BEFORE THE

Federal Communications Commission

WASHINGTON, D.C.

	)	
In the Matter of	)	
	)	
Effects on Broadband Communications Networks	)	PS Docket No. 10-92
Of Damage to or Failure of Network Equipment	)	
Or Severe Overload	)	
	)	

COMMENTS OF COMCAST CORPORATION

Kathryn A. Zachem
Mary P. McManus
David M. Don
COMCAST CORPORATION
2001 Pennsylvania Ave., NW
Suite 500
Washington, DC 20006
(202) 379-7134

Brian A. Rankin
COMCAST CABLE
COMMUNICATIONS, LLC
One Comcast Center
1701 John F. Kennedy Boulevard
Philadelphia, PA 19103-2838

James L. Casserly
Ryan G. Wallach
Daniel K. Alvarez
WILLKIE FARR & GALLAGHER LLP
1875 K Street, N.W.
Washington, DC 20006

Attorneys for Comcast Corporation

June 25, 2010

TABLE OF CONTENTS

Page

I. INTRODUCTION AND SUMMARY 1

II. COMCAST HAS DESIGNED ITS BROADBAND NETWORK TO MAXIMIZE RELIABILITY AND SURVIVABILITY. 4

A. Comcast's Broadband Network Is Designed To Minimize the Number of Major Single Points of Failure. 5

B. Comcast's Broadband Network Has Redundant Facilities and Links That Ensure the Ongoing Reliability of Comcast's Services. 10

C. Comcast Provisions Bandwidth To Account for Potentially Severe Traffic Loads in Order To Prevent Any Traffic Spike from Crippling the Network. 13

III. REAL-WORLD EXPERIENCES CONFIRM THE RELIABILITY AND SURVIVABILITY OF COMCAST'S BROADBAND NETWORK. 15

IV. GIVEN THE DYNAMIC NATURE OF BROADBAND NETWORKS AND THE DIVERSE MEANS TO CORRECT PROBLEMS, THE COMMISSION SHOULD REFRAIN FROM MANDATING SOLUTIONS FOR POTENTIAL PROBLEMS. 16

V. CONCLUSION 19

BEFORE THE

Federal Communications Commission

WASHINGTON, D.C.

In the Matter of	)	
Effects on Broadband Communications Networks Of Damage to or Failure of Network Equipment Or Severe Overload	)	PS Docket No. 10-92

COMMENTS OF COMCAST CORPORATION

Comcast Corporation ("Comcast") hereby responds to the above-captioned Notice of Inquiry ("*Notice*").[1] The *Notice* seeks comment on a number of issues related to the reliability and survivability of broadband networks. Comcast is proud of how it has designed its broadband network and implemented safeguards to ensure that its network is reliable and resilient even in the face of extreme conditions. Comcast is pleased to share this information with the Commission so that it better understands the present state of survivability in broadband networks and that any vulnerabilities to failures are minimal.

I. INTRODUCTION AND SUMMARY

Over the past 15 years, the Internet has become a central feature in the lives of hundreds of millions of Americans who use it as a hub for information, entertainment, commerce, politics, education, social and cultural development, and so much more. Congress, in the Telecommunications Act of 1996 (the "1996 Act"), foresaw that the Internet represented "an

---

[1] *See In re Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload*, Notice of Inquiry, 25 FCC Rcd. 4333 (2010) ("*Notice*").

extraordinary advance in the availability of educational and informational resources to our citizens" that would "offer users a great degree of control over the information they receive"; provide "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity"; and deliver "a variety of political, educational, cultural, and entertainment services."[2] That vision is a reality for the more than 200 million Americans who have broadband Internet service today, and is within reach for the 90 million Americans who can obtain broadband Internet service, but choose not to.[3] This success is due primarily to the investment in and deployment of innovative, reliable broadband networks by the private sector.[4]

In response to the deregulatory policies enacted by Congress in the 1996 Act, cable, telephone, wireless, satellite, and other companies invested hundreds of billions of dollars to build state-of-the-art broadband networks that today are available to over 95 percent of Americans.[5] The cable industry alone has invested $160 billion in broadband networks in that timeframe.[6] The deployment of these broadband networks has directly and indirectly created millions of jobs and has been an integral part of this nation's economic growth and development.

---

[2] Telecommunications Act of 1996, Pub. L. No. 104-104, § 509, 110 Stat. 56, 138 (codified at 47 U.S.C. § 230(a)).

[3] *See Connecting America: The National Broadband Plan*, at xi, 3, 6 n.7, 20 (Mar. 16, 2010), *available at* http://download.broadband.gov/plan/national-broadband-plan.pdf.

[4] *See id.* at xi ("Fueled primarily by private sector investment and innovation, the American broadband ecosystem has evolved rapidly.").

[5] *See id.* at 20 ("Today, 290 million Americans -- 95% of the U.S. population -- live in housing units with access to terrestrial, fixed broadband infrastructure . . . .").

[6] *See* Nat'l Cable & Telecomm. Ass'n, Investments in Infrastructure, http://www.ncta.com/StatsGroup/Investments.aspx (last visited June 21, 2010) (reporting that cable industry capital expenditures between 1996 and 2009 totaled $161.2 billion, with capital expenditures for 2009 totaling $14.4 billion).

Across the nation, cable operators are using their broadband networks to offer consumers broadband Internet service with download speeds of 10, 20, 50, and 100 Mbps or more.[7]

Since 1996, Comcast has invested tens of billions of dollars to deploy fiber and upgrade its network. This has enabled Comcast to make dramatic improvements in our cable services and to introduce new services, including broadband Internet service. Today, Comcast High-Speed Internet ("HSI") service is available to over 99 percent of the homes in our footprint.[8] More than 50 million American households can now access Comcast's HSI service, and over 16.4 million do so.[9] As a result of our investments, and the quality service we deliver, Comcast has become the largest provider of residential broadband Internet service in the nation. Our broadband network is reliable and resilient, and it can meet consumers' demands for broadband Internet service with more bandwidth and more speed today and into the future.

Throughout this time, network operators (whether private, academic, or government) have taken responsibility for ensuring that their broadband networks delivered the services that consumers needed and demanded. For decades, the survivability and reliability of the Internet has been entrusted to network operators, individually, and working in collaboration with each other and with broad-based third-party technical groups. The result has been a remarkably resilient and reliable network of broadband networks that use packet-switched technology and that have many built-in redundancies and few single points of failure.

---

[7] *See, e.g.*, Press Release, Cablevision Sys. Corp., *Cablevision Breaks the Century Mark* (Apr. 28, 2009), *available at* http://www.cablevision.com/about/news/article.jsp?d=042809.

[8] *See* Comcast Corp., *Earnings First Quarter 2010: Trending Schedules* (Apr. 28, 2010), *available at* http://www.cmcsk.com/earningdetails.cfm?QYear=2010&QQuarter=1.

[9] *See id.*

Packet-switched networks, by their very nature, are designed to be resilient and reliable.[10] The technical groups that make up the "Internet community" -- e.g., North American Network Operators Group ("NANOG"), Internet Engineering Task Force ("IETF"), Internet Society ("ISOC"), Internet Corporation for Assigned Names and Numbers ("ICANN"), Message Anti-Abuse Working Group ("MAAWG"), and others -- have played a key role in how broadband networks have been designed and deployed to ensure that the Internet keeps running smoothly and efficiently. These kinds of inclusive and broad-based Internet technical groups, in collaboration with groups such as the Commission's Communications Security, Reliability, and Interoperability Council ("CSRIC") and the newly-formed Broadband Internet Technology Advisory Group ("BITAG"), should continue to play an important role in maintaining a well-functioning Internet.[11] A collaborative, results-oriented, open process for addressing engineering and management issues has been the hallmark of Internet governance from the very beginning.

II. COMCAST HAS DESIGNED ITS BROADBAND NETWORK TO MAXIMIZE RELIABILITY AND SURVIVABILITY.

The *Notice* seeks comment on several issues concerning reliability and survivability of broadband networks, including broadband networks' ability to withstand and recover from physical damage, the adequacy and effectiveness of redundancy in broadband networks to ensure

---

[10] As the Commission explained as far back as 1998: "Instead of maintaining an end-to-end channel of communications for the length of the information transfer, packet switching breaks the information up into smaller packets that are transmitted separately over the most efficient route available, and then reassembled, microseconds later, at their destination." *In re Deployment of Wireline Services Offering Advanced Telecommunications Capability*, Memorandum Opinion & Order & NPRM, 13 FCC Rcd. 24011 ¶ 6 (1998).

[11] Communications Security, Reliability and Interoperability Council (CSRIC), http://www.fcc.gov/pshs/advisory/csric/ (last visited June 21, 2010); Press Release, Broadband Internet Tech. Advisory Group, *Initial Plans for Broadband Internet Technical Advisory Group Announced* (June 9, 2010), *available at* http://www.prnewswire.com/news-releases/initial-plans-for-broadband-internet-technical-advisory-group-announced-95950709.html.

that networks can "rout[e] around failures," and broadband networks' ability "to maintain effective operation during severe network congestion or overload" during pandemics and similar events.[12] These are not novel concerns for networks, however. Network operators have had to safeguard against potential failures ever since networks were first invented. Importantly, when it comes to the broadband networks that make up the Internet, actual incidents of failure are infrequent and brief because of the design of most networks and because of safeguards against failures implemented by network operators. As America's leading provider of residential broadband Internet service, Comcast has designed its broadband network and implemented safeguards to ensure that the network can continue to deliver the service customers expect and demand, even under challenging circumstances.

A. Comcast's Broadband Network Is Designed To Minimize the Number of Major Single Points of Failure.

From its inception, Comcast's broadband network has been designed to be reliable and resilient. The primary method by which Comcast ensures its broadband network is reliable and resilient is by building into its network significant redundancy and back-up systems in order to minimize major single points of failure in any part of the network. To date, this design approach has been extremely successful in allowing Comcast to meet the needs of its customers in all manner of adverse conditions.

As a general matter, Comcast typically designs its broadband network based on an active/active design (as opposed to an active/standby design). This means that, rather than only using back-up systems in the event of a failure to the primary system, Comcast's "back-up"

---

[12] *Notice* ¶¶ 7, 10, 13, 15.

systems are in active use on a daily basis, but with sufficient capacity to accommodate any failures that may occur to the primary system. Comcast has found that operating a back-up system with reserve capacity is better than keeping the back-up system in standby mode, as a system that is regularly in use tends to be prepared to handle disasters more readily than a system that has been sitting idle and unused for an extended period of time. Such an approach is utilized for many of our services. By building active redundancy into the broadband network, Comcast is able to safeguard against virtually any unexpected failure of part of the network.

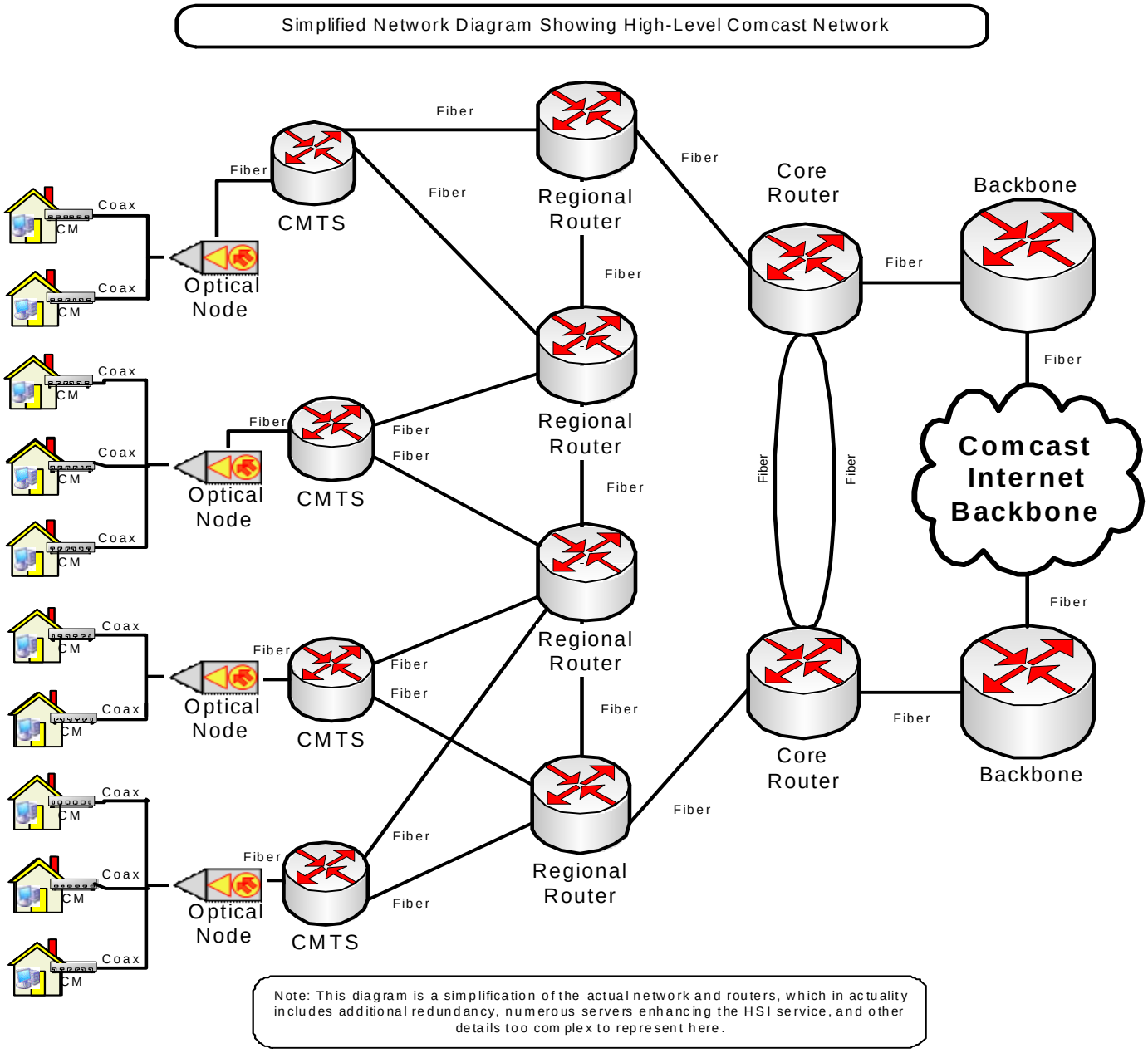
The local portion of Comcast's broadband Internet network is what is commonly referred to as a hybrid fiber-coax network, with coaxial cable connecting each customer's cable modem (or other equipment) to the customer's local neighborhood Optical Node, and over 147,000 miles of fiber optic cables connecting the Optical Nodes to the Cable Modem Termination Systems ("CMTSes"), the regional networks, and the backbone.[13] Each CMTS has routers with multiple "ports" that handle traffic coming from and going to various Optical Nodes and then from the Optical Nodes to the equipment in customers' homes.[14] Today, Comcast has over 3000 CMTSes deployed throughout our broadband network. Routers at the CMTSes are then connected (or "homed") via fiber links into at least two different regional routers (or, occasionally, different cards on the same router) located in the regional network. If any single router or card fails, traffic is automatically re-routed around the failed router or card.

---

[13] By running fiber deep into neighborhoods and utilizing existing coaxial cable from an Optical Node to customers' homes, Comcast has been able to rapidly deploy broadband infrastructure that offers the highest quality of services to a broad and diverse population. This technology also affords Comcast the ability to expand service offerings and further extend the fiber portion of its network as required to satisfy consumer demand.

[14] 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.

The following diagram provides a simplified graphical depiction of Comcast's broadband Internet network architecture in most markets:



As Diagram 1 depicts, in order to localize and minimize the effects of any network failure, as traffic moves away from customers' homes, Comcast builds even more redundancy into the broadband network. For example, the regional networks are generally built around a

central fiber ring with at least two core routers. These regional networks typically are composed of "strings" of routers, with each regional router connected to the string by at least two independent fiber connections (i.e., each router is "dual-homed" to the string of routers), and the string itself dual-homed to the core routers, and then from the core routers to the backbone network. This design builds into the network significant redundancy that minimizes single points-of-failure and ensures that the network can withstand multiple failures with minimal effect on as few customers as possible.

Moreover, capacity planning is undertaken with an eye towards ensuring that capacity is available in failure scenarios. Each of the routers and links between routers is designed to have sufficient capacity to handle any traffic increases from a failed router or card. Comcast's regional and backbone networks are comprised of fiber links deployed in 10 Gigabit increments (i.e., 10 Gbps, 20 Gbps, etc.), with a number of links currently exceeding 40 Gbps. By deploying additional capacity in 10 Gigabit increments, Comcast ensures that any upgrade to capacity provides sufficient capacity for traffic growth on that network link, as well as sufficient capacity to carry traffic if another link goes down for any reason. In addition, Comcast's broadband network has significant reserve capacity that can handle unexpected surges in traffic (such as one might expect during a pandemic, or what Comcast experienced during the significant weather incidents in the Mid-Atlantic and Northeastern United States this past winter).

Comcast's backbone is extensive, and almost every location it serves throughout the country has multiple fiber links to other locations. As a result, if one fiber link goes down, then traffic is simply rerouted over one of the other links. In effect, Comcast's backbone network is designed to serve as a nationwide, interconnected fiber ring with fiber running around the points

on the outside of the ring as well as crisscrossing between various hubs in the middle of the ring. Thus, if any single fiber link, router, or card fails, traffic automatically is routed around the failure. This system maximizes the likelihood that Comcast's broadband network continues to function and customers can continue to be able to use their HSI service even when multiple failures might occur.

Comcast has designed its entire broadband network -- from the backbone to the home -- to minimize failures and the places such failures can occur; it has done so largely by building into the network significant redundancy. That said, as in any network, there inevitably exist single points of failure for which redundancy is impractical. In Comcast's broadband network, the primary single point of failure that might be considered "major" is at Comcast's CMTSes.[15] Because the CMTS is the aggregation point for traffic to and from Optical Nodes, a CMTS failure will affect the traffic for the Optical Nodes it serves and the customers served by those Optical Nodes.

To protect against such failures, however, Comcast employs a rigorous monitoring, testing, and replacement schedule for network equipment such as its CMTSes. Comcast regularly tests its CMTSes and monitors their performance for any indication of potential failure. Over the last 18-24 months, the CMTSes that serve about 81 percent of the network have been replaced or upgraded as part of the transition to DOCSIS 3.0. To prevent failures within a CMTS, each CMTS has multiple cards and ports that can serve as back-ups to one another. So,

---

[15] *See Notice* ¶ 10 (seeking comment on "the major single points of failure in broadband architecture (for example, edge router, gateway router, transport links, cell sites, and VoIP servers"). Failures can also be experienced: (1) between a CMTS and an Optical Node it serves, e.g., a fiber cut, which would affect all the customers served by that Optical Node, typically a few hundred customers; (2) at an Optical Node, which would affect potentially all the customers served by that Optical Node; or (3) between the Optical Node and customers' cable modems, which would only affect certain customers. These potential failures, however, affect a decreasing number of customers and are easier to repair quickly.

if a single card or port fails on a CMTS, the customers served by that card or port can be moved to another to minimize any disruption.

In addition to its efforts to ensure sufficient redundancy and minimize single points of failure, Comcast implements extensive safeguards to protect against failures in its broadband network. For example, Comcast's facilities that house broadband network elements are built to best-in-class standards and are designed to withstand extreme environmental conditions such as floods, hurricanes, and snowstorms. Moreover, in the case of power loss to the facilities, Comcast has installed back-up power and, in many cases, additional back-up generators to ensure that its broadband network remains operational. With respect to access to these facilities, Comcast does not publicly disclose the location for most of its facilities, and Comcast establishes and enforces stringent access controls and identification procedures for all personnel seeking access to Comcast's broadband network infrastructure. Comcast's practices with respect to physical security are consistent with the "best practices" specified by the Network Reliability and Interoperability Council.[16]

B. Comcast's Broadband Network Has Redundant Facilities and Links That Ensure the Ongoing Reliability of Comcast's Services.

The *Notice* recognizes that "[r]edundancy is used in communications networks to improve survivability."[17] But the *Notice* states "concern[] that the level of redundancy and the effectiveness of that redundancy in routing around failures may be inadequate in broadband

---

[16] *See* Network Reliability & Interoperability Council, NRIC Best Practices Selector Tool, http://www.bell-labs.com/user/krauscher/nric/ (last visited June 21, 2010).

[17] *Notice* ¶ 13.

communications networks."[18] As demonstrated above, however, Comcast's network has significant redundancy and reserve capacity built into its infrastructure. Moreover, Comcast has built in safeguards to ensure that, when failures do occur, they are resolved quickly.

In addition to typically having each CMTS dual-homed to routers in the regional network, the routers in the regional network interconnected to other regional routers, and the regional routers dual-homed to the backbone, Comcast actively monitors the health of all its routers and links and takes proactive preemptive action as necessary. Comcast has a variety of tools that monitor the broadband network and report "link down" events. Topology events, such as an outage in a particular geographic area, are also monitored and reported. Both activities are ticketed and reacted to promptly by network operations personnel 24 hours a day, 7 days a week, 365 days a year.

If a failure occurs at any point in the network, the routing systems are designed to converge automatically to minimize downtime. When failures do occur, typically the link going down will trigger a routing update and within one second the traffic will have found a new path to the destination. In rare cases, a link may fail without triggering a "link down" event. When that happens, it typically will take the broadband network approximately six seconds to recognize the failure on its own and route around the failed link.

In addition to the redundancies built into the broadband network, Comcast has established multi-site redundancy for key features of the HSI service such as the Domain Name System ("DNS") service look-up and routing and Dynamic Host Configuration Protocol ("DHCP") IP address assignment. These key features that Comcast offers as part of the HSI

---

[18] *Id.*

service are hosted in regional Application Points of Presence ("APOPs"), which are essentially regional data centers. The HSI service is configured in such a way that, should a customer lose her primary APOP for DHCP, DNS, device provisioning, and other key aspects of the HSI service, those features will fail over to a secondary data center to maintain the quality of the HSI service.

Other features and services that are part of Comcast's HSI service also have reserve capacity to handle major site or facility failures. For example, the Comcast e-mail system is hosted in two National Datacenters. If a disaster affected one of those sites, the second site has sufficient capacity to handle 100 percent of our customers' e-mail.

The *Notice* states that the Commission is "concerned that the level of redundancy and the effectiveness of that redundancy in routing around failures may be inadequate in broadband communications networks."[19] Fiber and wire cuts, downed links, malfunctioning routers and switches, and similar network segment disruptions are events that any network operator must deal with in the normal course of business. Comcast's key broadband network segments are designed to route around such failures; that design is tested periodically, both as part of regular procedures for monitoring the network and, from time to time, when such events actually occur and affect the network. Comcast's experience thus far has been that these events are essentially non-occurrences with respect to the proper functioning of the network, a testament to the validity of our broadband network design and to the equipment that we utilize.

Only in a very few rural markets have Comcast's traditional broadband network design and reliability safeguards not been implemented. For example, in order to deploy its broadband

---

[19] *Id.*.

network to Farmington, NM, Comcast had to obtain the right to lay fiber across Native American lands and only was permitted to lay one cable. In markets like Farmington, therefore, were Comcast to suffer a fiber cut on its fiber link to the backbone, Internet traffic would be stranded until the fiber cut was fixed. Of course, disruption of service in these areas is not a concern limited to broadband networks, but is a concern for telephone and electricity networks as well. Fortunately, given Comcast's network monitoring technology and because this would be considered a "hard down condition," it would be an immediate priority for repair, and service would be restored as quickly as possible.

C. Comcast Provisions Bandwidth To Account for Potentially Severe Traffic Loads in Order To Prevent Any Traffic Spike from Crippling the Network.

Historic usage patterns demonstrate that traffic on broadband networks is fairly bursty in nature, with certain times of the day seeing usage peak and other times seeing usage bottom. Given this pattern, Comcast provisions bandwidth and resources in a manner designed to offset a number of variables that can impact our customers' experiences, including severe traffic loads and surges that could otherwise cripple the network.[20] In fact, Comcast's broadband networks (especially the regional and backbone networks that do not have congestion management systems similar to the FairShare system Comcast has in place to manage congestion on the local portion) are designed to handle peak loads. To do so, among other things, we split nodes, move

---

[20] The variables over which Comcast has *some* control that affect customers' Internet experiences include: the provisioned speeds the network is engineered to deliver; the bandwidth available for the HSI service; the behavior of our network during unexpected surges in Internet traffic and any resulting momentary congestion, and some of the resulting effects on customers; the presence of spam and viruses in e-mail destined to the Comcast.net e-mail domain; the transmission of spam from our network; and the mitigation of attacks on our network. Variables over which Comcast has *no* control include: the speed of the server at the other end of a download or upload; the end user's software settings; the performance capabilities, configuration, and environmental factors of customers' home network and end devices; the presence of viruses and malware on customers' devices or on servers customers connect to; and whether congestion occurs between Comcast's network and the network of the end servers to which customers may be connecting.

fiber deeper into the network, deploy improved processing technologies (e.g., transitioning from DOCSIS 2.0 to DOCSIS 3.0), add capacity in the regional and backbone networks, and reallocate capacity as needed.

In assessing whether additional capacity is needed for the HSI service in any particular area, Comcast considers, among other things, the bandwidth currently available, how many channels are dedicated to HSI, the traffic trends (e.g., whether high consumption in an area is consistent or an anomaly), and the size of the service groups (i.e., the number of cable modems or other customer premises equipment sharing a port). Often, the most expedient and efficient means to increase the overall bandwidth available to customers in an area is to reduce the number of customers sharing that bandwidth, for example by splitting the node. Splitting nodes results in the reduction of the statistical multiplexing, or sharing, of the bandwidth dedicated to the HSI service, and ensures that Comcast continues to provision an acceptable level of bandwidth on a per-subscriber basis, based on customer data usage trends.[21]

As described above, Comcast's regional and backbone networks have been built with sufficient capacity to handle significant increases in usage for years to come, and additional capacity can be added as necessary. Comcast makes adjustments to its regional and backbone networks based on consideration of variables similar to those examined for splitting nodes, but at a more macro level. Specifically, we monitor regional, backbone, and other network segment utilization in order to ensure that there is sufficient capacity to handle traffic peaks and traffic growth. Comcast uses various tools, including some off-the-shelf software tools, as well as highly customized software tools, to enable it to monitor network utilization and adjust routing

---

[21] Splitting nodes also reduces the number of customers that could be impacted if a failure was experienced in an Optical Node.

tables and other configurations as necessary to minimize congestion on any particular link in the broadband network. Comcast uses time-tested measurements and processes to add capacity when usage is trending higher.

III. REAL-WORLD EXPERIENCES CONFIRM THE RELIABILITY AND SURVIVABILITY OF COMCAST'S BROADBAND NETWORK.

The Commission has expressed concern that pandemics or bioterror attacks could shift large amounts of traffic to residential broadband networks, and that the resulting congestion could threaten the orderly functioning of the economy and prevent access to critical public safety services.[22] Fortunately, incidents such as pandemics and bioterror attacks are few and far between. Comcast does, however, have real-world experience with the issues that concern the Commission because similar events that damage networks or shift large amounts of traffic to residential broadband networks are not uncommon and occur occasionally throughout the country. For example, in the last six months, Comcast has dealt with at least two major weather events that posed challenges to broadband network survivability and reliability. In both the winter-weather incidents in the Mid-Atlantic and Northeastern United States and the flooding in Nashville this past spring, Comcast's broadband network proved to be resilient and reliable.

When the Washington, DC metropolitan area effectively was shut down due to snow this past January and February, Comcast's broadband network remained operational and our customers in the region were able to telecommute despite increases in network traffic. Comcast's broadband network and customers in Philadelphia and Boston similarly were

---

[22] *See Notice* ¶ 15.

unaffected. In fact, during that time period, our customer care call centers showed no noticeable increase in calls related to service outages.

When Nashville was flooded this past spring, Comcast's facilities proved resilient and largely were not affected, although Comcast was prepared to act. Comcast's broadband network continued to deliver all of Comcast's services. Action plans in the event that Comcast's facilities had been affected included steps to migrate critical services to other diverse locations.

In short, pandemic-like events for broadband networks are not as infrequent as some might think, but they pass with little notice because the safeguards that many broadband network operators such as Comcast have implemented are designed to handle such events. Notably, Comcast's broadband network design and safeguards are not the result of government mandates, but have been guided by Comcast's engineers and the principles developed in collaboration with the Internet community with an eye towards ensuring that customers continue to receive high-quality service with as little interruption as possible.

IV. GIVEN THE DYNAMIC NATURE OF BROADBAND NETWORKS AND THE DIVERSE MEANS TO CORRECT PROBLEMS, THE COMMISSION SHOULD REFRAIN FROM MANDATING SOLUTIONS FOR POTENTIAL PROBLEMS.

The Internet has often been described as a "*network* of *networks* that consists of millions of private, public, academic, business, and government networks,"[23] "each with its own rules."[24] Since the Internet's first days, individual network operators decided for themselves what steps to take to ensure the resiliency and reliability of their own network infrastructure. This is eminently

---

[23] Internet, http://en.wikipedia.org/wiki/Internet (last visited June 21, 2010).

[24] Robin Anderson & Andy Johnston, *Unix Unleashed* 220 (2002); *see Netscape Communications Corp. v. Valueclick, Inc.*, 684 F. Supp. 2d 678, 696-97 (E.D. Va. 2009) (discussing "the undisputed proposition that the Internet is a 'network of networks,' comprised of a veritable panoply of servers and indeed over a billion Internet users").

sensible, in light of the fact that different networks necessarily face different threats and risks, and has been to the benefit of consumers and the public interest. Network operators have addressed survivability and reliability concerns in a large variety of ways, and this has fostered experimentation, innovation, and, ultimately, improvements in the design of the broadband networks that comprise the Internet.

Two core design principles of the Internet, as a packet-based network that uses a distributed directory service (the DNS), are that the network has multiple points of interconnection and that routing and naming resources are widely distributed. As such, these core design principles of the Internet themselves help sustain the survivability and reliability of Comcast's broadband network and other parts of the Internet.

In addition, Internet community technical bodies have analyzed and adopted best practices to provide guidance for network operators on how to ensure the reliability and survivability of the Internet. Numerous groups ranging from the NANOG to the IETF to the ISOC have all played key roles in the continued experimentation, innovation, and improvements of the Internet. They are tried and true and have sustained the growth of the Internet successfully for many years. In short, the industry's collaboration with the Internet community has worked well to establish and implement standards that reflect the common interest in assuring interoperability, reliability, and survivability of broadband networks and the Internet.

The Commission can play a constructive role in this space by working with these groups, broadband network operators, other members of the Internet community, and other stakeholders to continue to improve industry best practices. In fact, many of these organizations already issue documents on best practices, such as the "Best Current Practice" series of Request for Comment (RFC) documents from the IETF. The Commission already has chartered such a collaborative

group focused on public safety, CSRIC, to "[r]ecommend[] best practices and actions the Commission can take to ensure the security, reliability, operability, and interoperability of public safety communications systems" and "best practices and actions the Commission can take to improve the reliability and resiliency of communications infrastructure."[25] Working collaboratively with broadband network operators and others in the Internet community, as well as groups similar to CSRIC or the recently launched BITAG, the Commission can ensure that the myriad of broadband network designs and reliability and resiliency safeguards that are implemented are consistent with those practices.

---

[25] Public Notice, FCC, *FCC Announces Membership of the Communications Security, Reliability, and Interoperability Council (CSRIC)* (Oct. 26, 2009), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-09-2297A1.pdf.

V. CONCLUSION

For as long as there has been an Internet, the operators of the broadband networks that are part of the Internet have taken responsibility for ensuring that their networks deliver the service that consumers need and demand. The survivability and reliability of broadband networks and the Internet long has been entrusted to each network operator, in collaboration with broad-based third-party technical groups such as IETF, ISOC, NANOG, ICANN, and MAAWG, and the result has been the development of remarkably resilient and reliable packet-switched broadband networks that have many built-in redundancies and few major single points of failure. The Commission should ensure that these kinds of inclusive and broad-based technical groups continue to play the important role they have thus far in maintaining a well-functioning Internet.

Respectfully submitted,

/s/ Kathryn A. Zachem

Kathryn A. Zachem
Mary P. McManus
David M. Don
COMCAST CORPORATION
2001 Pennsylvania Ave., NW Suite 500
Washington, DC 20006
(202) 379-7134

Brian A. Rankin
COMCAST CABLE
COMMUNICATIONS, LLC
One Comcast Center
1701 John F. Kennedy Boulevard
Philadelphia, PA 19103-2838

James L. Casserly
Ryan G. Wallach
Daniel K. Alvarez
WILLKIE FARR & GALLAGHER LLP
1875 K Street, N.W.
Washington, DC 20006

Attorneys for Comcast Corporation

June 25, 2010