

Consumers and Network Management

A primer for consumers, advocates and policy makers

Network management – the process used to maintain the integrity and operations of a communications network – is a beneficial and necessary function of modern networks that has nonetheless become embroiled in the controversies related to network neutrality and traffic congestion on the Internet.

This three-part series examines network management – what it is, how it works, what it means to consumers, and what policies would most benefit consumers and network operators in their efforts to maintain effective communications. Part II discusses how network management affects both the networks and consumers.

All networks require some level of management in order to operate efficiently and reliably.

Whether the network is a road, an airway, a waterway, an electrical grid or a telecommunications network, it must make use of management practices best suited for its own mission, its own requirements, its own priorities and its own users.

Some of these practices are never seen by the consumer – as when a pilot follows a specific flight pattern departing an airport, or when information packets are routed on a telecommunications network.

Others, like restrictions on watering lawns during droughts, or electrical "brownouts" during times of peak demand, are more conspicuous and may present inconveniences for some, but are necessary to the effective operation of the network for the common benefit of the greatest number of users.

Specific techniques of management for telecommunications networks are obviously

Six Ways Network Management Helps Consumers

- 1. Enables new features, applications and services.**
- 2. Protects against malicious activity**
- 3. Provides enhanced privacy and security for data**
- 4. Limits spam**
- 5. Improves reliability and reduces network traffic congestion**
- 6. Achieves better cost efficiencies**

different than those for roads or other types of networks. But the basic tenets of network management are the same – reliability, speed, efficiency and security.

Recapping Network Management

As noted in Part I of this series¹, network management practices are implemented at every layer of the network in order to protect the integrity and reliability of data flows. The practices at each layer work together to form a web of protection that spans the entire network.

Network management practices are intended to be flexible and fast – when necessary, reacting to and neutralizing a threat even before they are visible to the human eye.

Though the discussion of network management in Part I was necessarily technical in nature, the conclusions it reached are not:

- The Internet as initially conceived was not designed to carry the volume or diversity of content, applications and services we take for granted on today's networks.
- The Internet is not a single, monolithic entity but rather a global network of tens of thousands of individual, privately owned and managed telecommunications networks.
- The history of network management for the Internet has been a story of evolution and growth, as network owners and operators have struggled to meet rising demand for bandwidth and adapted to new consumers needs.

Largely invisible to users, network management delivers six key benefits:

- 1. It enables new features, applications and services.** Adding capacity alone

¹ See <http://www.usiia.org>

would never have enabled today's enhanced services such as Voice Over IP or telemedicine. George Ou has presented a persuasive argument for this fact,² showing how VoIP packets need to be properly interlaced with other traffic over the Internet to prevent jitter, latency problems and other issues that would render communication impossible. Managing the networks that make up the Internet is one of the ways that enable users to enjoy a range of new online features and services.

- 2. It protects against malicious activity.**

There are now more than 100,000 known computer viruses, worms and Trojan horses³ – and the list grows each year. In order to protect users from identity theft, loss of data, infection of their computers and denial of service attacks, networks use advanced management techniques. And these are not just static protections – today's networks require an almost instantaneous response to attacks, and must be able to cope with rapidly mutating threats. To do this, network management systems incorporate artificial intelligence elements that enable the network to "learn" from each attack and adapt to new threats as they arise.

- 3. It provides enhanced privacy and security for data.**

Even where there is not a direct or overt threat, it is prudent – and sometimes even essential – to keep some information private and secure. Bank records, health records,

² See George Ou's "Technology for Mortals" at <http://formortals.com/Home/tabid/36/EntryID/34/Default.aspx>

³ See Computer Knowledge primer on viruses at <http://www.cknow.com/vtutor/NumberofViruses.html>

and financial transactions are examples of such information. Here, the protection afforded by network management and by such applications as a Virtual Private Network⁴ help to safeguard consumers from prying eyes.

4. **It limits spam.** Not all of the threats to the integrity of a network come from viruses. It's estimated that more than 80 percent of e-mail is spam.⁵ One of the principal successes of network management since 1993 has been the ability to filter out a significant portion of these unwanted communications while enabling other traffic to pass through effectively.
5. **It improves reliability and reduces network traffic congestion.** Every network becomes congested at some point. Early management techniques that treated the network as a "dumb pipe" solved this congestion problem by first slowing transmission and then dumping data packets until the congestion went away. On managed networks, such as those used by businesses, universities and hospitals, the manager follows agreed protocols to re-route, prioritize and shape the traffic to avoid bottlenecks that would otherwise render some applications useless.
6. **It achieves better cost efficiencies.** Taken together, the various elements

⁴ A Virtual Private Network is essentially a private and secure connection that is carried within a public communications network such as the Internet. For a detailed explanation, see the Wikipedia article on VPNs at :

http://en.wikipedia.org/wiki/Virtual_private_network

⁵ Secure Computing; "Trends in E-Mail, Web and Malware Threats;"

<http://www.securecomputing.com/index.cfm?sk=1739>

of network management enhance the experience of Internet users and provide cost efficiencies that enable network operators to provide users with more value for the dollar.

Even with effective capacity management, a user's Internet experience is not fully in control of the broadband network operator. Because the Internet is a network of networks and many different devices can be used to access the Internet, performance inherently can be affected by a number of variables, including an access line problem, overloads on the content provider's server, interference with a wireless router's signal, poorly designed applications, or the performance of the user's PC.

Still, effective network management can and does enhance the experience for the broadest number of users across the thousands of networks that comprise today's Internet.

Challenges

Given that network management helps maintain networks' security and provides numerous benefits to consumers, why has it become a subject of controversy?

The debate over network management is one element of a broader discussion over the growing demand for Internet capacity and how to address it. For example, growth in Peer-to-peer (P2P) networking can create stress on network capacity. Efforts by some network operators to help alleviate these strains have been the subject of debate and scrutiny by the Federal Communications Commission.

Broadband networks have been designed to reflect the way most people use the Internet -- to download information. More

bandwidth, therefore, has been allocated to downloading than uploading. But P2P does both simultaneously, sometimes creating network bottlenecks by uploading large amounts of data.

On broadband networks that rely wholly on shared connections, such as are used in cable Internet services – or those with limited bandwidth, as with satellite and wireless services – this means that the majority of users may experience slowdowns because of congestion caused by a small number of P2P users.

Some P2P software attempts to speed up file transfers by breaking a large file, such as a video file, into smaller pieces for transfer over the Internet, turning everyone who downloads the file simultaneously into an uploader as well.

When a large file is being exchanged between Internet users, pieces of that file can be downloaded from dozens or even hundreds of other users. But at the same time, as it begins to receive the file, the downloading computer also is transmitting pieces of the file to dozens or hundreds of other users. This viral nature of the application can speed up file transfers for individual users, but also can cause congestion issues in the network and can degrade the performance experienced by users who are not using P2P to transfer files.

The congestion potential is further compounded because files may be transferred from remote locations even if they are available locally. That means the P2P traffic travels longer distances and spends more time on the network than necessary, which raises traffic levels.

Since it is estimated that P2P traffic accounts for as much as 75 percent of all

upstream and 36.5 percent of all downstream traffic on the US Internet,⁶ this massive exchange of data is a potential issue for broadband networks that rely on shared capacity for efficiency and controlling costs, and can be especially acute for networks, such as cable, satellite, and wireless, that rely on a shared network infrastructure.

Responding To The Challenges

Clearly, challenges can arise when a minority of users takes up a disproportionate share of the available bandwidth.

In fact, the Federal Trade Commission (FTC) considered the issue of “Internet congestion” and noted that “the use of bandwidth-intensive applications like certain peer-to-peer file-sharing protocols by even a small minority of users is already consuming so many network resources as to be worrisome . . . even a small portion of Internet users may effectively degrade service for the majority of end users.”⁷

Nor is this uniquely an American problem.⁸ In Japan, which is recognized for high speeds that allow them to move very large amounts of data, many ISPs are taking steps to curb the use of P2P because of congestion concerns.

Network operators have attempted to respond to these issues by finding ways to equalize the bandwidth available to all the users of the network. In Texas, Time

⁶ David Caputo of Sandvine, in comments to the Canada Telecom Summit, June, 2008.

⁷ See FTC Staff Report, “Broadband Connectivity Competition Policy,” Federal Trade Commission, at 28-29 (June 2007)

⁸ See “The Welfare Impacts of Broadband Network Management,” Phoenix Center, March 2008.

Warner is experimenting with a "tiered pricing" system that would base the service tiers offered to consumers, at least partially, on the total amount of bandwidth they consume each month rather than just on speed. Other companies, including AT&T, have announced new programs to enable consumers to buy the bandwidth they desire. High-use subscribers would pay more to use more, while low-use subscribers would save money.

In a more controversial tactic, cable Internet provider Comcast has allegedly used a technique that generates manufactured re-set messages to computers communicating via BitTorrent's P2P protocols, which can delay or halt file transfers. On review by the Federal Communications Commission, however, the Commission concluded that Comcast's network management practices discriminate among applications rather than treating all equally and are inconsistent with the concept of an open and accessible Internet. Comcast will be required under an FCC Order to submit details of its discriminatory program and a plan to remedy the discrimination.⁹

Recently, Comcast has announced agreements with some P2P providers to work together to make file sharing more "network-friendly" for its subscribers.

The broadband industry more generally, including leading providers of P2P software, has been at work, quietly and collaboratively seeking solutions that potentially would help enable more efficient uses of peer-to-peer file sharing and reduce the impact of P2P on the networks.

In August of 2007, researchers at the University of Washington and Yale

⁹ FCC News release DOC-284286A1 dated August 1, 2008 and available at www.fcc.gov.

University unveiled a new design called P4P.¹⁰

This new design may enable P2P to work more efficiently with networks on the Internet. Following up on that research, an ad hoc "P4P Working Group" was formed by leading broadband networking companies to explore ways in which peer-to-peer companies and network operators could work together to achieve greater efficiency and faster downloads on a more equitable basis.

In April of 2008, Verizon announced successful tests of a P4P system that it believes may speed downloads by as much as 60 percent while reducing stress and bottlenecks on the network. The company, part of the "P4P Working Group," plans to continue the tests.

In addition to the cooperative efforts among major Internet participants to address congestion and other potential threats to the Internet, some have urged limitations on network management. In Part III of this series, we will examine policy issues that may affect Internet users' online experience and the ability of broadband networks to meet the demands of today and tomorrow.

¹⁰ See "P4P: Explicit Procedures For Cooperative Control Between P2P And network Providers," University of Washington and Yale University.

Author: David P. McClure
Date: August 8, 2008
Published by: US Internet Industry Assn.
1800 Diagonal Road
Suite 600
Alexandria, va 22314
(703) 647-7440 Voice
(703) 647-6009 Fax
(703) 851-4784 Mobile
InfoUSIIA@usiia.org
<http://www.usiia.org>

Formed in 1994, the US Internet Industry Association is the primary trade association for companies engaged in Internet commerce, content and connectivity. USIIA serves its members through legislative advocacy and professional services. The association is headquartered in Alexandria, VA.

David P. McClure is President and Chief Executive Officer of the US Internet Industry Association. A technologist by education and experience, McClure has held positions in the Internet, computing, aerospace and environmental services industries. He is widely published on technical and business topics, and is the author of more than 40 white papers related to Internet and Broadband policy, governance and economics.

© *Copyright 2008, US Internet Industry Association. All rights reserved.*