SANDVINE

Best Practices for Network Neutrality:

Reasonable Network Management

CONTENTS

EXECUTIVE SUMMARY

Massive investments in Internet infrastructure by communications service providers (CSPs) have enabled consumer Internet traffic to grow at 40% per year in mature markets, and at even higher rates in developing markets.

Yet, despite these efforts, capacity bottlenecks still appear. The simple fact is that to keep Internet access affordable, infrastructure must be shared in an oversubscription model.

No amount of capacity expansion can completely eliminate congestion, so CSPs must find additional means of preserving fair access and high quality of experience for their subscribers. These solutions are broadly referred to as traffic optimization, a subset of which is called traffic management.

Increased regulation, broadly referred to as network neutrality, places requirements on how CSPs can manage their networks, and often place disclosure requirements around the management techniques.

This paper explains how to achieve the concurrent goals of providing sustainable high-speed data service while complying with network neutrality guidelines and principles.

By adhering to five key principles, CSPs can continue to accommodate enormous data growth while employing reasonable traffic management techniques to protect the network's ability to deliver high-quality subscriber services.

INTRODUCTION TO NETWORK NEUTRALITY IN POLICY CONTROL

Network neutrality lacks a consistent definition globally, but one key aspect of it tries to address how communications service providers (CSPs) can manage traffic in their network. Regulations in Canada, the United States, Europe, and other jurisdictions have generally accepted the notion of "reasonable network management" as part of network neutrality.

However, whether official regulations exist or not, wherever the concept of network neutrality exists in the public mind, CSPs seek to establish policies that can stand up to public and regulatory scrutiny.

Through research, public commentary, and the socialization of network neutrality issues with such entities as the Canadian Radio-television and Telecommunications Commission (CRTC)[1], the Federal Communications Commission (FCC)[2] in the United States, and the Body of European Regulators of Electronic Communications (BEREC) in Europe, Sandvine is uniquely qualified to provide principles and best practices for network management that align with global standards (whether official or not) and directly relate to public concerns about network neutrality.[3]

1 CRTC decision rules are located here: http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm

2 FCC guidelines are located here: http://www.fcc.gov/guides/open-internet

3 You can learn more about Sandvine's activities with respect to Network Neutrality, including links to many of our submissions and our public commentary, at this page: https://www.sandvine.com/trends/network-neutrality.html

BEST PRACTICES

Network management is typically introduced to protect or enhance subscriber quality of experience, whether in general or when portions of the network are congested. While there will always be voices that object to any kind of traffic management, it is nevertheless possible for CSPs to achieve their network management goals without running afoul of public perception and official regulation.

To maximize the likelihood of success, network management solutions should adhere to the following best practices:

- Legitimate and demonstrable technical need
- Narrow-tailoring in terms of the stated technical goal of a traffic management practice
- Proportional and reasonable effect in achieving the goal
- Transparent disclosure
- Auditable and demonstrable

Legitimate and Demonstrable Technical Need

The operator must have a legitimate and demonstrable technical need for the network management practice. The architectural strengths and weaknesses of various network access types provide the majority of the technical needs for network management.

A network management practice that is unreasonable in one access network may well be reasonable in another. This context is crucial: solutions fare best when they directly address a legitimate problem, such as congestion, and when they do so with proportional precision.

To be successful, a traffic management practice must be described in such a way that both the technical need and the practice are clear, and the traffic management practice seeks only to address this need and nothing more.

Narrowly Tailored

All networks have variations in usage patterns, whether by time of day, by geography, by user demographics, or by other factors. As a consequence, oversubscription and QoE are non-uniform across the network.

A properly constructed network management plan takes this into account, and focuses as narrowly as possible on the problem to be solved. It does not try to force a one-size-fits-all solution into all areas at all times. When applied correctly, management of traffic during times of congestion is a win-win as the majority of subscribers continue to have a good quality QoE and the access network lifetime is extended, allowing network investments to be optimally prioritized.

In an access network environment, there are several areas of ‘narrowly tailored’ that might be technically considered for addressing subscribers who are causing disproportionate congestion. These include:

- Network type (DOCSIS 3.0, UMTS, DSL, LTE, WiFi, Satellite, etc.)
- How access nodes and links interact
- Subscriber density per access node (QAM, DSLAM, Mobile Cell)
- Subscriber usage patterns and service plans per access node
- Backhaul network capacity
- Unforeseeable events

A reasonable network management practice takes these factors, and more, into account. It applies itself differently, or not at all, depending on the conditions that are currently present. For example, a network management practice might be self-tuning, and could disable management when no congestion is present. In a cable network it might operate differently when congestion is present on a single user, versus on a single RF channel, versus on a bonded set of RF channels, versus on the CMTS backhaul uplink. It might detect congestion

passively by setting a maximum bandwidth threshold per node and monitoring the bandwidth usage, or it might do so actively by measuring the real-time latency in the access network and triggering according to a latency threshold attached to subscriber quality of experience.

A successful traffic management practice will narrowly-tailor itself to the situation at hand at the time it is needed. It will not apply in a broad fashion across the broad average of a network.

Proportional and Reasonable Effect

The network management policy needs to take into account the concept of proportional effect and response. A 'reasonableness' test helps define the acceptability of network management. This test stems from the common-law concept of 'what would a typical person agree is reasonable', and is therefore somewhat subjective in definition. Some precision of what is reasonable can be achieved through the best practice of seeking proportionality in terms of the final outcome of a policy seeking to address a problem such as network congestion.

Despite the common misconception, it's been definitively proven that long-term heavy users aren't the contributors to congestion when it occurs, which makes targeting long-term heavy users during times of congestion out of proportion and inaccurate—and therefore not reasonable. Similarly, it would be considered unreasonable by most to take a subscriber causing 15% of the congestion on a network and manage their bandwidth to 1% of peak rate for all time. However, a reasonable argument for fair distribution can be made to reduce the priority of traffic of the top five percent of active (i.e., right now) bandwidth users during times of congestion, which as a group typically consume more than half the network's bandwidth at a given point in time. In reducing the traffic priority of this ever-changing minority during times of congestion, the latency—and by extension, QoE—of the other 95% of the network's users remains good.

Reasonableness can be defined through contract, which means it relates directly to the best practice of transparent disclosure described below. If typical users, understanding the disclosed network management policies in use, contract for the service, then the policy must be reasonable by definition. Reasonable is defined entirely in the frame of reference of the end-user, the customer of the service provider.

Transparent Disclosure

Transparency is a challenging concept. The subtle technical nuances of networks (latency, loss, jitter, shared-access, and the necessity of oversubscription models, etc.) are difficult to describe in simple enough terms for the average layperson. Analogies, although helpful to form a basis, rapidly become inappropriate as they diverge from the original problem. Network management practices evolve over time, and new technologies have seen the emergence of traffic management practices based on deep packet inspection (DPI). Since we are relying on transparency as a means of supporting reasonableness, what's relevant to disclose is any aspect that would affect the actions or perceptions of the typical consumer.

The operator must make the material information publicly available to allow understanding of the network management policy by those impacted by it. The disclosure should be sufficient for a consumer to form an informed opinion on whether the practice will affect them, which applications might be affected, when they might be affected, and what the impact might be, including impact to speed, latency, and general experience. Similarly, subscribers should be notified in advance of any planned changes to network management practices.

Disclosure might take many concurrent forms. The most popular include network management FAQs, notices included in billing material, acceptable use policies, terms of service, etc.[4]

4 See examples from Cox Communications (http://www.cox.com/aboutus/policies.cox?sc_id=corp_gov_red_z_policy-config_vanity), Virgin Media (http://help.virginmedia.com/system/selfservice.controller?CMD=VIEW_ARTICLE&ARTICLE_ID=3103&CURRENT_CMD=SEARCH&CONFIGURATION=1001&PARTITION_ID=1&USERTYPE=1&LANGUAGE=en&COUNTY=us&VM_CUSTOMER_TYPE=Cable), and Xplornet (https://www.xplornet.com/legal/usage-traffic-policies/)

Auditable and Demonstrable

Owing to the public scrutiny of capital investment in networks, and network management policies, it becomes important for a CSP to demonstrate that the above criteria were met.

On audit, a service provider should be able to provide the following:

1. Justification of the technical need that caused the creation of the network management policy
2. What affect the policy had on the user experience
3. How they have disclosed their policy to the end-user
4. How the policy took into account network and time variances (i.e., how it was tailored)

In addition, the audit should be able to demonstrate the above were met using technical results. These results might include information on the user experience for the typical user for typical locations in the network.

CONCLUSIONS

Network management policies based on traffic management must be technically legitimate, narrowly tailored, proportional and reasonable, transparently disclosed, and auditable.

Reasonable network management requires disclosure of the policy in such a way that the typical user can understand the impact to them, and reasonableness is framed entirely from the end-user perspective.

Access-agnostic network policy control is required to create a network management practice that spans multiple devices and multiple access technologies. The network management practice must take into account the specific conditions of the access technology.

Strong reporting and business intelligence is required to be coupled to the network management practice to support auditing and the understanding of demand, capacity, and user experience. As a typical service provider, this may seem like a minefield of requirements, but a few simple up front planning activities can make for a highly successful traffic management practice.

Summary of Best Practices for Network Management

Best Practice	Criteria	Example
Legitimate and Demonstrable Technical Need	The fielded solution must be shown to address something tangible that occurs as a problem in the network (simply seeking to arbitrarily reduce bandwidth consumption without stating a technical issue is not valid)	The network becomes frequently congested at various locations, affecting subscriber QoE, and the problem must be addressed
Narrowly Tailored	Defining a policy that actually addresses the stated problem to be solved, and nothing more	If the stated goal is to manage congestion, then traffic should only be managed when congestion is present
Proportional and Reasonable Effect	Managing traffic to achieve a precision effect that ties directly to the stated goal (e.g., congestion management)	Managing the real contributors to congestion during times of congestion rather than simply managing long-term heavy users
Transparent Disclosure	Making available full details of how a policy will affect the consumer experience so that they can make an informed choice	Online FAQs, direct mail, terms of conditions, fair use policies, etc.
Auditable and Demonstrable	A CSP must be able to clearly demonstrate to itself, regulators and the public that a solution meets the first three criteria above	Detailed reporting of the traffic management policy effects

Related Resources

You might also find these resources useful:

- The Sandvine whitepaper Network Congestion Management: Considerations and Techniques[5]
- The Sandvine technology showcase The QualityGuard Congestion Response System[6]
- Also, Comcast describes their protocol-agnostic congestion management in RFC 6057, which is available online[7]

Invitation to Provide Feedback

Thank you for taking the time to read this whitepaper. We hope that you found it useful, and that it contributed to a greater understanding of reasonable network management and Network Neutrality in general.

If you have any feedback at all, then please get in touch with us at **whitepapers@sandvine.com**.

5 https://www.sandvine.com/downloads/general/whitepapers/network-congestion-management.pdf

6 https://www.sandvine.com/downloads/general/sandvine-technology-showcases/qualityguard-congestion-response-system.pdf

7 https://tools.ietf.org/html/rfc6057

v20180423

ABOUT SANDVINE

Sandvine helps organizations run world-class networks with Active Network Intelligence, leveraging machine learning analytics and closed-loop automation to identify and adapt to network behavior in real-time. With Sandvine, organizations have the power of a highly automated platform from a single vendor that delivers a deep understanding of their network data to drive faster, better decisions. For more information, visit **sandvine.com** or follow Sandvine on Twitter at **@Sandvine.**

SANDVINE

USA
47448 Fremont Blvd,
Fremont,
CA 94538,
USA
T. +1 510.230.2777

EUROPE
Birger Svenssons
Väg 28D
432 40 Varberg,
Sweden
T. +46 340.48 38 00

CANADA
408 Albert Street,
Waterloo,
Ontario N2L 3V3,
Canada
T. +1 519.880.2600

ASIA
RMZ Ecoworld,
Building-1, Ground Floor,
East Wing Devarabeesanahalli,
Bellandur, Outer Ring Road,
Bangalore 560103, India
T. +91 80677.43333