ATTACHMENT A:

COMCAST CORPORATION
DESCRIPTION OF CURRENT NETWORK MANAGEMENT PRACTICES

COMCAST CORPORATION
DESCRIPTION OF CURRENT NETWORK MANAGEMENT PRACTICES

Pursuant to Paragraphs 54 and 59 of the Commission's *Memorandum Opinion & Order* regarding how Comcast manages congestion on its High-Speed Internet ("HSI") network, Comcast hereby "disclose[s] to the Commission the precise contours of the network management practices at issue here, including what equipment has been utilized, when it began to be employed, when and under what circumstances it has been used, how it has been configured, what protocols have been affected, and where it has been deployed."[1]

I. INTRODUCTION

Comcast's HSI network is a shared network. This means that our HSI customers share upstream and downstream bandwidth with their neighbors. Although the available bandwidth is substantial, so, too, is the demand. Thus, when a relatively small number of customers in a neighborhood place disproportionate demands on network resources, this can cause congestion that degrades their neighbors' Internet experience. In our experience, over the past several years, the primary cause of congestion (particularly in the upstream portion of our network) has been the high-volume consumption of bandwidth associated with use of certain peer-to-peer ("P2P") protocols. In order to tailor our network management efforts to this reality, Comcast's current congestion management practices were designed to address this primary contributor to congestion. Our objective in doing so was to provide all our customers with the best possible broadband Internet experience in the marketplace.

As described in Attachment B, in response to significant stated concerns of the Internet community, Comcast had already announced plans to transition away from its P2P-specific

---

[1] *In re Formal Complaint of Free Press & Pub. Knowledge Against Comcast Corp. for Secretly Degrading Peer-to-Peer Applications; Broadband Industry Practices; Petition of Free Press et al. for Declaratory Ruling That Degrading an Internet Application Violates the FCC's Internet Policy Statement & Does Not Meet an Exception for "Reasonable Network Management,"* Mem. Op. and Order, FCC 08-183 ¶¶ 54, 59 (Aug. 20, 2008) ("*Order*").

congestion management practices and terminate them entirely by December 31, 2008. Paragraph 54 of the *Order* directs Comcast to describe these current practices, and we do so here.[2]

At the outset, we provide some background on how these practices came into being and how they work in a general sense. We then provide the greater detail required by the *Order*.

II. BACKGROUND

To understand exactly how Comcast currently manages congestion on its network, it is helpful to have a general understanding of how Comcast's HSI network is designed.[3] Comcast's HSI network is what is commonly referred to as a hybrid fiber-coax network, with coaxial cable connecting each subscriber's cable modem to an Optical Node, and fiber optic cables connecting the Optical Node, through distribution hubs, to the Cable Modem Termination System ("CMTS"), which is also known as the "data node." The CMTSes are then connected to higher-level routers, which in turn are connected to Comcast's Internet backbone facilities. Today, Comcast has approximately 3300 CMTSes deployed throughout our network, serving our 14.4 million HSI subscribers.

Each CMTS has multiple "ports" that handle traffic coming into and leaving the CMTS. In particular, each cable modem deployed on the Comcast HSI network is connected to the CMTS through the "ports" on the CMTS. These ports can be either "downstream" ports or "upstream" ports, depending on whether they send information to cable modems (downstream) or receive information from cable modems (upstream) attached to the port. Today, on average,

---

[2] Although the *Order* focuses entirely on Comcast's current practices with respect to controlling network congestion, Comcast's efforts to deliver a superior Internet experience involve a wide variety of other network management efforts beyond congestion control. As Comcast has previously explained, we actively manage our HSI network in order to enhance our customers' Internet experience by, among other things, blocking spam, preventing viruses from harming the network and our subscribers, thwarting denial-of-service attacks, and empowering our customers' ability to control the content that enters their homes.

[3] The reader may find it useful to refer to the attached glossary for additional explanation of unfamiliar terms.

about 275 cable modems share the same downstream port and about 100 cable modems share the same upstream port. As will be described later in this document, Comcast's current congestion management practices focus solely on a subset of *upstream* traffic.

Internet usage patterns are dynamic and change constantly over time. As broadband networks deliver higher speeds, this enables the deployment of new content, applications, and services, which in turn leads more and more households to discover the benefits of broadband Internet services. Several years ago, Comcast became aware of a growing problem of congestion on its HSI network, as traffic volumes, particularly for upstream bandwidth (which is provisioned in lesser quantities than downstream bandwidth[4]), were growing rapidly and affecting the use of various applications and services that are particularly sensitive to latency (i.e., packets arriving slowly) or jitter (i.e., packets arriving with variable delay).

In order to diagnose the cause of the congestion and explore means to alleviate it, in May 2005, Comcast began trialing network management technology developed by Sandvine, Inc. The Sandvine technology identified which protocols were generating the most traffic and where in the network the congestion was occurring. After jointly reviewing significant amounts of usage data, Comcast and Sandvine determined that the use of several P2P protocols was regularly generating disproportionate burdens on the network, primarily on the upstream portion of the network, causing congestion that was affecting other users on the network.

As previously explained on the record and described in greater detail below, in order to mitigate congestion, Comcast determined that it should manage *only* those protocols that placed

[4] This asymmetric provisioning of bandwidth is based on how the vast majority of consumers have historically used the Internet, i.e., most consumers have been far more interested in how fast they could surf the web, how fast they could download files, and whether they could watch streaming video than in uploading large files. Even today, with the widespread proliferation of services that place greater demand on upstream resources, most consumers still download much more than they upload, and so we continue to architect our network to optimize the experience of the vast majority of our users. As usage patterns change over time, so, too, will our provisioning practices.

excessive burdens on the network, and that it should manage those protocols in a minimally intrusive way utilizing the technology available at the time. More specifically, in an effort to avoid upstream congestion, Comcast established thresholds for the number of simultaneous unidirectional uploads that can be initiated for each of the managed protocols in any given geographic area; when the number of simultaneous sessions remains below those thresholds, uploads are not managed. The thresholds for each protocol vary depending upon a number of factors discussed in detail below, including how the particular protocol operates and the burden that the particular protocol was determined to place on our upstream bandwidth. These management practices were not based on the type (video, music, data, etc.) or content of traffic being uploaded.

The Sandvine equipment has been used (1) to determine when the number of simultaneous unidirectional upload sessions for a particular P2P protocol in a particular geographic area reaches its pre-determined threshold, and (2) when a threshold is reached, to temporarily delay the initiation of any new unidirectional upload sessions for that protocol until the number of simultaneous unidirectional upload sessions drops below that threshold.

III. WHAT EQUIPMENT IS UTILIZED?

The specific equipment Comcast uses to effectuate its network management practices is a device known as the Sandvine Policy Traffic Switch 8210 ("Sandvine PTS 8210"). Literature describing this product is attached. The following sections explain where and how Comcast uses the Sandvine PTS 8210.

IV. WHERE HAS THE EQUIPMENT BEEN DEPLOYED AND WHEN AND UNDER WHAT CIRCUMSTANCES HAS IT BEEN USED?

Comcast initially began technical trials with the Sandvine PTS 8210s starting in May 2005. Commercial (i.e., not trial) deployment of this equipment took place over an extended period of time, beginning in 2006. We achieved wide-scale deployment in 2007.[5]

On Comcast's network, the Sandvine PTS 8210 is deployed "out-of-line" (that is, out of the regular traffic flow)[6] and is located adjacent to the CMTS. Upstream traffic from cable modems will pass through the CMTS on its way to upstream routers, and then, depending on the traffic's ultimate destination, onto Comcast's Internet backbone. A "mirror" replicates the traffic flow that is heading upstream from the CMTS without otherwise delaying it and sends it to the Sandvine PTS 8210, where the protocols in the traffic flow are identified and the congestion management policy is applied in the manner described in greater detail below. In some circumstances, two small CMTSes located near each other may be managed by a single Sandvine PTS 8210.[7] The following graphics provide a simplified illustration of these two configurations:

[5] Some locations currently have a network design that is different from the standard Comcast network design because we are trialing new protocol-agnostic congestion management practices in those locations, we are preparing those locations for evolution to DOCSIS 3.0 (which has already been launched in one market), or we acquired those systems from other operators and are in the process of standardizing them. The congestion management practices described herein are not used in those systems. The locations of our trials have been widely publicized, but disclosure of proprietary plans regarding the order and timing for network investments and service upgrades would cause substantial competitive harm.

[6] Comcast deploys the Sandvine PTS 8210 "out-of-line" so as to not create an additional potential "point-of-failure" (i.e., a point in the network where the failure of a piece of equipment would cause the network to cease operating properly). The Sandvine equipment can also be deployed "in-line," which can make the management effectuated by the equipment nearly undetectable, but Comcast does not employ this configuration.

[7] Although the PTS generally monitors traffic and effectuates policy at the CMTS level, the session management interface is administered at the Upstream Router, one layer higher in the overall architecture.

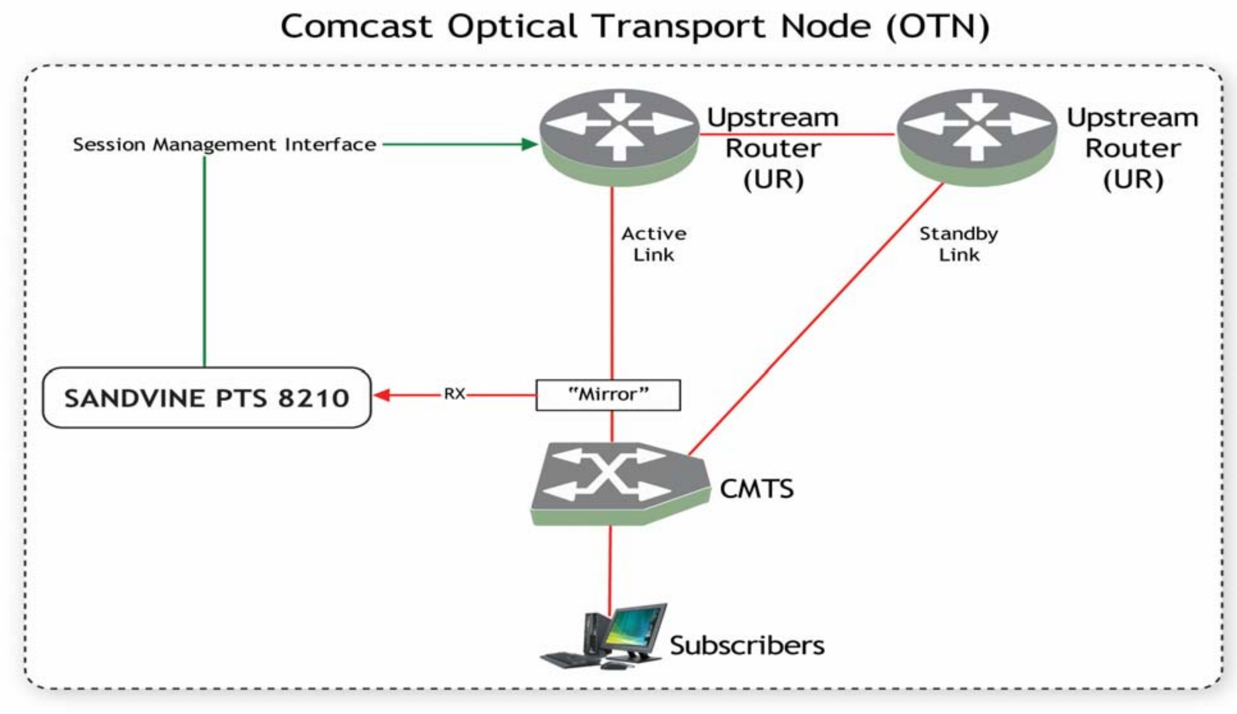


Diagram 1: Sandvine PTS Serving One CMTS.

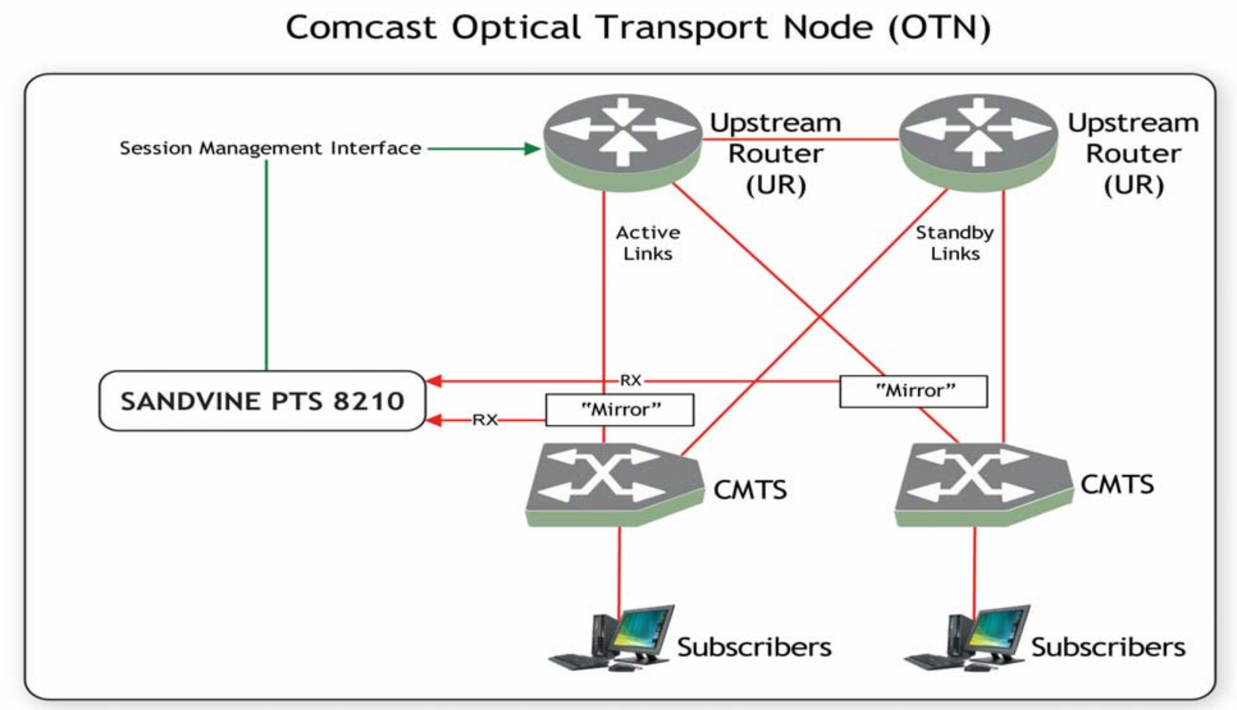


Diagram 2: Sandvine PTS Serving Two CMTSes.

V. HOW HAS THE EQUIPMENT BEEN CONFIGURED AND WHAT PROTOCOLS HAVE BEEN AFFECTED?

For purposes of managing network congestion,[8] the Sandvine PTS 8210 has been configured to identify unidirectional P2P uploads for the protocols -- identified below -- that were determined to be the primary causes of upstream congestion.[9] To do this, the Sandvine PTS uses technology that processes the addressing, protocol, and header information of a particular packet to determine the session type. The Sandvine PTSes, as deployed on Comcast's network, *do not inspect the content*. These devices only examine the relevant header information in the packet that indicates what type of protocol is being used (i.e., P2P, VoIP, e-mail, etc.). The equipment used does *not* read the contents of the message in order to determine whether the P2P packet is text, music, or video; listen to what is said in a VoIP packet; read the text of an e-mail packet; identify whether any packet contains political speech, commercial speech, or entertainment; or try to discern whether packets are personal or business, legal or illicit, etc.

The following diagram graphically depicts the session identification technique undertaken by the Sandvine PTS 8210 as deployed on Comcast's network. The first layers include addressing, protocol, and other "header" information that tells the network equipment what kind of packet it is. The "content" layer is the actual web page, music file, picture, video, etc., and is not examined by the Sandvine equipment.

---

[8] The Sandvine PTS 8210 has not been used solely to manage congestion. It also performs numerous functions related to network management and security, including traffic analysis, anti-spam measures, denial-of-service attack prevention, and other similar functions.

[9] A "unidirectional upload" session is different from an upload associated with a "bidirectional upload" session. A session is considered bidirectional when the user is simultaneously uploading to *and* downloading from another individual using a single TCP flow. Two of the protocols that are managed, BitTorrent and eDonkey, use bidirectional sessions; the other protocols only use unidirectional sessions. A large percentage of P2P traffic is bidirectional and is not managed by these techniques.

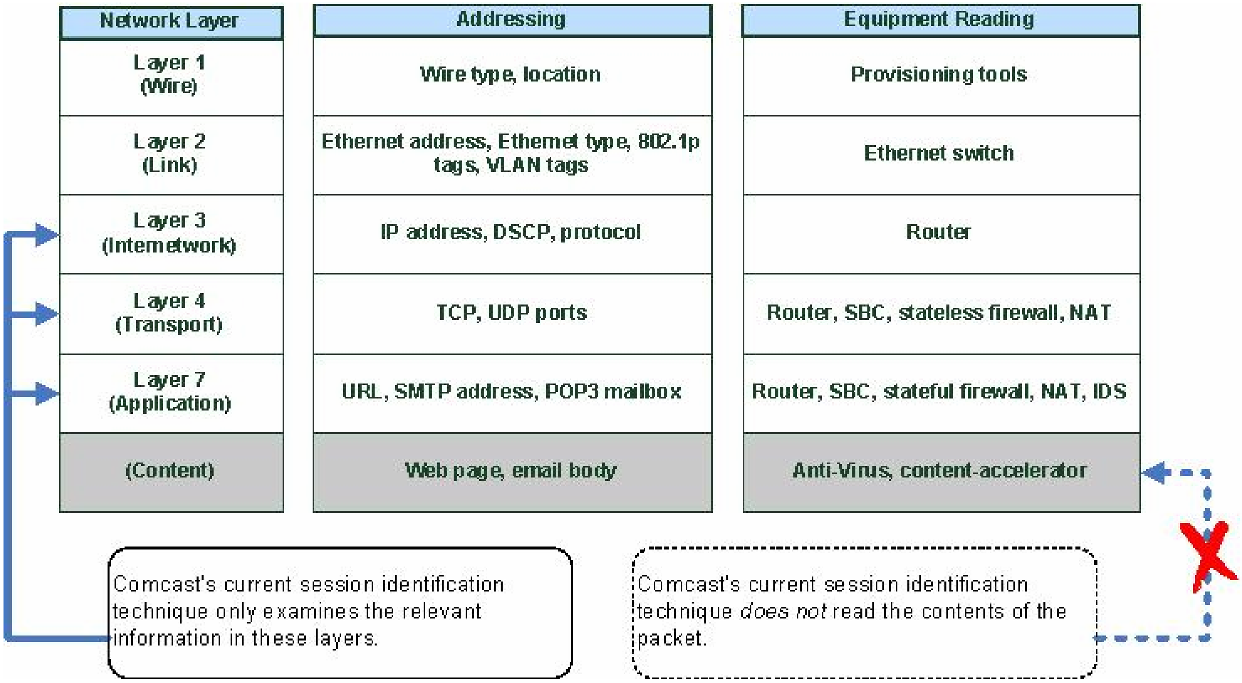


Diagram 3: Session Identification Technique.

In selecting which P2P protocol uploads to manage, network data were analyzed that identified the particular protocols that were generating disproportionate amounts of traffic. Based on that analysis, five P2P protocols were identified to be managed: Ares, BitTorrent, eDonkey, FastTrack, and Gnutella. Four of those protocols have been subject to Comcast's management practices since Comcast first implemented these practices. Ares was added in November 2007 after traffic analysis showed that it, too, was generating disproportionate demands on network resources.

For each of the managed P2P protocols, the PTS monitors and identifies the number of simultaneous unidirectional uploads that are passed from the CMTS to the upstream router. Because of the prevalence of P2P traffic on the upstream portion of our network, the number of simultaneous unidirectional upload sessions of any particular P2P protocol at any given time serves as a useful proxy for determining the level of overall network congestion. For each of the protocols, a session threshold is in place that is intended to provide for equivalently fair access between the protocols, but still mitigate the likelihood of congestion that could cause service degradation for our customers.

Developing session thresholds for each P2P protocol must take into account the unique characteristics and behavior of each particular protocol. For example, BitTorrent and eDonkey use both bidirectional and unidirectional upload sessions, whereas Ares, FastTrack, and Gnutella only use unidirectional upload sessions.[10] And even between BitTorrent and eDonkey, there are significant differences. The BitTorrent protocol more heavily promotes bidirectional uploads as compared to eDonkey, so, while they both may have the same total number of sessions, BitTorrent would have a much higher percentage of bidirectional sessions than eDonkey. Differences also arise between Ares, FastTrack, and Gnutella. For example, each protocol consumes different amounts of bandwidth per session (e.g., a high percentage of Ares unidirectional uploads consume negligible bandwidth).

The following table lays out by protocol the simultaneous unidirectional upload session thresholds for each protocol as well as the typical ratio of bidirectional to unidirectional traffic observed on our HSI network for those P2P protocols that use both, and other factors that contribute to the overall bandwidth consumption by protocol.

[10] Session thresholds are not applied to bidirectional uploads so as to not interfere with the corresponding download.

Protocol	Ratio Bi:Uni	Session Equivalence[11]	Uni Threshold	Notes
Ares	(N/A)	150	150	Many overhead flows exist for signaling, using little or no bandwidth. The session limit is set higher to account for this. Ares is typically used for small files.
BitTorrent	~20:1	~160	8	High ratio of bidirectional to unidirectional flows. The bidirectional to unidirectional ratio varies. Typically used for large files.
eDonkey	~.3:1	~42	32	Low ratio of bidirectional to unidirectional flows. Used for large files.
FastTrack	(N/A)	24	24	Typically used for large files.
Gnutella	(N/A)	80	80	Typically used for small files.

Table 1: Managed Protocols, Relevant Thresholds, and Other Notes

When the number of unidirectional upload sessions for any of the managed P2P protocols for a particular Sandvine PTS reaches the pre-determined session threshold, the Sandvine PTS issues instructions called "reset packets" that delay unidirectional uploads for that particular P2P protocol in the geographic area managed by that Sandvine PTS. The "reset" is a flag in the packet header used to communicate an error condition in communication between two computers on the Internet. As used in our current congestion management practices, the reset packet is used to convey that the system cannot, at that moment, process additional high-resource demands without creating risk of congestion. Once the number of simultaneous unidirectional uploads falls below the pre-determined session limit threshold for a particular protocol, new uploads using that protocol are allowed to proceed. Some significant percentage of P2P sessions last

[11] This number reflects the total number of sessions that we estimate are on-going at any moment in time when the number of simultaneous upload sessions has met the threshold that has been established for that protocol.

only a few seconds, so, even when the thresholds are met, new opportunities for unidirectional uploads generally occur quite frequently.

VI. CONCLUSION

Data collected from our HSI network demonstrate that, even with these current management practices in place, P2P traffic continues to comprise approximately half of all upstream traffic transmitted on our HSI network -- and, in some locations, P2P traffic is as much as two-thirds of total upstream traffic. The data also show that, even for the most heavily used P2P protocols, more than 90 percent of these flows are unaffected by the congestion management. Data recently collected from our network show that, when a P2P upload from a particular computer was delayed by a reset packet, that same computer successfully initiated a P2P upload within one minute in 80 percent of the cases. In fact, most of our customers using P2P protocols to upload on any given day never experienced any delay at all.

Nonetheless, as Comcast previously stated and as the Order now requires, *Comcast will end these protocol-specific congestion management practices throughout its network by the end of 2008.*

Basic Glossary

Cable Modem:

A device located at the customer premise used to access the Comcast High Speed Internet (HSI) network. In some cases, the cable modem is owned by the customer, and in other cases it is owned by the cable operator. This device has an interface (i.e., someplace to plug in a cable) for connecting the coaxial cable provided by the cable company to the modem, as well as one or more interfaces for connecting the modem to a customer's PC or home gateway device (e.g., router, firewall, access point, etc.). In some cases, the cable modem function, i.e., the ability to access the Internet, is integrated into a home gateway device or embedded multimedia terminal adapter (eMTA). Once connected, the cable modem links the customer to the HSI network and ultimately the broader Internet.

Cable Modem Termination System (CMTS):

A piece of hardware located in a cable operator's local network (generally in a "headend") that acts as the gateway to the Internet for cable modems in a particular geographic area. A simple way to think of the CMTS is as a router with interfaces on one side leading to the Internet and interfaces on the other connecting to Optical Nodes and then customers.

Cable Modem Termination System Port:

A CMTS has both upstream and downstream network interfaces to serve the local access network, which we refer to as upstream or downstream ports. A port generally serves a neighborhood of hundreds of homes.

Channel Bonding:

A technique for combining multiple downstream and/or upstream channels to increase customers' download and/or upload speeds, respectively. Multiple channels from the HFC network can be bonded into a single virtual port (called a bonded group), which acts as a large single channel or port to provide increased speeds for customers. Channel bonding is a feature of Data Over Cable Service Interface Specification (DOCSIS) version 3.

Coaxial Cable (Coax):

A type of cable used by a cable operator to connect customer premise equipment (CPE) -- such as TVs, cable modems (including embedded multimedia terminal adapters), and Set Top Boxes -- to the Hybrid Fiber Coax (HFC) network. There are many grades of coaxial cable that are used for different purposes. Different types of coaxial cable are used for different purposes on the network.

Comcast High Speed Internet (HSI):

A service/product offered by Comcast for delivering Internet service over a broadband connection.

Customer Premise Equipment (CPE):

Any device that resides at the customer's residence.

Data Over Cable Service Interface Specification (DOCSIS):

A reference standard that specifies how components on cable networks need to be built to enable HSI service over an HFC network. These standards define the specifications for the cable modem and the CMTS such that any DOCSIS certified cable modem will work on any DOCSIS certified CMTS independent of the selected vendor. The interoperability of cable modems and cable modem termination systems allows customers to purchase a DOCSIS certified modem from a retail outlet and use it on their cable-networked home. These standards are available to the public at the CableLabs website, at http://www.cablelabs.com.

Downstream:

Description of the direction in which a signal travels. Downstream traffic occurs when users are downloading something from the Internet, such as watching a YouTube video, reading web pages, or downloading software updates.

Headend:

A cable facility responsible for receiving TV signals for distribution over the HFC network to the end customers. This facility typically also houses the cable modem termination systems. This is sometimes also called a "hub."

Hybrid Fiber Coax (HFC):

Network architecture used primarily by cable companies, comprising of fiber optic and coaxial cables that deliver Voice, Video, and Internet services to customers.

Internet Protocol (IP):

Set of standards for sending data across a packet switched network like the Internet. In the Open System Interconnection Basic Reference Model (OSI) model, IP operates in the "Network Layer" or "Layer 3." The HSI product utilizes IP to provide Internet access to customers.

Internet Protocol Detail Record (IPDR):

Standardized technology for monitoring subscribers' upstream and downstream Internet usage data based on their cable modem. The data is collected from the CMTS and sent to a server for further processing. Additional information is available at: http://www.ipdr.org.

Optical Node:

A component of the HFC network generally located in customers' local neighborhoods that is used to convert the optical signals sent over fiber-optic cables to electrical signals that can be sent over coaxial cable to customers' cable modems, or vice versa. A fiber optic cable connects the Optical Node, through distribution hubs, to the CMTS and coaxial cable connects the Optical Node to customers' cable modems.

Open System Interconnection Basic Reference Model (OSI Model):

A framework for defining various aspects of a communications network in a layered approach. Each layer is a collection of conceptually similar functions that provide services to the layer above it, and receive services from the layer below it. The seven layers of the OSI model are listed below:

Layer 7 – Application
Layer 6 – Presentation
Layer 5 – Session
Layer 4 – Transport
Layer 3 – Network
Layer 2 – Data Link
Layer 1 – Physical

Port:

A port is a physical interface on a device used to connect cables in order to connect with other devices for transferring information/data. An example of a physical port is a CMTS port. Prior to DOCSIS version 3, a single CMTS physical port was used for either transmitting or receiving data downstream or upstream to a given neighborhood. With DOCSIS version 3, and the channel bonding feature, multiple CMTS physical ports can be combined to create a virtual port.

Provisioned Bandwidth:

Comcast-specific definition The peak speed associated with a tier of service purchased by a customer. For example, a customer with a 16 Mbps/2 Mbps (Down/Up) speed tier would be said to be provisioned with 16 Mbps of downstream bandwidth and 2 Mbps of upstream bandwidth.

Quality of Service (QoS):

Set of techniques to manage network resources to ensure a level of performance to specific data flows. One method for providing QoS to a network is by differentiating the type of traffic by class or flow and assigning priorities to each type. When the network becomes congested, the data packets that are marked as having higher priority will have higher likelihood of getting serviced.

Transmission Control Protocol (TCP):

Set of standard rules for reliably communicating data between programs operating on computers. TCP operates in the "Transport Layer" or "Layer 4" of the OSI model and deals with the ordered delivery of data to specific programs. If we compare the data communication network to the US Postal Service mail with delivery confirmation, the Network Layer would be analogous to the Postal Address of the recipient where the TCP Layer would be the ATTN field or the person that is to receive the mail. Once the receiving program receives the data, an acknowledgement is returned to the sending program.

Upstream:

Description of the direction in which a signal travels. Upstream traffic occurs when users are uploading something to the network, such as sending email, sharing P2P files, or uploading photos to a digital photo website.

Sandvine Policy Traffic Switch Portfolio


Real Performance. Real Networks. Real Intelligence

Sandvine Policy Traffic Switch (PTS) portfolio helps service providers to better profit from application traffic. Our policy management solutions address key challenges such as managing bandwidth-intensive traffic, controlling malicious threats, enabling new services and identifying application quality trends. These policy management solutions are deployed on a single intelligent platform to simplify the network architecture and ensure a fast return on investment.

Service providers today are focusing on policy management solutions to differentiate and protect their IP service offering. This critical technology must be easily deployed throughout the network and delivered reliably for today's demanding subscribers. Sandvine has recognized these important requirements with the introduction of 10 GE interfaces, scalable performance with the largest network deployment base of 80Gbps and an innovative approach to transparently handle asymmetry in large tier-one networks.

With extensive deployments worldwide, Sandvine has proven experience in large service provider networks. Let us show you how we can help your business.

sandvine®
Intelligent Broadband Networks

Policy Management Solutions

Sandvine's portfolio of policy management solutions addresses immediate challenges throughout the service provider: Engineering must manage growing bandwidth pressures; Marketing must launch new services; Security must control network threats; and Network Operations has to ensure service quality. Sandvine provides visibility into application traffic along with a powerful set of policy solutions.

Traffic Optimization

File-sharing traffic still dominates networks with even more subscribers actively using P2P today. The implication is clear – Network Engineering must preserve the subscriber experience while managing traffic intelligently. Sandvine's Intelligent Traffic Management solution offers the widest range of subscriber fairness options including P2P session management and adaptive traffic shaping. And our powerful network-class capability enables service providers to easily tailor traffic policies for each service category.

Network Integrity

A service provider's own subscribers have become a major source of malicious traffic leading to inconsistent service quality. Sandvine's Network Integrity solution protects the network against unpredictable attacks such as worms, DoS attacks, spam trojans and DNS server attacks. Our unique combination of DPI signature recognition plus behavioral analysis means effective zero-day protection and fewer customer support calls.

Service Creation

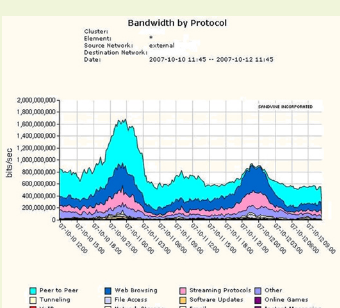
Today's best-effort networks are poorly suited to deal with jitter and delay sensitive multimedia applications. This means service providers have an immediate opportunity to introduce new prioritized services for gaming, VoIP and other multimedia applications. The latest capabilities of the PTS enable service providers to generate an additional revenue stream from targeted advertising.

Operations Management

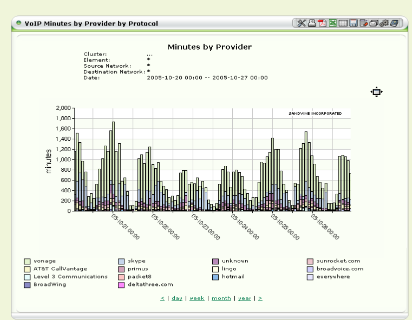
Residential subscribers are demanding higher service quality as Internet applications, particularly VoIP, become a key part of our lifestyles. The result for service providers? Escalating costs as Customer Support deal with difficult complaints about service degradation. Sandvine's solution uses comprehensive VoIP QoE metrics to alert Network Operations about VoIP quality trends so they can resolve problems before subscribers are affected.

What are your subscribers doing online?

Subscriber behavior has always been difficult to characterize. What applications are popular? How does usage vary by service? Are third-party services increasing? Sandvine Network Demographics reporting, without impinging on subscriber privacy, provides valuable insights into application behavior and trends.



And with an understanding of subscriber behavior comes the ability to implement policies that improve the subscriber experience.



PTS Platform Advantages

Gain Control & Visibility

Major service provider networks are prone to asymmetric routes where inbound and outbound traffic for a subscriber follow different routes - making stateful identification impossible. Sandvine has overcome this challenge with unique cluster technology that ensures accurate protocol identification without any changes to the network routing. Today, most service providers are deploying PTS platforms towards the services edge of the network for maximum visibility of subscriber traffic – this ensures application traffic is properly prioritized as it first enters the network and provides complete network-wide reporting.

True Scalability

Our PTS portfolio provides true scalability for extremely cost-effective deployments from small remote hubs to large centralized sites. The PTS 14000 and PTS 8210 platforms offer a broad selection of performance, interface types and port densities that are easily tailored to the wide-ranging sites across large service provider networks. Both platforms deliver the same proven feature set to ensure that subscriber services and traffic management policies are universal across the entire network.

The PTS 14000 architecture delivers up to a remarkable 80 Gbps easily handling today's growing multimedia traffic. In addition, Sandvine's Virtual Switch Clusters combine the inspection performance and data ports from multiple PTS 14000 units to deliver the performance necessary at major aggregation points.

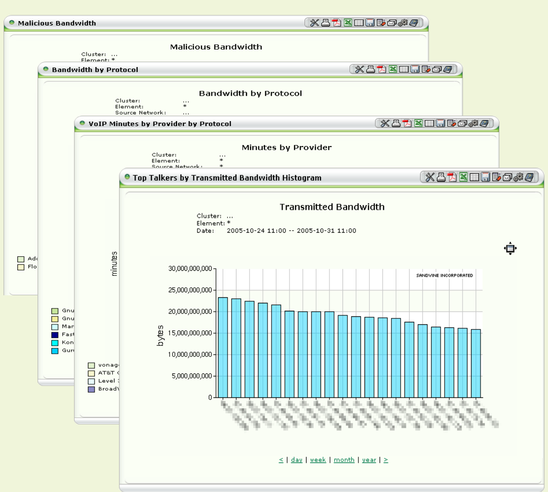
Leading Redundancy Options

High availability is critical throughout the services architecture so Sandvine provides a complete range of redundancy features and options. For many service providers, the preferred approach is to introduce n:n+1 redundancy, that is not only extremely cost-effective, but offers more comprehensive protection than simple hardware replication alone. Our integrated interface-bypass capability ensures that subscriber traffic continues uninterrupted in the event of a power failure or major system event.

Centralized Policy Management

Our Service Definition Manager grants service providers complete control over their network. The intuitive and user-friendly GUI enables them to configure and deploy network-wide policies quickly and easily from a central management system. The Service Definition Manager also provides centralized physical element administration, deployments management and network association control.

Let Sandvine recommend the best deployment options for your unique service provider network.



With over 150 fully-customizable reports, Sandvine Network Demographics provides decision-critical information to major organizational departments - including marketing, operations, security, and support.

Characterize and apply policy to:

- Peer-to-Peer
- Web Browsing
- News Groups
- Instant Messaging
- Email
- Database
- Streaming Protocols
- Tunneling (including VPN)
- VoIP
- Remote Connectivity
- Network Administration
- File Access Protocols
- Network Storage protocols
- Gaming protocols
- ...and many more.

Technical Summary

General

- PTS platforms are highly scalable network elements enabling Sandvine's full suite of policy management solutions
- Leading stateful traffic identification using advanced signature recognition and behavioral analysis
- Broadest range of policy management options including unique subscriber fairness approaches to preserve your subscribers' Internet experience
- Cluster technology delivers unmatched scalability and easily solves network asymmetric route challenges

Platform and Interface Options

Platforms can be deployed independently or as clusters with PTS 14000 Virtual Switch Clusters delivering up to 80 Gbps performance.

Platform	1452X	1451X	1421X	8210
Performance	10 Gbps	10 Gbps	4 Gbps	1 Gbps
10 GE	2 port	-	-	-
GE MM or SM	-	12 port	12 port	4 port
10/100/1000T	-	12 port	12 port	4 port
1GE Integration	4	8	8	1 port
10 GE Integration	6 port	2 port	2 port	-

* Performance shown as aggregate throughput
* Maximum number of interface ports is shown
* Bypass interfaces can be internal and/or external
* 10GE Integration ports are normally used for virtual switch cluster connectivity

High Availability

- n:n+1 for simple, cost-effective redundancy
- Interface bypass option for power failures and major system events
- Optional features such as hardware replication and link-pair redundancy

Protocol Support

- Peer-to-peer, web browsing, news groups, instant messaging, email, database, streaming protocols, tunneling including VPN, VoIP, remote connectivity, network administration, file access protocols, network storage protocols, game protocols

Policy Management

- Powerful network-class capability to apply policy management by service type
- Session Management – optimizes upstream bandwidth - intensive application sessions
- FairShare™ - allocates equitable network resouces during periods of congestion
- Traffic Shaping - manages aggregate or per subscriber application traffic
- Integration Interfaces - targeted advertising, caching, content filtering and traffic mirroring
- Applicationn Marking - sets application IP TOS/DSCP field bits to identify prioritized traffic
- Captive portal communications - redirects user HTTP sessions to target URL for better service management
- Attack Traffic Mitigation detects and mitigates network threats before services are affected

Subscriber Policy Broker

- Subscriber Policy Broker for simple, centralized policy definition & management
- Service Definition Manager - user friendly and intuitive GUI for quick and easy centralized policy configuration and deployment
- Industry-standard API to easily integrate with external systems
- Subscriber identification option via DHCP, RADIUS, Diameter or OSS integration

Network Demographics

- Advanced application reporting with full network-wide, region and subscriber views
- Unique network-class reporting to better understand subscriber behavior
- Value-added analysis including VoIP call details and QoE reporting

Physical Specifications *(PTS 14000 / 8210)*

- Dimensions: W 17" x H 7" x D 23" (432mm x 177.8mm x 584.2mm) / W 16.75" x H 1.75" x D 22.5" (419mm x 44.4mm x 571.5mm)
- Mounting: 19" rack - 4 RU / 19" rack - 1 RU
- Weight: 75 lbs (34 kg) / 24 lbs (11 kg)
- AC 100 – 240 V or DC 42 – 60 V input
- Operating temperature 0˚C to +40˚C
- Humidity 5% to 85% non-condensing

Approvals

- NEBS Level 3 compliance
- Product Safety and EMC approvals for Argentina, Australia, Canada, Europe, Mexico, New Zealand, Russia, South Africa, South Korea, Taiwan and USA

sandvine®
Intelligent Broadband Networks

Headquarters
Sandvine Incorporated
Waterloo, Canada (GMT-5)
Phone: +1 519.880.2600
Email: sales@sandvine.com

European Offices
Sandvine Limited
Basingstoke, UK (GMT)
Phone: +44 (0) 1256 698021
Email: sales@sandvine.co.uk

Visit www.sandvine.com

Last Revised:2008-05-14