



The University of Manchester

Organization

University of Manchester
Manchester, UK
www.manchester.ac.uk

Industry

Higher Education

Challenge

- Improve Internet link throughput
- Gain visibility into network activity
- Block unsanctioned peer-to-peer applications

Solution

- Deploy PacketShaper 10000 on the Internet link
- Gain visibility into network activity
- Implement and enforce network usage

Benefits

- Improved Internet throughput by protecting vital applications
- Identified and controlled recreational traffic bandwidth from students
- Enabled faster containment of network attacks and viruses

University of Manchester Manchester, UK

The Largest Single-site University in the UK Gets P2P Under Control

The problem is all too familiar. There should be plenty of bandwidth on the Internet link, but there was no throughput available for important research and business applications for University faculty, staff and students. The University of Manchester suspected that there were unauthorized Peer-to-Peer (P2P) applications on the network, but they were unable to really see what was going on or – more importantly – fix the problem.

Big University with Big Network Problems

The University of Manchester is the largest single-site university in the United Kingdom and has 11,500 residence rooms connected to its campus network. Before deploying Blue Coat® PacketShaper®, students were, at times, using all available bandwidth on the University's 1 Gbps Internet link due to huge numbers of users running P2P applications such as Kazaa and BitTorrent.

University networks are particularly vulnerable to unsanctioned downloading and file-sharing because the machines connected in residential rooms are the students' personal computers and, as such, are unmanaged in terms of software running on them. Another concern is that these unmanaged PCs can be virus infected and unpatched or not firewalled. This makes it vital for universities to control traffic such as P2P, both from a legal and financial perspective.

The University network managers estimated that up to 70% of available bandwidth was being used up by unsanctioned downloads. Since installing Blue Coat's PacketShaper 10000 on the Internet link they have been able to remove nearly all of the harmful P2P traffic from their network. The PacketShaper 10000 has solved the critical bandwidth problems that were crippling the University's network.

Complete Visibility, No More P2P

The most important aim of the installation was to gain visibility of what was happening on the networks in the residential halls and eliminate potentially harmful P2P traffic. A key goal for the University was to stop the spread of viruses. While gaining visibility into network activity and providing control over that activity, any chosen solution had to ensure that the network was available to all users all of the time, with no performance penalty.

With needs and requirements understood, the University network managers researched the market offerings and considered the Pallisade PacketHound, Cisco NBAR and the Allot NetEnforcer. In the end, they decided that the PacketShaper appliance was the most intuitive solution to use and manage, and most clearly offered what was wanted in terms of managing a network of this scale. The PacketShaper monitors traffic on the network, provides complete visibility into all of the applications running, and allows network administrators to allocate bandwidth to important applications while limiting or blocking others.



"We unanimously think that we made the right choice in placing the PacketShaper on the network."

- Ben Horner, IT networks officer

"We now rely on the PacketShaper to offer application control," said Ben Horner, IT networks officer at the University of Manchester. "Deploying Blue Coat at our network core has enabled us to effectively block all unwanted P2P traffic at the same time as allowing useful P2P traffic such as Skype to transit the network. The visibility we obtain from the reporting tools is an invaluable aid in understanding how our network is used."

Currently 11,500 student rooms are connected to the network, and the University plans to expand this number. With this expansion, the ability to manage such a large network will be even more important. Traffic from 45 separate sites is processed through the PacketShaper 10000, which is installed on the connection between the student halls and the Internet. This deployment has been so successful that the University is considering installing a PacketShaper on the connection between the student halls and campus in the future too.

"We unanimously think that we made the right choice in placing the PacketShaper on the network," continued Horner. "We have seen the most enormous decrease in the amount of bandwidth being used, and we now have a very clear view of what the students are using the network for and where new areas of concern may be. It is early days for statistics on traffic, but we definitely know that we don't want to remove the PacketShaper any time soon."