Network Bandwidth Management

This document was designed to inform users about how Telecommunications and Networking manages Internet bandwidth and why it is necessary. The question “Why is my Internet connection slow?” is a difficult question to answer because there are many factors that impact performance. To help you understand the bandwidth management process you first need a general understanding of some terms and how they relate to you:

Bandwidth

Bandwidth is the capacity of a network to carry information. Simply stated, it is the amount of information that can flow through the network. Think of bandwidth as an interstate. The cars on the interstate represent the data you are trying to move, the lanes represent the bandwidth. The more lanes (bandwidth) the interstate has, the faster the cars (data) move. When high demand bandwidth applications or viruses attack the network, these lanes are flooded causing the lanes to become congested. The result is that all cars move slower down the interstate.

Bandwidth Management

Bandwidth management is a technique designed to manage the bandwidth or priority of various applications on the network. Without bandwidth management, an application or a user could consume all available bandwidth within a network preventing other applications or users from being able to effectively use the network. The technologies used to implement bandwidth management are based upon an approach called QoS (Quality of Service). Bandwidth management works by identifying application traffic passing through the network and then applying QoS policies used to protect, prioritize, or restrict these applications. In this manner, mission critical applications can be protected and non-mission critical applications can be managed to prevent over consumption. Without bandwidth management, non-mission critical applications could starve other applications of the bandwidth needed to be functional.

PacketShaper (a trademark of Packeteer)

PacketShaper is one type of product used to implement bandwidth management policies to protect Internet connectivity for Illinois State University. There are 3 levels of QoS policies. The first level is designed to protect mission critical applications from bandwidth starvation during high volume periods. Some of these applications are also prioritized to improve response time and consistency. The second level consists of applications not classified in either the first or third level policies. These applications are susceptible to bandwidth starvation during peak volume. The third level is designed to restrict the volume of non-mission critical applications to prevent them from over consuming limited Internet bandwidth.

Peer-to-Peer (P2P) applications

P2P applications allow users to share electronic media such as audio, video, document, or even applications over the network. These applications allow users to download (or upload) files amongst themselves and are not dependent upon a centralized server. As such, the only bandwidth constraints that p2p applications have relates to the connectivity of each user. Examples of P2P applications include but are not limited to KaZaA, BitTorrent, Abacast, DirectConnect, LimeWire, Gnutella, iTunes, eDonkey and Audiogalaxy.

Internal Network Bandwidth

Internal network bandwidth refers to the available capacity on the campus network known as ISUnet. There are no network bandwidth restrictions on data exchanged between computers connected to the campus network. The rate at which this data is transferred amongst these systems is not currently throttled. This is possible because there is a great deal of network capacity available throughout the campus network.

External Network Bandwidth

External network bandwidth refers to the capacity between the campus network and the Internet. As of August 2, 2004, the University maintains a combined 162Mb/s (megabits per second) of Internet connectivity between two different ISPs (Internet Service Provider). The University may increase Internet connectivity by purchasing additional capacity from one or more ISPs (Internet Service Provider). However, increasing Internet capacity is very costly and can only done incrementally. In addition, transfer rates on the public Internet are unpredictable due to the connectivity of millions of computers worldwide. To protect Internet connectivity for the University, network bandwidth management is used to control the volume of data being transferred between computers connected to the campus network and other computers on the Internet. Using this approach, mission critical applications are protected and non-mission critical applications are managed.

Mission critical applications

Since the mission of Illinois State University is teaching, learning, and research, mission critical applications are those applications that are fundamental to support this mission. These applications include but are not limited to:

- the web (ie: HTTP, HTTPS)
- file transfer (ie: FTP – not peer to peer)
- email (ie: SMTP, POP, IMAP)
- streaming video (ie: Real, QuickTime, Windows Media, RTSP, etc)
- interactive video (ie : H323, SIP, RTP, etc)
- terminal emulation (ie: telnet, SSH)
- VPN
- instant messaging (ie: AIM, MSM, etc)

Non-mission critical applications

Non-mission critical applications are applications that do not support the mission of the University. These applications are not being blocked by the University, but they are restricted to the amount of external network bandwidth they can consume. These applications include but are not limited to:

- P2P (ie: KaZaA, BitTorrent, Abacast, DirectConnect, LimeWire, Gnutella, iTunes, eDonkey and Audiogalaxy, etc)
- gaming (ie: HalfLife, Doom, America’s Army, Medal of Honor, etc)

Why is my Internet connection so slow?

The answer is dependent upon which application you are using, what you are connecting to, and when you are doing it. During peak volume in the early to late evenings, non-mission critical applications will likely experience reduced response times. p2p volume can consume nearly all available Internet capacity if not managed. When this volume reaches the maximum capacity that has been defined for the non-mission critical QoS policy, the transfer rates will begin to diminish and become unpredictable. Since almost every ISP also uses bandwidth management to control the volume consumed by these applications, it is not possible to determine where this volume is being throttled. Gaming applications rarely reach capacity. During the last academic year, the campus network was bombarded by large amounts of DoS

(Denial of Service) traffic originating from computers connected to the campus network that were infected with a variety of viruses. This condition greatly diminished the amount of available bandwidth for other Internet applications.

P2P applications

P2P (peer to peer) applications have consumed up to 80 percent of consumed external network bandwidth during peak load. Because the use of p2p applications can quickly overwhelm Internet connectivity for the University, this application class is restricted by our bandwidth management products. Between 7AM and midnight, all p2p applications concurrently in use on campus can consume up to 25% of total Internet capacity. Between midnight and 7AM, up to 60% of total Internet capacity can be consumed. These times of day restrictions are applied 7 days a week. If you are experiencing poor performance with p2p applications, this is because there are many other users that are also using p2p causing the maximum amount of external network bandwidth to be reached. Our recommendation is that you take advantage of the extra capacity available between midnight and 7AM to increase the response times of your file transfers. Remember that it is against University policy to download or offer to others for download copyrighted materials.

Gaming

All gaming applications can concurrently consume up to 8Mb/s of external network bandwidth throughout the day. This restriction does not change based upon time of day or day of week.

IM

IM (Instant Messaging) is a popular application that while not restricted makes use of available bandwidth. The file transfer feature of IM is classified as p2p and bound to the same restrictions.

DoS

DoS (Denial of Service) is an attack targeted at a network, computer, or combination of systems from one or more network attached computers. Typically, large volumes of network traffic are used to create a DoS attack causing the network to experience degraded performance or even loss of service. DoS traffic can originate from computer viruses, worms, Trojans, bots or other electronic security threats and can spread through vulnerabilities in operating systems, by email attachments, through instant messaging, or file sharing using p2p. To defend against these threats, the University has implemented a variety of technologies within the network and on the central email system to help identify and block the source of these threats. However, the best defense against these threats is through the use of anti-virus software and automatic operating system updating. This is why the new CoA (Conditions of Access) were created. Remember that you must comply with the CoA or risk losing network access.

Why is my cable connection at home so much faster?

Unlike the company that provides your cable connection at home, Illinois State University is not a commercial Internet Service Provider (ISP). The University must protect those applications that are dependent upon connectivity to the Internet and critical to the function of the University. A commercial ISP is not concerned with protecting mission critical University applications and therefore does not have the same application restrictions as the University. In addition, commercial ISPs charge a much higher fee (typically $30-$50) a month to provide their users with a fast Internet connection with fewer restrictions. This allows them to maintain much more Internet capacity than what the University can provide.

Illinois State University has an academic mission to follow. While using the University's Internet service, you should be able to access mission critical resources needed for coursework while non-mission critical applications such as P2P and gaming may exhibit slower performance.

Does Illinois State University manage bandwidth?

Yes. We are currently using PacketShaper appliances to identify and prioritize traffic passing between the campus network and the Internet. This product uses application based signatures to provide a fair and equitable amount of bandwidth for all users. This means that a user who wants to use non-mission critical applications may experience degraded service during peak periods to protect mission critical applications.

How does this "PacketShaper" control bandwidth?

Since we can identify application traffic that move across the network based on signatures we can set restrictions on specific types of data transfers.

Any traffic going between computers connected to the campus network is not restricted. Restrictions apply only when this traffic is exchanged between a computer connected to the campus network and the Internet.

P2P and games are limited as to the amount of bandwidth they can consume. We realize that this may mean degraded downloads and occasional problems when connecting with other peers; however, P2P traffic is not mission critical to the University. p2p applications will consume all available Internet capacity unless managed. Between 7AM and midnight, all p2p applications concurrently in use on campus can consume up to 25% of total Internet capacity. Between midnight and 7AM, up to 60% of total Internet capacity can be consumed.

What can I do to help improve the University's Network?

Users have a responsibility to keep their anti-virus signatures and operating systems patches up-to-date regardless of operating system or version. This is now a requirement for connectivity to ISUnet as described by the new CoA (Conditions of Access).

Windows 2000 and XP are the two biggest risks on the network right now (which you may find surprising since they are superior to Win95/98/ME in many ways). But exploits into these operating systems are being found by industry professionals on an almost daily basis. When a less-than-scrupulous individual writes a virus or worm like Nachi and Blaster that makes use of those exploits, the survivability of the network relies on the hope that users have patched their computers. If they haven't, then these worms spread like wildfire and all network users suffer as a result.