CableLabs®

The leading innovation and R&D lab for the global cable industry

November 21, 2019

Re: Public consultation on draft BEREC Guidelines on common approaches to the identification of the network termination point in different network topologies ["NTP Guidelines", BOR (19) 181]

CableLabs, the research and innovation consortium of the global cable communications industry, hereby provides technical input to the above-referenced BEREC consultation. CableLabs' membership includes 16 European cable operators, as well as operators in North America, Asia, and Latin America, representing 180 million subscribers and 500 million individual users in total.[1] CableLabs works to develop the future of cable broadband network technologies, which cable operators then deploy to serve customers with ever-increasing levels of performance.

As we detail further below, regulators' definition of the appropriate network termination point must be informed by the technological realities of cable networks. The specifications developed by CableLabs, and adopted as standards by the Society of Cable Telecommunications Engineers (SCTE), the European Telecommunications Standards Institute (ETSI), and the International Telecommunication Union (ITU), are utilized by our members in Europe and across the globe to enable market-leading performance and security in the provision of broadband service. These specifications rely on equipment that often resides on consumer premises, such as a modem, router, or set-top box. These devices are managed by operators in order to provide service to end-users in accordance with cable standards and are certified by CableLabs for this purpose. National regulatory authorities must preserve operators' ability to qualify, deploy, operate and manage these devices in order to maintain and advance the performance and security of cable networks. The success of the cable industry's innovation model, of which network endpoints are integral, is evident in the modern role of broadband as a critical enabler of economies and societies.

Contact: Rob Alderfer, Vice President of Technology Policy
r.alderfer@cablelabs.com

[1] CableLabs, *About CableLabs*, available at: https://www.cablelabs.com/about-cablelabs

Table of Contents

1) Introduction

CableLabs, the research, development, and innovation arm of the global cable industry, hereby provides input to BEREC as it considers guidelines to define the network termination point (NTP). As we will describe, an operator's management of network endpoints is critical to ensuring consistent high-performing services, as well as the security of those services and the data carried over cable broadband networks.

Cable network specifications developed and published by CableLabs, with the participation of cable operators and technology manufacturers, which are then standardized by the Society of Cable Telecommunications Engineers (SCTE), the European Telecommunications Standards Institute (ETSI), and the International Telecommunication Union (ITU), provide the basis of cable-based services around the world. Operators ensure adherence to these specifications by qualifying, deploying, operating, and managing network equipment. Key elements of this equipment reside on the premises of end-users. Adherence to these standards, including through qualification and deployment of certified devices, is central to the network innovation model of the cable industry, which is centered around CableLabs.[2] Through our work with cable operators and technology manufacturers, cable network performance has grown substantially, and consistent security and data protection practices are enabled. The success of this model is evident in the blooming of broadband Internet access into an engine that powers modern economies and societies.

In this contribution, we first describe the architecture of cable networks. We then describe the how network endpoints are integral to the performance and security of cable broadband service. We also outline CableLabs' certification program, which ensures that network devices conform to CableLabs' specifications. We observe how these practices are conducive to innovation. Finally, we conclude with specific reflections on how these technological realities should influence the present consultation, and we outline why one particular option articulated by BEREC ('Option C') is most conducive to continued advancement in cable broadband performance and is essential to network security.

2) Cable Network Overview

Since the early 1990s, cable operators have employed hybrid fiber-coaxial (HFC) networks to initially deliver television signals, and later broadband and voice services. An HFC network is comprised of a fiber portion which connects a "headend" or regional hub to optical nodes. Within the headend or regional hub, the cable modem termination system (CMTS) creates the broadband signal - known as Data over Cable Service Interface Specification, or DOCSIS - which is then transmitted over fiber to the optical nodes. The number of homes passed per node continues to decrease as cable operators continue to extend fiber closer to the subscriber, increasing the overall capacity available to each subscriber.

In the optical node, the DOCSIS broadband signal is transformed from an optical signal to a radio frequency (RF) signal for transmission over the coaxial network to subscriber homes. In the coaxial portion of the HFC network, one or more amplifiers may be used to extend the

[2] CableLabs, through its wholly-owned subsidiary, Kyrio, performs certification testing of cable network devices to ensure compliance with the CableLabs specifications, and cable operators globally rely on this certification.

reach of the RF signal. Subscribers connected via coaxial cable to the same optical node port are typically referred to as a service group, and those subscribers necessarily share the total broadband capacity provided to that coaxial segment. Each optical node may support more than one service group. The RF signal is then terminated in the subscriber's home at a cable modem, which often includes an integrated Wi-Fi access point and embedded Multimedia Terminal Adapter (eMTA) for wireline Voice Over IP (VoIP) telephony services. The Wi-Fi access point enables users to attach a diverse range of devices to their network; the eMTA connects telephone devices.

The cable modem resides at the consumer premise and is an integral network element in the provision of cable broadband services. It communicates with the CMTS using the standardized DOCSIS protocols to enable the provision of broadband service over the shared HFC network.

3) Network Endpoints Are Essential to Cable Network Performance

Since 1997 and the launch of the original DOCSIS specification, the cable industry has steadily increased the performance capabilities of cable broadband service. As summarized in the table below, DOCSIS technology has realized major advances with each iteration.

The Evolution of DOCSIS

	DOCSIS 1.0	DOCSIS 1.1	DOCSIS 2.0	DOCSIS 3.0	DOCSIS 3.1	DOCSIS 4.0
Highlights	Initial cable broadband technology	Added voice over IP service	Higher upstream speed	Greatly enhanced capacity	Capacity and efficiency progression	**Symmetrical streaming and increased upload speeds**
Max Downstream Capacity	40 Mbps	40 Mbps	40 Mbps	1 Gbps	10 Gbps	**10 Gbps**
Max Upstream Capacity	10 Mbps	10 Mbps	30 Mbps	100 Mbps	1-2 Gbps	**10 Gbps**
Initial Specification Date	1997	1999	2001	2006	2013	**2019**

Cable Broadband Advancement Through Generations of Technology

Today, the cable industry is widely deploying the latest commercially available cable broadband technology, known as DOCSIS 3.1, that can provide up to 10 Gbps of downstream capacity and readily support gigabit-speed broadband services. Moreover, the next technology enhancement – DOCSIS 4.0 – will enable symmetric (upstream and down) gigabit services and is nearing commercial availability.

Each modem must decode and transmit DOCSIS signaling in order to support broadband service. The improvement in performance in successive generations of DOCSIS is enabled by a range of factors, which are dependent in significant part on advancements within the modem. These include increased spectral efficiency, more advanced error correction, and

greater channel bandwidth. Cable modems must incorporate the necessary technical features in order for users to benefit from these advancements. For that reason, operators deploy new modems in a methodical fashion in coordination with the upgrade of other network elements to support the provision of the latest cable broadband services.

Many modems in use today also integrate a Wi-Fi router. Though Wi-Fi signaling is distinct from DOCSIS, similar advancements in Wi-Fi technology – grater spectral efficiency and wider channel bandwidth, among other things, leading to higher speeds – complement the evolution of DOCSIS. As new DOCSIS modems are provisioned, operators will also incorporate the latest Wi-Fi technology so that consumers can experience the full benefit of network upgrades. Furthermore, integration of Wi-Fi technology into cable modem gateways enables operators to proactively maintain end-user Wi-Fi access points to ensure a high quality of service and security. These benefits can also be achieved through standalone modems and routers that are both managed by network operators. Advanced network maintenance techniques developed by CableLabs are used by operators to proactively remediate service quality issues; the use of these techniques is reliant on qualified, managed modems and routers that meet modern specifications.

4) Network Endpoints Are Essential to Cable Network Security

Cable operators have long incorporated security to protect the delivery of cable services. From the earliest days, cable operators have faced attackers seeking to steal video service, customer data, and video content. With broadband Internet access service, cable operators face new attacks based on a very different threat landscape and attack vectors.

A cable operator runs a single physical network with multiple distinct and separate logical networks. We focus in this section on two of those logical networks: One is the network for traditional cable video delivery (e.g., digital broadcast television, that is, video delivered over the cable network, but not over the broadband Internet access connection). The other network is for the provision of broadband Internet access service. In each, network endpoints that reside on consumer premises are integral to the provision of service.

a) Securing Video Service

While cable operators provide video and broadband services over the same medium, video and broadband data are transmitted over separate channels (or frequencies) and the encoding of the video and broadband are different and not interchangeable, inherently adding a layer of protection to each service from intrusion by the other.

Cable operators use a conditional access system (CAS) to provide security for the delivery of video content from the headend to the set top box that resides in homes. In Europe, cable operators use a system based on the Digital Video Broadcasting (DVB) standards, SimulCrypt and MultiCrpyt. DVB CAS contains three essential physical elements: (i) broadcast equipment at the headend that encrypts (scrambles) and transmits video to the set top box, (ii) set-top boxes that receive signals and transmit them to a security module (typically dedicated tamper resistant hardware) within the box, and (iii) the security module that determines if the set top box is authorized to receive the video and decrypts accordingly. Content providers typically have content protection requirements they place on their

distributors, including cable operators. Operators must therefore deploy qualified set-top boxes in order to deliver video services and must regularly maintain and update them.

As the nature of video service continues to evolve, so have the necessary security features. Video content delivered over the Internet ("Over-the-Top" or "OTT" video) is secured using digital rights management (DRM) systems. DRM systems were originally adopted by Over the Top (OTT) video providers and more recently by cable operators to deliver cable-provided video content to Internet-connected retail devices. Current generation cable set top boxes are designed to receive and render video signals received both from traditional cable video delivery services and from OTT sources delivered over the Internet by third-party providers. In this way, cable operators integrate online video sources into the set-top boxes that they manage. These delivery architectures and new innovations all rely on operator-managed devices that reside on customer premises.

b) Securing Broadband Service

Building on the industry's experience in securing video service delivery, cable operators have long recognized that security of the network is critical to the provision of broadband Internet access service. From the start, the cable industry has incorporated into its broadband service security by design as expressed through the core tenets of information security – confidentiality, integrity, and availability. These principles also enable data protection for information that traverses the cable network.

The DOCSIS cable broadband specification includes security protections that ensure the confidentiality, integrity, and availability of broadband service in the access network. Security was a significant consideration in the very first version of the DOCSIS specifications and has been improved with each successive version of the specifications. This security focus is driven, in part, because accessing the Internet on a DOCSIS network requires that cable subscribers make use of the shared HFC medium. Each subscriber's Internet traffic is transmitted over a common hybrid-fiber coaxial cable that also carries the Internet traffic of a group of other subscribers in the same neighborhood. Therefore, the initial DOCSIS specification had to include security in its design to prevent hackers from eavesdropping on subscriber Internet traffic between the cable modem and the CMTS. Today, a variety of advanced techniques are utilized to secure cable broadband networks and protect the data that traverses those networks.

DOCSIS security in the cable modem is defined and implemented through a combination of hardware and software requirements. Both the hardware and software elements are critical to network security, and the integrity of both the cable modem hardware and software must be maintained for this reason. The following sections cover the relevant aspects of the DOCSIS security specifications, which cover cable modems.

i. Encrypted Communications

The first DOCSIS specifications addressed security through the Baseline Privacy Interface (BPI). BPI provides a fundamental level of protection for all devices that attach to the cable modem network. BPI prevents a user from passively listening to others' traffic on the shared cable network. In short, BPI encrypts all traffic flows between each cable modem and the

CMTS to ensure those transmissions remain confidential. Stronger encryption algorithms have been specified as appropriate in the DOCSIS specifications. With DOCSIS 3.1, a cable operator can now encrypt communications using 2048 RSA encryption, a very strong security standard that is further detailed below.

ii. Secure Device Authentication

Along with encryption algorithms, DOCSIS network security has improved over time using ever-stronger digital keys. In 2000, a Public Key Infrastructure (PKI) was adopted in the DOCSIS 1.1 specification. Cable's PKI, which is managed by CableLabs' subsidiary, Kyrio, provides the same type of device authentication (protecting against rogue devices) and data encryption that is used by banks and the military. Cable's PKI security allows a cable operator to authenticate cable modems on their network, permitting a cable modem to access the CMTS, thereby allowing access to the cable operator's network and the Internet, and disallowing a modem to access the network in the event of a security breach. The cable PKI provides a unique, immutable, and attestable digital identity to each and every cable modem and CMTS on the cable plant at the time of manufacture. These digital identities, known as digital certificates, bind to the device and serve to authenticate its identity in a manner that is extremely difficult to spoof. The security benefits of PKI are not limited to cable technology. CableLabs, through Kyrio, has issued over 500 million digital certificates, many in sectors beyond cable, making cable's PKI one of the largest PKIs in the world.

A PKI is only as secure as its implementation and that is in part a function of the care taken to provide certificates only to trusted organizations. The digital certificate identifies the modem, the manufacturer, the certificate version and issuer, and key validity dates. Cable modem and CMTS manufacturers only receive digital certificates to insert into their cable devices after verification and after the manufacturer has contractually agreed that it will safeguard the digital certificates and only use them in cable modems and CMTSs that are built in conformance with CableLabs' specifications. This ensures that the digital certificates are not put into insecure network devices or devices designed to harm the Internet. The manufacturer receives the digital certificates through a secure delivery mechanism. Digital certificates that are lost, stolen or otherwise compromised are revoked to prevent the affected device(s) from accessing the cable network.

iii. Secure Software Updates

The integrity of the cable modem software is protected through the use of digital certificates that ensure only software updates that come from the specific cable modem manufacturer via the cable operator can be downloaded into the cable modem. This protocol is standardized in DOCSIS, since software delivered through any other mechanism would expose cable networks to security abuse.

This high level of security provided by secure software download is achieved through special digital certificates, called "code verification certificates" or CVCs, which are provided to the manufacturer and the cable operator. A CVC digitally signs a software update so that the software update is both encrypted and identified with its source. A cable modem will only accept software updates that are signed with the appropriate CVC. Use of a CVC to secure software updates ensures that the source of the software is trusted and minimizes the risk

that a cable modem will be infected with malware or other malicious code as part of the software update process.

iv. Increasing Cryptographic Strength

Cable has continued to strengthen the implementation of its PKI. Cable modems and CMTSs built to the DOCSIS 3.1 specifications follow the cryptography guidelines of the U.S. National Institute of Standards and Technology (NIST) and use a 2048 RSA key for encryption. It is estimated that that it would take a current standard desktop computer more than 6 quadrillion years to crack a 2048 RSA encryption key.

v. Prevention of IP Address Spoofing

Cable operators have incorporated technology to prevent the use of spoofed Internet Protocol (IP) addresses. Every device on the Internet that routes traffic or directly terminates traffic receives a public IP address that serves such purposes as allowing the end-user to reach a web page and receive email. The cable operator assigns a public IP address to each device attached directly to its network (e.g., a router in a cable modem). Each packet sent from the device includes this unique source IP address. IP address spoofing occurs when someone creates a false IP address to conceal the identity of the device, to have a device impersonate another device, or pretend to be on a different ISP's network. While IP address spoofing has some legitimate uses, such as testing a website's performance, IP address spoofing is also used to conceal someone's identity when they are committing illegal acts, such as distributed denial of service (DDoS) attacks.

Cable operators are able to block outbound Internet traffic sent with a spoofed IP address at the CMTS. The CMTS checks IP packets sent from the customer premise equipment to ensure that the source IP address on the packets matches the source IP address assigned by the CMTS. If the addresses do not match, then the CMTS discards the packet. The incorporated anti-spoofing measures are very similar in substance and method to the Internet Engineering Task Force (IETF) standards for anti-spoofing.

vi. Protections Against Cloned Cable Modems

The cable industry continues to deploy increased security features to combat the issue of cloned modems. A cloned modem is used to steal broadband service and is also used to hide criminal activity on the Internet. Cloned modems occur when one modem presents itself on the cable network as a different modem. Every networked device has a network interface card (NIC) which assists in connecting the device to a network such as the Internet. It is the NIC that turns the data from your device into the electronic signals that pass over the cable network and become packets on the Internet. The NIC has a media access control (MAC) address that is hardcoded into the NIC during the manufacturing process. While an IP address is used to locate a device on a network, much like a building has a street address, the MAC address identifies the NIC. Each NIC's MAC address is a unique 48-bit hexadecimal address. This unique 48-bit address translates into 281 quadrillion unique possible addresses; therefore, the likelihood of two modems with the same MAC address on the same network segment is extremely low.

Cable modem cloning occurs when the MAC address and other pertinent information are taken from one modem and used in another modem. The cloned modem would then be allowed on the cable network and would receive broadband service like the original modem. These attacks involve copying all or pertinent parts of one modem's firmware onto a different modem, requiring physical access to the modem as well as a high level of technical expertise. Specifically, to create a cloned modem it is necessary to physically modify it by first disassembling the enclosure, soldering wires to the circuit board, attaching it to a development system, modifying the modem software, and then performing a sideload attack to reflash the software in the modem. Because of the DOCSIS standards, this risk is limited in scale and scope.

The DOCSIS network has continued to evolve to provide increased security measures to minimize the risk of cable modem cloning. For example, these measures include preventing a cloned cable modem from downloading old files to further its impersonation, IP address verification, message integrity checks between the CMTS and the modem to ensure the integrity of files downloaded from the CMTS to the modem, and using digital certificates uniquely assigned to each modem.

5) CableLabs Certification Enables Network Performance, Security, and Interoperability

As discussed above, CableLabs has developed various specifications to facilitate the manufacture of interoperable and secure cable devices, including CMTSs, cable modems, set top boxes, and eMTAs. CableLabs also administers a test and certification program through its subsidiary, Kryio, to ensure conformance with these specifications and interoperable functionality with other CableLabs certified devices.

Following CableLabs / Kyrio testing of devices that seek qualification, certification decisions based on those test results are made by a Certification Board, which is comprised of technical representatives from cable operator companies. Operators make device qualification and deployment decisions based on this certification process because certification ensures a consistent level of performance, security, and interoperability for cable network devices, including those that reside at the user-end of the network. Furthermore, interoperable devices based on common specifications facilitate competition between device manufacturers, consumer choice, widespread deployment of new technologies, and lower costs to both cable operators and consumers.

6) Cable's Technology Development Model is Highly Conducive to Innovation

CableLabs' technology development model places an emphasis on joint technology development with cable operators and technology manufacturers, who participate in the development of specifications. Advances in these specifications over time, which continues today, has generated significant improvements in network performance and security. Testing, certification, and qualification ensures that cable network endpoints adhere to these ever-advancing cable standards.

These principles and practices are conducive to innovation in communications networks. Not only does this approach enable progress in network performance, but it also has fostered a dynamic and innovative broadband market.

Today's performance of cable broadband is well in excess of the requirements of online applications and has led to a flourishing ecosystem of Internet-connected devices. Cable broadband has become a catalyst for a broad range of digital innovation. The industry's development model, centered around CableLabs, allows cable operators to stay ahead of customer demand for broadband connectivity and to deliver other network services such as television and telephony.

A range of economic research, from McKinsey[3] to the ITU[4], has shown that the benefits of broadband underpin a large segment of nations' gross domestic product, employment, and consumer surplus. Growth is aided by broadband through the adoption of efficient business processes, the introduction of new online services, and the investment and labor directly involved in the deployment and operation of networks. Economic dynamism is enhanced as new firms gain access to global markets at low cost. And consumers benefit through increased choice and lower costs for goods and services.

There are also non-economic benefits of broadband: Access to information enables a more engaged body politic, new forms of expression for individuals, and human connection that can occur across vast geographies in real-time.

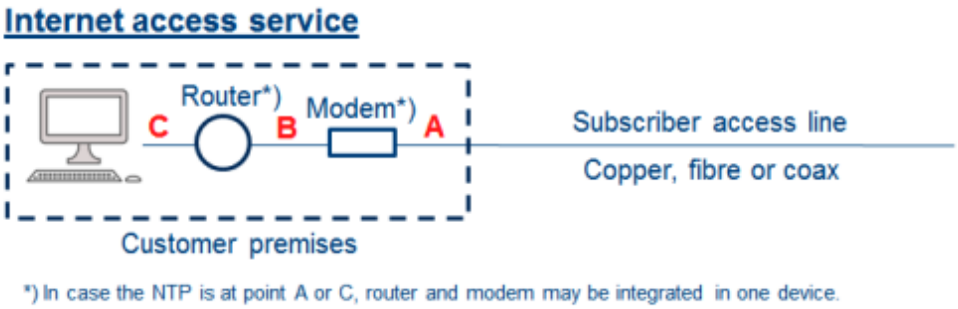
In short, broadband has become a transformative force that will continue to shape communications and society. Enabling this impact are the networks that make broadband Internet access possible. Integral elements of these networks are their endpoints, and it is imperative that operators qualify, deploy, operate and manage these devices in order to maintain the performance, security, and interoperability of cable networks. Doing so will enable a continuation of the network advances that have characterized the recent history of the Internet.

7) Implications for BEREC NTP Guidelines

In this contribution, we have outlined the importance of network endpoints to broadband and other cable network services. Regulators must account for these technological realities as they seek to define a Network Termination Point.

In the NTP Guidelines consultation, BEREC outlines three distinct options for defining the NTP, as shown in their Figure 2 below.[5]

[3] McKinsey Global Institute, "The great transformer: The impact of the Internet on economic growth and prosperity", October 2011.
[4] International Telecommunications Union, "The Impact of Broadband on the Economy: Research to Date and Policy Issues", April 2012.
[5] Public consultation on NTP Guidelines, at p.4, BEREC [BOR (19) 181].



Source: BEREC

Figure 2: Different locations of the fixed NTP in case of an internet access service

In distinguishing three distinct NTP options ('A', 'B', and 'C'), BEREC depicts an overly simplified, fixed view of network equipment. Nevertheless, among the options, Option C is most conducive to broadband network innovation and security.

a) 'Option A' Is Inconsistent with Technological Reality

As outlined in this contribution, the standardized incorporation of DOCSIS signaling into a cable modem is essential for the provision of secure cable broadband service. Cable networks clearly do not terminate on the network side of the modem; modems are a part of the network, and BEREC's Option A is inconsistent with technological reality.

BEREC recognizes that any use of Option A as the NTP requires end-users to take responsibility for the proper operation of modems, and for their ongoing security.[6] However, end users cannot reasonably be expected to ensure conformance with relevant network standards and for judging the adequacy and trust of security updates. In fact, this is why CableLabs conducts extensive certification testing, and why cable's DOCSIS standards require modem software updates to occur through the secure code verification certificates (CVCs) described in Section 4(b)(iii) of this response. Undermining this practice would not only make individual end-users more vulnerable to Internet security threats, it would also risk broader harms to the Internet as compromised devices are used in distributed denial of service (DDoS) attacks and other exploits.

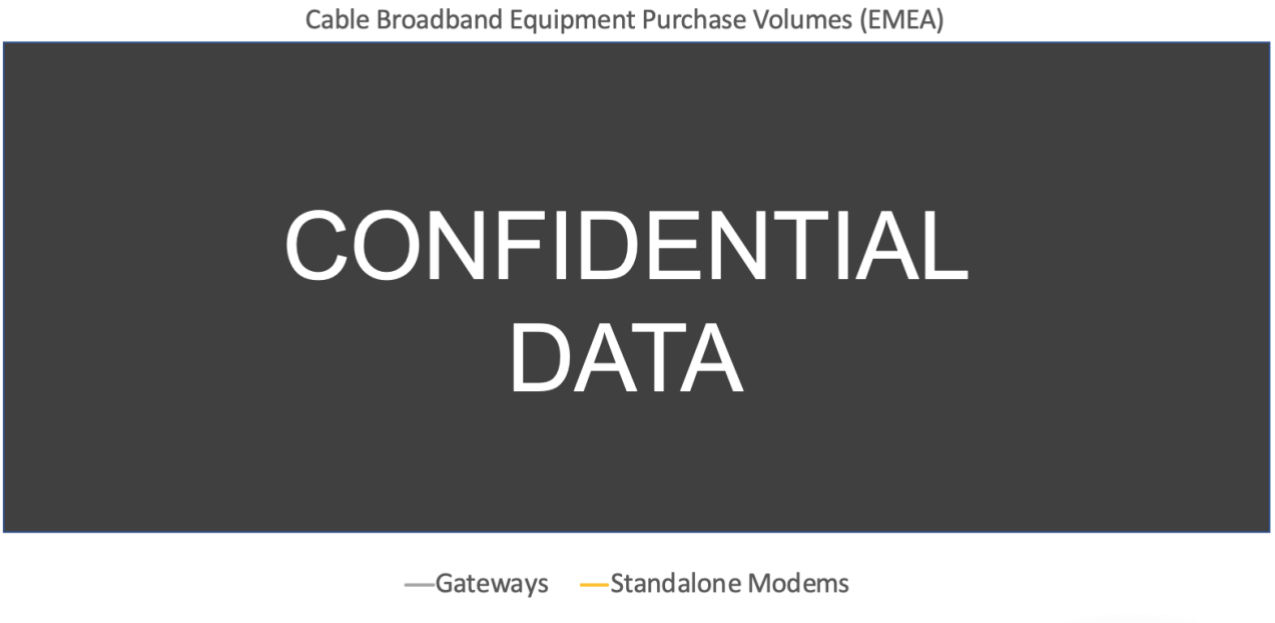
It is therefore apparent that the use of Option A as the NTP would undercut the operation of the network, network maintenance, and its upgrade over time, both in terms of performance and security. As we have described, the modem's proper place as part of the cable network is not detrimental to Internet application or device innovation. To the contrary, this reality has led to rapid expansion in the performance of networks. Broadband services have never been more integral to everyday life, and consumer choice of Internet applications and connected devices has never been more plentiful.

b) 'Option B' Runs Counter to Technology Trends

Option B may be a plausible NTP definition in some limited cases – primarily, for those end-users that do not utilize an integrated modem / router gateway, and instead utilize a router

[6] Public consultation on NTP Guidelines, at paras.70-75, 88-94, BEREC [BOR (19) 181].

that is not managed by a network operator. While we acknowledge that Wi-Fi signaling is distinct from DOCSIS, and this separation is technologically possible, BEREC must in turn acknowledge that the majority of users do in fact utilize integrated gateway devices that include both a modem and router. This is reflected in new equipment purchase volumes, shown in the chart below.



Integrated Modem/Router Gateways Are the Norm in European Cable[7]

Furthermore, as different physical and logical networks converge to offer advanced services to end-users, the motivation for integrated gateways and operator-managed routers becomes stronger. Gateways and managed routers enable consistent network performance through the incorporation of modern DOCSIS and Wi-Fi technologies, and also enable proactive maintenance of both media. The cable industry has been working to integrate Wi-Fi performance features and metrics into industry performance metrics in order to enable consistent quality of service.[8] The benefits of this network-administered gateways, modems and routers also extend to security. For instance, CableLabs is developing a technology known as Micronets, which will automatically provision user networks into subnets in order to protect the network and associated devices.[9] This security-focused innovation is facilitated by network-administered modems, routers, and gateways. Therefore, utilizing Option B as a static NTP definition risks these performance and security benefits, and may halt or slow developments that are highly beneficial for Internet users.

c) ‘Option C’ Is Consistent with Innovative Development

[7] [CONFIDENTIAL]
[8] See, for example, *Proactive Network Maintenance*, described here: https://www.cablelabs.com/technologies/proactive-network-maintenance
[9] https://www.cablelabs.com/technologies/micronets

Option C is therefore the NTP definition that best reflects the realities of cable network technology development and service provision. Enabling performance and security features to be integrated in both modem and router leads to more consistent and rapid advancement of network performance and security. These effects benefit the broader online ecosystem, as users on a large scale enjoy these benefits and enable a mass market for Internet-enabled applications, services, and devices.