

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 III addresses the challenges for policy makers in attempting to balance the desires of consumers with the realities of network engineering.

It is a simple and incontrovertible fact. All networks require some form of management if they are to remain operational, reliable and secure, and capable of delivering services. Nowhere is this more apparent than in the public Internet.

The Internet was born into a small and controlled academic environment in which engineers could more easily manage its growth and functionality through looser and informally agreed-upon rules of the road. Even within this close-knit, loose and informal environment, however, the need for more sophisticated network management capabilities became obvious.

The Internet was barely launched when it became apparent that the basic Internet Protocol (IP) needed to be enhanced by a Transmission Control Protocol (TCP) to manage traffic flows. In the 1980s, the Internet suffered an infamous "meltdown" due to the growth in traffic, and in the 1990's the advent of commercial traffic and consumers on the Internet caused the World Wide Web to be known as the "World Wide Wait."

The Internet during these periods was a relatively small entity that could more

On August 5, 2005, the Federal Communications Commission formally adopted four principles to govern connectivity. In doing so, the Commission clearly stated, "we are not adopting rules in this policy statement. The principles we adopt are subject to reasonable network management."

easily adjust to address such challenges. There were relatively few users (in comparison to the 1.3 billion users of the commercial Internet today), and the economic value of the Internet was negligible compared with today. Nor did the Internet of that era face the challenges it does today.

On the one hand, the networks that make up the Internet today must be constantly upgraded and expanded to handle the exciting growth in new and valuable applications and services. Though a testament to success, these innovations spur new growth in traffic and expanded uses that can cause congestion and place significant stress on the networks.

Sadly, today's Internet also faces malicious threats, such as viruses, hacker attacks and other attempts to deliberately damage the networks.

In response to both the early growing pains and the more recent stresses, network operators have developed and continue to develop a variety of management techniques and technical tools to keep the networks operating as smoothly and efficiently as possible and also to minimize service disruptions.

Challenges for Network Operators

As noted in Parts I and II of this series,¹ the Internet is not a single entity but rather the interconnection of thousands of networks that voluntarily communicate with one another through a common set of protocols.

Today, more and more Internet users are using broadband connections to link to the Internet. Although broadband architecture varies from network to network, virtually all broadband networks contain shared facilities. In typical cable modem systems, most of the distribution network is shared among the subscribers in a given neighborhood.

In a typical DSL-based broadband network, subscribers share all links on the network side of the DSLAM (the "digital subscriber line access multiplexer"). During peak usage periods, congestion in these shared facilities has the potential to degrade basic Internet access for all subscribers. Such congestion presents a rapidly growing challenge for network engineers, who must balance the need for *high quality*

service against the need for *affordable* service, and must do so across a subscriber base with disparate and constantly changing usage patterns.

The demand for high-bandwidth and real-time services, especially video, has created a congestion problem on the Internet, but this congestion problem is even more severe in wireless networks, where providers must contend not just with *economic* constraints on capacity upgrades, but with *regulatory* constraints on the spectrum available for voice and data uses.

Overall, industry experts expect that "video traffic will represent at least 80 percent of all Internet traffic" by 2010.²

And video is only one of several emerging applications that are placing new demands on the Internet's access and backbone networks. Others include music downloading services as iTunes, which have supplanted compact discs as the primary means of music distribution; on-line printing and photo-sharing services such as Kodak, Snapfish, Shutterfly, and Photobucket; and the enormously popular class of "massively multiplayer online role-playing game[s]," such as Sony's *EverQuest* and Blizzard Entertainment's *World of Warcraft*.³

The network-management challenges posed by consumer use of bandwidth-intensive applications arise, moreover, not just from an increase in the *total* volume of Internet traffic, but also from the escalating magnitude of unpredictable *spikes* in

¹ See <http://www.usiia.org>

² Norton, *Video Internet*, *supra*, at 2; Yankee Group, *2006 Internet Video Forecast: Broadband Emerges as an Alternative Channel for Video Distribution* 6-7 (Dec. 2006)

³ Robert Litan & Hal Singer, *Unintended Consequences of Net Neutrality Regulation*, 5 J. Telecomm. & High Tech. L. 533, 547 (2006-2007).

Internet traffic and from the increasing sophistication of available applications. The need for effective network management is not limited to the consumer marketplace. Businesses, universities, and government agencies of all shapes and sizes are increasingly using managed services to accommodate bandwidth-intensive applications that place significant demands on network resources.

Public and private health-care providers, for example, are demanding more robust and sophisticated capabilities from broadband networks to facilitate the delivery of remote diagnostic and surgical services, high-definition imaging, and converged voice, video and data applications.

A recent report from the Joint Advisory Committee (“JAC”) on Communications Capabilities of Emergency Medical and Public Health Care Facilities highlights this point. The JAC, which was established by this Commission together with the National Telecommunications and Information Administration to examine the communications capabilities and needs of emergency medical and public health-care facilities, concluded that

“[c]onverged healthcare, clinical, business, and EMS applications, can only perform well on well-designed managed networks with sufficient bandwidth to enable reliable, secure, application-aware networking.”⁴

As the JAC explained:

⁴ Report to Congress, Joint Advisory Committee on Communications Capabilities of Emergency Medical and Public Health Care Facilities, at (http://energycommerce.house.gov/Press_110/JAC.Report_FINAL%20Jan.3.2008.pdf).

Many of the emerging real-time life-saving technologies (remote surgical procedures, tele-presence networks, and even converged voice and video) require very consistent and predictable handling of traffic by the network. Packet loss, delays in packet transmission (‘latency’), and inconsistent packet delivery interval times (‘jitter’) have significant impact on a variety of emerging real-time health care applications. To reduce latency and jitter, managed networks are generally needed that can prioritize real-time (and potentially life-saving) communications ahead of packets used for file transfer and e-mail.⁵

The Role of Technology Policy

Public policy is the process by which elected officials and regulators implement policies designed to maximize public benefit in balance with individual rights.

Government efforts to make policy generally consist of attempts to make decisions on behalf of the public good, many times through a series of tradeoffs and compromises. And, because circumstances change, often unpredictably, policymakers cannot know in advance how their decisions will work in practice. Thus, sharp changes in direction carry significant risk. Most observers believe that policymaking in the area of technology is especially difficult for a number of reasons, including:

- **Technology changes rapidly.** The breathtaking pace of technological innovation often means that today’s “problem” is fixed by the market before the ink is dry on new laws or

⁵ Id

regulations. What's more, the policy "solution" may have a counterproductive when applied to technologies that did not even exist at the time the policy was enacted.

- **Technology is global.** Policies that have jurisdiction over just one geographic area become meaningless in a global environment. Nowhere is this more apparent than with the Internet, which is not only global but is comprised of tens of thousands of individual networks.
- **Technology is complicated.** Its basis lies in hard science and engineering. The "split-the-difference" compromises that often characterize the political decision-making process may not readily apply to the scientific or engineering challenges that present themselves in technology.

This level of complexity brings to the process the substantial risk of making a poor decision, or a decision with unforeseen and unanticipated consequences. Suggestions for simple "bright line" tests as a basis for outright bans on certain practices essentially ignore both the complexity of network operation and the interdependent relationship of internal network operations.

Public policy made while the technology is still evolving carries the additional risk that promising and valuable technologies will be stifled by rules that unintentionally curb innovation and that investment in emerging technologies will be more difficult because new policies have interjected higher levels of risk and uncertainty into the marketplace.

Aware of the difficulty inherent in establishing policy for an emerging and rapidly evolving medium like the Internet, policymakers heretofore have largely chosen

-- with great success -- to let the Internet evolve largely free from government micromanagement and heavy-handed intervention. Rather, they have sought to foster an environment that:

- **Encourages innovation, growth and investment.**
- **Promotes the availability of affordable Internet access to every citizen**
- **Promotes competition, while also allowing Internet-based businesses the freedom and flexibility to innovate**
- **Raises public awareness of the benefits of the Internet and how it works.**

An example of this oversight approach is the adoption of four "connectivity principles" by the FCC.

FCC Connectivity Principles

As the Internet became a more significant factor in American's daily lives, the Federal Communications Commission decided it was important to spell out some basic principles to define what consumers should expect from their online experience.

Those principles needed to be succinct, easily understood and relatively easy to apply. Because the Commission recognized that the Internet was still evolving, it intentionally left room for interpretation so that the principles could apply to varying sets of facts.

Moreover, the principles consciously and purposely followed an oversight-based model, trusting the marketplace as the first line of remediation for potential problems,

rather than a government-driven command and control approach.

Here's how the Commission stated the four principles when they adopted them on August 5, 2005:

- *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to access the lawful Internet content of their choice.*
- To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement.
- To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to connect their choice of legal devices that do not harm the network.
- To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to competition among network providers, application and service providers, and content providers.

The FCC noted upon their adoption that, "we are not adopting rules in this policy statement. The principles we adopt are subject to reasonable network management."⁶ However, the principles

⁶ See FCC Policy Statement, August 5, 2005, at hraunfoss.fcc.gov/edocs_public/attachmatch/FC-C-05-151A1.doc

have been generally accepted as an official statement of national policy goals.

There have been relatively few instances in which actions in the Internet marketplace have raised questions about the furtherance of the principles. In fact, the Comcast/BitTorrent dispute is really a case of first impression.

The Issue of Network Management

The Federal Communications Commission is currently engaged in a process to potentially give more specific guidance about the definition of "reasonable network management" as stated in its adoption of the connectivity principles.

The inquiry rises from a controversy over a decision by Comcast, a network operator, to delay and/or block peer-to-peer (P2P) traffic that it believed was using an excessive amount of network resources and creating congestion that could degrade service to all network users.

A complaint filed with the FCC by Vuze, Inc., whose business model relies on P2P traffic, argued that Comcast's action was unreasonable. It also accused Comcast of misleading network users by failing to disclose its actions.

An inquiry by the FCC was appropriate because it follows -- and reinforces -- the existing adjudication process for complaints. Under this process, complaints are handled on an individual basis and adjudicated based on the circumstances of that complaint.

On August 1, 2008, the Commission issued an Order under this adjudication process. In the Order, Comcast was found to have contravened federal policy by unduly

interfering with Internet users' right to access the lawful Internet content and to use the applications of their choice. Specifically, the Commission found that Comcast had deployed equipment throughout its network to monitor the content of its customers' Internet connections and selectively block specific types of connections known as peer-to-peer connections.

Comcast was directed under the Order⁷ to

- Disclose the details of its discriminatory network management practices to the Commission
- Submit a compliance plan describing how it intends to stop these discriminatory management practices by the end of the year
- Disclose to customers and the Commission the network management practices that will replace current practices

The Issue of Transparency

Another issue attracting renewed interest as consumers' usage patterns change involves the Terms of Service (TOS) agreements that govern the contractual relationship between Internet providers and users of their services.

A typical TOS agreement from an Internet provider can run a dozen pages of legal language and some provisions in these agreements may be difficult to understand. For example, some TOS agreements provide only vague disclosures about any limits on how much bandwidth a consumer can use.

⁷ Action by the Commission, August 1, 2008, by Memorandum Opinion and Order (FCC 08-183).

USIIA believes voluntary adoption of basic transparency principles could help provide consumers better and clearer information.

These principles are still under development, but generally address three areas:

- **Broadband network operators should provide consumers a clear and transparent statement of their Terms of Service.** Consumers should be provided enough information, perhaps in a plain language supplement to the legal language of the TOS, to help them decide if a plan will meet their needs. Key information would include the rates, terms, and conditions of their services. The provider should also describe the performance of their service and factors that might affect performance.
- **Consumers should be informed if certain network management practices may impact the performance of the service.** Providers should explain whether practices that, among other things, protect the security of their network, ensure quality service, and prevent unlawful activity on their network might affect consumers' online experience. These disclosures should avoid technical descriptions of the management techniques that might compromise network security and integrity or facilitate abuse of the network.
- **Applications providers should describe how their products might impact a user's broadband service, particularly in terms of utilizing bandwidth in ways that might cause them to violate their Terms of Service Agreement.** Consumers should be informed if an application might affect other applications the consumer may

use. They also should be informed if and how an application might affect other users sharing the same Internet connection. If an application has other risks associated with it (e.g., a particular application may make available for others to download files stored on an individual's PC that contain sensitive and private information), those risks should be clearly detailed.

The Dispute Process is Working

In the final analysis, the process in the market for improving communication amongst providers and between providers and consumers is working as it should. Network management practices are serving to protect the networks and their users. Industry is amending its practices in response to requests by consumers. Standards are being re-written over the long term, contractual agreements are likewise being amended through a process of negotiation, and network operators are working with application and content providers to identify ways to better address congestion issues and to work more cooperatively and collaboratively.

The current FCC actions are an extension of this process, serving to identify areas and issues where laws are in conflict – or where the principles adopted by the Commission do not sufficiently address threats to the network or its users.

In this effort, and in particular the efforts of both the broadband industry and the Federal communications Commission to encourage providers of services, applications and devices to better communicate with consumers, USIIA lends both its endorsement and support.

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.*