and software which involve additional financial burden. It is a very complex and time consuming solution due to its expensive nature because it needs to get approvals from various authorities in a hierarchical manner within the organisation and also at the government level, and as a result bureaucratic delay for immediate solution. So it was decided to go on parallel for second option, i.e. "*Policy Based Bandwidth Management*" for immediate relief to the genuine users and mission critical applications.

9. Policy Based Bandwidth Management.

The goal of managing network capacity is to have the right amount of bandwidth in the right place at the right time for the right set of users and applications. Network components have two common characteristics: a finite transmission capacity and a measurable utilization or load. Bandwidth management requires that the load or capacity relationship of key facilities must be understood, in order to ensure sufficient bandwidth to keep a business or service functioning properly and profitably. To ensure enough bandwidth, bottlenecks must be identified and dealt with on a case-by-case basis, based on business priorities [1]. The bandwidth management is not one time job rather it is continuous cycle where consistent monitoring of the network traffic is done followed by implementation of solutions as policy matter.

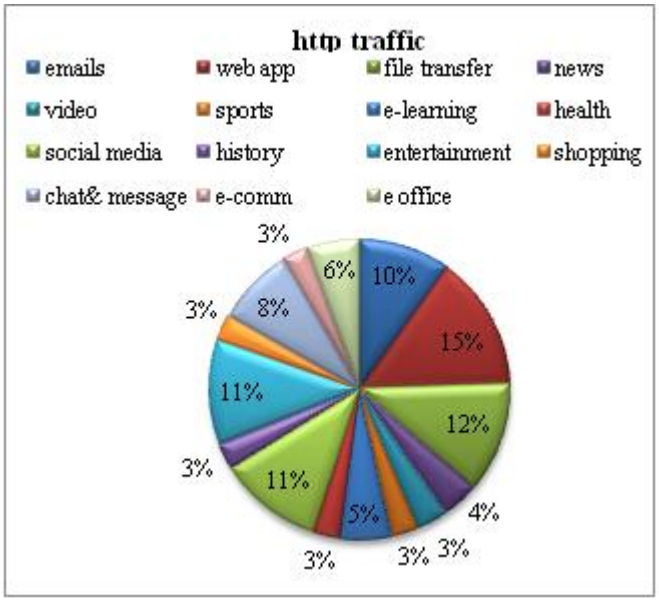


Figure 3: Application Category-wise Traffic Load

When application specific graphs as shown in fig.3 was analysed. It reveals that File transfer was on the first rank in the list of top ten websites visited by the users. Nearly 15 percent of the traffic was due to the updates of various applications installed on users computer. Major contributor was the windows update. About 14 percent traffic was due to audio and video downloads. A load of about 6 percent was observed due to email traffic. There was a significant load of about 5 percent on the bandwidth due to DNS (Domain Name System) queries. Because the organisation was using DNS of its Intranet Service Provider and every request is routed to it for resolving universal resource locator. It was very disappointing that there was a very little access (about 1 percent) of database application being access at field units. The above facts are clearly indicating that nearly more than 60 percent traffic is due to unproductive practice of applications which are not correlated with organisational or offices works. So, it was decided to frame polices for Intranet Access in the organisation after getting above feedback.

10. Design of Policy Framework

Keeping in view the above mentioned bandwidth utilisation facts which came into picture during the traffic monitoring phase, we as organisation prepared a first version of the policy framework for Intranet Access. The main aim of this framework as described [9]. "Intranet access is provided to achieve or sustain organisational or business goals. Using it for personal reasons compromises that goal by potentially slowing or halting important network services. This is why we have chosen to prohibit personal Intranet use, except for the limited use. The research results indicate that there was a need to block following web applications with immediate effect: (*i*) social networking websites (*ii*) Audio and Video Downloads, (*iii*) file transfer, (*iv*) Chatting (*v*) Hacking, (*vi*) Weapons, (*vii*) news reading online, (*viii*) Games and Gambling, etc. In addition to above, the traffic related to updates of any application was blocked in working hours. Users were advised to schedule their updates in late hours. To deal with DNS traffic, it was decided to install organisation's own DNS serves. But for the time being, the Cyberoam was used for this purpose because it had the capabilities to provide DNS service to some extent. Furthermore, the p2p types of application protocol category were blocked. In addition to above solutions, it was also decided to install following servers: Mail Server, Web Cache Server, Windows Update Server, Antivirus Update Server, etc. in second phase/ version of the policy to minimize traffic on network by resolving users' request locally.

a) Mail server receives incoming emails from local users and remote senders and forwards outgoing emails for delivery. The implementation of a mail server in the Organisation will allow fast and concise communication among multiple users in addition to efficient method of information dissemination. Emails can be checked out anytime, anywhere. It will also facilitate in reduction of traffic earlier caused by accessing other email services.
b) Web Cache & Server caches for web documents i to reduce bandwidth usage, server load, and perceived lag. A web cache server sits between web servers and clients, and saves copies of the responses coming from web servers to the clients. Then, if there is another request for the same URL, it can use the response that it has, instead of asking the original server for it again. It reduces the amount of bandwidth used by clients. This saves money and keeps the bandwidth requirements lower and more manageable.
c) Windows Update Server can provide regular updates locally to the users. By implementing this server, the unnecessary traffic related to windows update was reduced. Even the windows server could be configured to get updates during night hours to avoid individual rush during peak hours. This has help to save the bandwidth in working hours and can make the use of bandwidth available in night.
d) Antivirus Update Server can also help to reduce unnecessary anti viruses update traffic during day timings. The antivirus updates on a single system can serve the purpose of whole organisation using centralised controlling environment. This will also help to reduce unnecessary load on bandwidth during peak hours.

11. Implementation

Network was completely monitored and analyzed for 30 days. Analysis was done daily, weekly, monthly basis. We have formulated the bandwidth management strategy and set up to implement in four location of chanakya . Policy-based bandwidth management is probably the simplest to implement in the sense that the management of components comprise of gateway routers, switches, firewalls and proxy caches – all of which, with the possible exception of proxy caches, are already a functioning and integral part of most office networks..

11.1 Site Access Restrictions

Site access restrictions was implemented by:

- Applying ACLs based on IP addresses on gateway router.
- Employing filtering software at the gateway router or at another node in the network.

- Employing a Proxy Cache to restrict access to sites based upon IP address and/or port number.

11.2 Application and Protocol Restrictions

Use of certain protocols was prevented by:

- Employing tools like Cyberoam.
- Closely monitoring user activity and taking appropriate action when transgressions occur.

11.3 User Monitoring

This may be required to restrict and control the use of certain applications such as P2P. The bandwidth saving achieved by the extensive monitoring of user activities and the rigorous application of the rules in the case of transgression, can be significant.

11.4 Traffic Prioritisation

Traffic prioritisation and the discarding of traffic was achieved by the use of tools like Cyberoam (or such as PacketeerTM).

12. Result and Performance Analysis.

Cyberoam application filtering is a highly-scalable and robust tool that allows a complete application control of the network's resources. By utilizing our policy-based bandwidth management, we tried to filter bandwidth of" time-critical applications, by assigning multiple levels of Application filtering based on protocol and IP. The bandwidth of network monitored in Dec 2014 is shown in figure 3 and after applying the protocol filtering the result achieved in shown in figure 4. It is experienced that unwanted traffic was reduced and mission critical traffic was enhanced and hence application is available at area offices and field units. Using application filtering and other techniques 30% bandwidth saving was achieved. The application/protocol increase and decrease after employing policy based techniques is as shown in figure 6 and bandwidth availability for mission critical application in figure 8. In figure 7, it is seen that how mission critical application (priority (P1), time critical application (P2) and normal or less priority (P3) traffic was controlled by applying policy based traffic and bandwidth management. Initially P1 traffic was 27% and P3 was around 65%. After enforcing policy based controlled it is now 60 % and mission critical applications are accessible at field and mobile units/offices of Chanakya. Form figure 8 it is observed that around 30% bandwidth was saved for mission critical application in Chanakya.

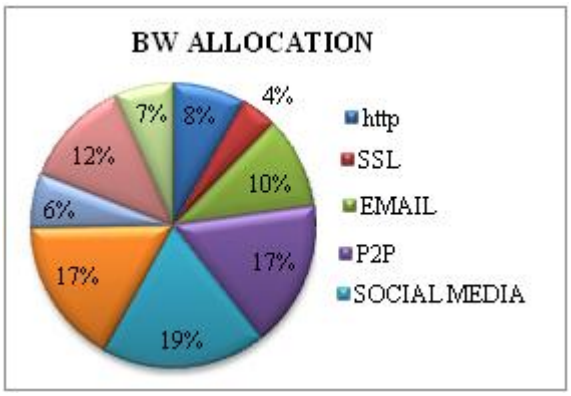


Figure 4: Bandwidth allocation in December 2014

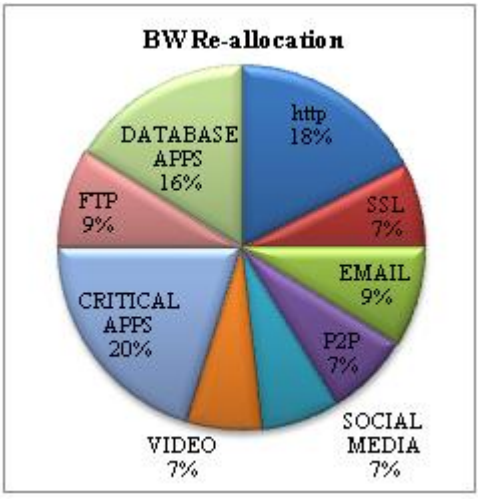
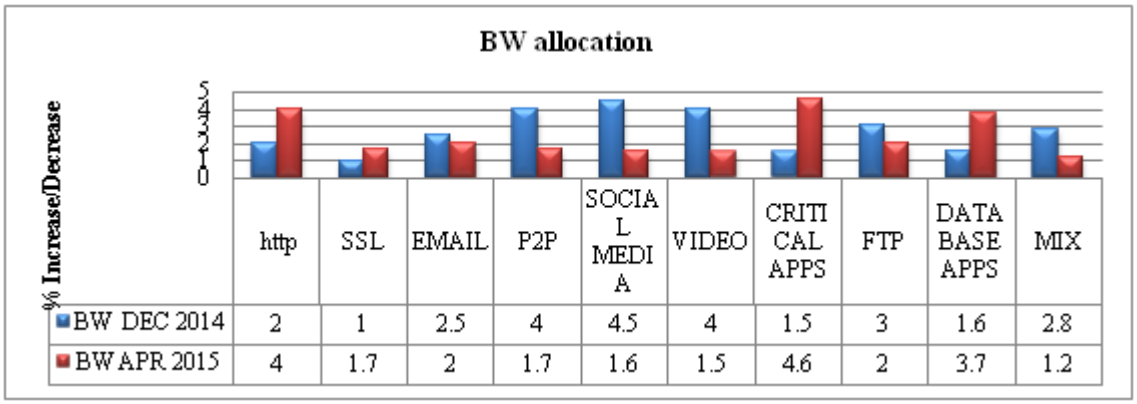


Figure 5: Bandwidth Re-Allocation in April 2015



	http	SSL	EMAIL	P2P	SOCIAL MEDIA	VIDEO	CRITICAL APPS	FTP	DATABASE APPS	MIX
BW DEC 2014	2	1	2.5	4	4.5	4	1.5	3	1.6	2.8
BW APR 2015	4	1.7	2	1.7	1.6	1.5	4.6	2	3.7	1.2

Figure 6: Increase/Decrease of Bandwidth of protocol/application

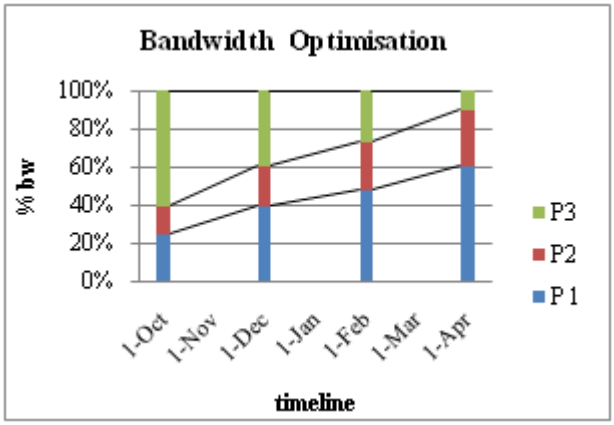


Figure 7: Management of priority (P1), Priority (P2) and priority (P3) traffic before and after policy based optimization from October 2014 to April 2015.

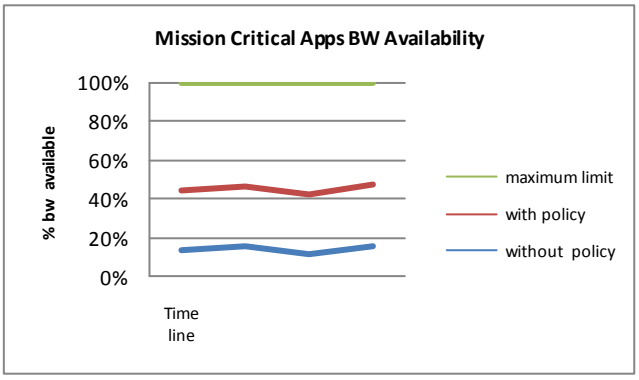


Figure 8: Bandwidth Availability for Mission Critical Application

13. Conclusions and Future Works

Bandwidth management is a serious and emerging challenge for almost all organisations in the present world of Information Technology. Lack of appropriate bandwidth management is preventing useful Intranet Access which in turn yielding low quality of organisational and offices works. Better management of bandwidth makes Intranet Access wider especially for those who need it in actual. Unfortunately there is relatively little understanding about the importance of managing bandwidth because of low awareness, lack of technical staff, improper implementation of Intranet Usage Policy, non supportive attitude of authorities, etc. Bandwidth is a very valuable and limited resource, so there is a need to enhance awareness level among all stakeholders within the organisation in addition to implement a common acceptable policy. Policy should encourage organisational activities and throttle of unproductive and individual centric activities. The IT professionals responsible for management of organisation network system have to monitor network traffic and users' behaviour continuously on network followed by analysis of web applications eating valuable resource. Furthermore, provision of trainings and technical tools is not sufficient for bandwidth management but there is a need to have a rich coordination among all stakeholders, authority and IT staff on a common acceptable Intranet Access Policy.

In this case study I could implemented only traffic filtering, priotisation, and quota system and netiquette and users awareness. The system can be more effectively employed by other freely available traffic and bandwidth management software and technique. In future compression techniques ,load balancing and cashing techniques can be utilised which are simple and freely available in markets. Bandwidth is precious matters and it should be handled with proper strategy and careful implementation by all stakeholder of organisation.

References

[1] Curz Peter, (2000). "Adopting a Business-Oriented Approach to Bandwidth Management — Technology Information". *Computer Technology Review*, 10 Dec. 2014 <http://findarticles.com/p/articles/mi_m0BRZ/is_3_20/ai_61620899/>

[2] "Cyberoam UTM announced On-appliance SSL VPN". (2014). Elitecore Technologies Limited. 10 Dec. 2014. <http://www.cyberoam.com/downloads/Brochure/CyberoamSSLVPNBrochure.pdf>

[3] Dualwan, (2014). "Bandwidth Management and Traffic Optimization". 12 Dec. 2014. http://dualwan.org/bandwidth-management.html

[4] "Optimising Intranet Bandwidth in Developing Country Higher Education". (2006). *International Network for Availability of Scientific Publications*. Oxford. 10 Dec. 2014. <http://www.inasp.info/uploaded/documents/BMOchap6. pdf>

[5] "The Need for Bandwidth Management: Taking Control of your Intranet Connection". (2010). 10 Dec. 2014. http://www.intranetwk.com/links/elron.html

[6] "Decentralized Network Management at UW". (2004). *Report from the Adhoc Committee on Network Management*, Organisation of Waterloo. 12 Dec. 2014. <http:// ist.uwaterloo.ca/CNAG/2004-10-network-mgmtmodel. html>

[7] Ocampo, Saturnino M., (2007). "ICT in Philippine Higher Education and Training". *15th SEAMEO-RIHED Governing Board Meeting and back-to-back Seminar on ICT in Organisation Teaching/Learning and Research in Southeast Asian Countries held at the Millennium Sirih Hotel*; Jakarta, Indonesia. August 23-24, 2007.

[8] Rosenberg Diana, (2005). "Digital Libraries". *International Network for the Availability of Scientific Publications (INASP)*. 13 Dec. 2014. < www.inasp.info>

[9] "How to Accelerate Your Intranet", (2006). 10 Dec. 2014. <bwmo.net/pdf/chapter2.pdf>

[10] McGuigan, Brendan. (2010). "What is bandwidth". 10 Dec. 2014 <http://www.wisegeek.com/what-isbandwidth. htm>

[11] Gray K., Thompson C., Clerehan R., et al. (2008). "Web 2.0 Authorship: Issues of Referencing and Citation for Academic Integrity". *The Intranet and Higher Education*, 11, pp. 112 – 118.

[12] "Bandwidth Management Position Paper". (2007). Aptivate. 12 Dec. 2014. www.aptivate.org/attach/...BMOPositionPaper/AptivateBMOPositionPaper.pdf>

[13] Chanakya virtual organization annual technical journal and IT Policy.
[14] Chanakya Technical Networks Components and infrastructure guide, 2014
[15] George Neisser, Bandwidth Management Advisory Service (BMAS), BMAS '*Good Practice Guide'*, ver 1, part 1, http://www.bmas.ja.net.

Author Profile

Ashok Tripathi has received his **B.E** . Degrees in Electronics Engineering from SGGS College of Engg & Technology, Nanded(India) in 1996, MBA from North Maharshta University, Jalgaon , MMS from Berhampur University , Odisha in Military Science and Technology in 2005 and PG Diploma in VLSI & Embedded System from C-DAC ,Pune in 2012, respectively. Presently he is pursuing **MTech** from Jagannath University, Jaipur, India in Embedded System Technology.

Associate Professor **Ramech Bharti** has received his M-Tech. Degrees in Electronics & communication Engineering from Malviya Institute of Technology, Jaipur ,India in 2010 and B-tech from SKITM&G, Jaipur in 2004.He is pursuing his Phd from Jagannath University. He has got teaching experience of 11 years in same field. Presently he is working as Associate Professor in department of Electronics and Communication Engineering, Jagannath University,Jaipur**.**