RYSAVY RESEARCH

Declaration of Peter Rysavy

FCC: Safeguarding and Securing the Open Internet

December 7, 2023

Table of Contents

Introduction & Summary

1. This declaration responds to the FCC's Notice of Proposed Rulemaking (NPRM) on *Safeguarding and Securing the Open Internet*.[1] It builds off of a prior declaration prepared for the 2017 *Restoring Internet Freedom* NPRM that described key technical facts about internet service that are pertinent to the legal classification of broadband.[2] This declaration explains recent developments in the domain name system (DNS) and caching services provided by internet service providers (ISPs), as well as other new technologies implemented in the last decade, that even further enhance broadband's capabilities for generating, acquiring, storing, transforming, processing, retrieving, utilizing and making available information via telecommunications. It proceeds in three parts: Information Service Classification, Public Switched Network/Interconnected Service, and Evolving Mobile Networks and Differentiated Offerings. This introduction presents a view of how the internet has evolved and summarizes the topics covered in detail in this declaration.

2. The internet was originally conceived as enabling the robust delivery of packets between end points across multiple nodes, primarily using Transmission Control Protocol (TCP) and Internet Protocol (IP). Early applications included email using Simple Mail Transfer Protocol (SMTP) and File Transfer Protocol (FTP). Content locations were static, and routes between end points seldom varied. Over the decades, and particularly since 1990, innovation has flourished on the internet, resulting not only in a vast array of new applications, but a fundamental change in the nature of the internet itself. Internet service, which began as a communications offering with limited intelligence, has evolved into a highly intelligent platform that processes and transforms information in multiple ways and at multiple nodes to both enhance the user experience and enable applications that would not otherwise be possible. Some key elements in this near-constant transformation are how ISPs and other nodes adapt, process, and optimize user content and how ISPs and other nodes dynamically optimize delivery paths for speed and efficiency. Further, content that used to be one location is now widely distributed, including within ISP networks, so much so that new internet architectures under investigation, such as Information Centric Networking (ICN) and Named Data Networking (NDN), do not rely on routing based on IP addresses but instead focus retrieval based on the content desired.[3] The

[1] FCC, *Safeguarding and Securing the Open Internet, Notice of Proposed Rulemaking – WC Docket No. 23-320*, Sep. 28, 2023. https://docs.fcc.gov/public/attachments/DOC-397309A1.pdf.

[2] Declaration of Peter Rysavy, (July 17, 2017), https://api.ctia.org/docs/default-source/fcc-filings/exhibit-a-rysavy-declaration-c1.pdf.

[3] IETF, Information-Centric Networking, https://datatracker.ietf.org/rg/icnrg/about/. Named Data Networking, https://named-data.net/.

IETF states, “Data becomes independent from location, application, storage, and means of transportation, enabling in-network caching and replication.” Note that the National Institute of Standards and Technology (NIST) is participating in this effort.

3. Subscribers of broadband internet access service make use of a variety of applications over their broadband connections, including social networking, instant messaging, email, web browsing, and video streaming, all of which offer some combination of generating, acquiring, storing, transforming, processing, retrieving, utilizing, and making information available—the characteristics of an information service.

4. Furthermore, this information is not static. It is processed and often altered at multiple points by the ISP, in the transmission of the information (*i.e.,* in parts of the path over which packets are routed), by third parties, and by content providers. Transmission of data has become intertwined with other services that provide value to users. The very transmission of data in the internet involves processing of information, in some cases transforming packets. Differentiated services, network address translation, proxy, firewalls, security functions, congestion mitigation, and IPv4-to-IPv6 integration are all examples. Another important function ISPs provide is caching (either themselves or through arrangements with third parties), which stores information and provides local retrieval, improving the user experience.

5. ISPs’ offerings can include multiple other services that store, transform, process, and retrieve information, including opt-in filtering for family safety, video optimization, and security functions.

6. All of these capabilities differentiate the internet from the Public Switched Telephone Network (PSTN). The two networks use dramatically different protocols, different architectures, different approaches in switching (packet versus circuit), different nodes within the networks, and they provide very different capabilities.

7. The popularity of IP-based services such as video streaming has contributed to the explosion in the amount of data traveling through the mobile broadband network, which can experience congestion to a greater and more sudden degree than other networks. To meet user expectations, video optimization, active queue management, and other traffic management functions are essential. Furthermore, with 5G, quality of service (QoS) mechanisms play a crucial role for mission-critical applications such as advanced industry automation, telemedicine, and drone control, all of which require intelligent traffic management. Another fundamental capability of 5G is Multi-access Edge Computing (MEC), which further intensifies information processing within the network, enabling applications such as augmented reality (AR) and distributed AI processing.

8. All of the above leads to the inescapable conclusion that broadband internet access service is dynamic and evolving and provides far more than mere transmission. Mobile broadband is not an element of the PSTN, and mobile broadband will increasingly offer differentiated capabilities that enable QoS enhancements for emerging services and applications.

Broadband Internet Access Service Involves Many Elements of Information Service

"Core" Broadband Internet Access Functionalities Are Information Services and Not Mere "Network Management"

9. The NPRM proposes to classify broadband internet access service as a telecommunications service like that provided over the PTSN. The NPRM, for example at ¶ 11 and ¶¶ 72-76, takes the general stance that internet access is a transmission technology implemented by TCP/IP protocols. The NPRM classifies any other related capability as either a network management function (*e.g.*, DNS, caching), or a separable service (*e.g.,* email). Users, however, do not subscribe to internet service with the mindset of sending packets to an IP address. Users want to engage with the world in multiple ways, such as driving with turn-by-turn navigation or streaming a new show. The functionalities described in this section enable this form of engagement because they allow ISPs to offer consumers the capabilities to manipulate information in a manner that contributes to what consumers value and seek out when they subscribe to a broadband internet access service. These offerings do not facilitate use of the network without changing the nature of the basic transmission, but rather add functionality that enhances the consumer's experience, expanding the network's capabilities beyond the mere transmission of data from one point to another.

<u>Routing</u>

10. The routing of Internet Protocol (IP) packets alone involves examination and processing of the packet at every router the packet traverses, including the routers managed by the ISP. Such examination and processing by the ISP is necessary to know which route to use *and* to implement policies, such as integrated or differentiated services. This information processing is inextricably intertwined with the transmission itself. For example, Cisco notes three separate processes for routing, including implementing routing protocols, maintaining the routing table, and the forwarding process.[4] These routers are not just located in the core of the internet but

[4] Cisco, "Configure Route Selection for Routers," Nov. 2022. https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8651-21.html (viewed Oct. 23, 2023).

are used by ISPs to communicate information to and from subscribers, to the internet, and to information servers they may provide, such as web servers, DNS servers, and email servers. Routing functions are integrated into current generation network equipment that is the next hop from an end user, connecting by a consumer-owned 5G wireless router,[5] fiber, a cable modem, or Digital Subscriber Line (DSL). Most home network equipment installed by ISPs also has routing, packet processing, and network address translation functions.

11. Internet routing is not merely transmission, because routing offers services beyond simply getting packets from one node to another. For example, the router may also enforce different policies, such as QoS, implemented through protocols such as Differentiated Services. The Internet Engineering Task Force's (IETF's) specification for Differentiated Services states: "This architecture is composed of a number of functional elements implemented in network nodes, including a small set of per-hop forwarding behaviors, packet classification functions, and traffic conditioning functions including metering, marking, shaping, and policing."[6] 5G wireless operators also implement QoS mechanisms for traffic differentiation. By way of example, the unlimited data service plans offered by some operators may deprioritize traffic for users that have exceeded a defined amount of data in circumstances involving network congestion.[7] This technique allows all subscribers to enjoy the benefits of the unlimited data plan; furthermore, subscribers are not adversely affected by users whose consumption of data could exceed the capacity of the cell. Providing users such additional value transcends network management. ISPs also provide a reliable and consistent customer experience by using methods such as Random Early Detection (RED) and Active Queue Management (AQM),[8] which selectively drop packets, forcing TCP transmitters to reduce the packet transmission rate. Analyzing traffic flows, implementing traffic policies, and acting upon the traffic flows involves acquiring, processing, and transforming information (for example, reordering or dropping packets). This functionality does more than facilitate mere transmission: Customers receive additional capabilities. In particular, their internet service works more reliably and more consistently, which makes a

[5] See for example, Verizon 5G Home Router. https://www.verizon.com/support/knowledge-base-227026/ (viewed Nov. 8, 2023). This device has parental controls, an information-processing feature.

[6] Internet Engineering Task Force, *An Architecture for Differentiated Services*, Request for Comments (RFC) 2475, https://tools.ietf.org/html/rfc2475.

[7] For example, see AT&T, "Data usage support." https://www.att.com/support/how-to/wireless/data-usage (viewed Oct. 23, 2023). The page states, "On an unlimited plan? We may temporarily slow your speed at any time if our network is busy. We may also slow it after you use more than 50GB or 22GB of data in a single bill period."

[8] IETF, "IETF Recommendations Regarding Active Queue Management," RFC 7567, https://tools.ietf.org/html/rfc7567.

variety of applications possible that in the absence of such techniques would work sluggishly, or not at all.

12. Cable internet access also can prioritize traffic using CableLabs' PacketCable Multimedia Specification (PCMM).[9] The specification states that its intent is "to support the deployment of general multimedia services by providing a technical definition of several IP-based signaling interfaces that leverage core QoS and policy management capabilities native to DOCSIS Versions 1.1 and greater." This capability acquires, processes, and transforms information. Comcast explains its open-source software implementation of PCMM as follows:

> For the past several months Comcast [has] been building a new policy engine for orchestrating Quality of Service (QoS) on our network and now we're excited to begin contributing key parts of that engine available to the open source community. QoS is a critical function for network operators. On our DOCSIS network, QoS technology is how we ensure that essential functions are allocated enough bandwidth to perform at the highest level. A good example is a voice call, which needs a certain amount of dedicated bandwidth to be crystal clear and without jitter.[10]

Consumers benefit from this technology because certain applications, such as the voice call mentioned in the Comcast example, operate in a dependable fashion and are not adversely affected by other traffic traversing the same broadband connection.

13. In addition, many ISPs allocate private addresses to users and must then perform network address translation (NAT) between the private and externally-facing, public IP addresses.[11] NAT, which acquires, stores, processes, and transforms packets, benefits customers in multiple ways. Without it, ISPs would not have a sufficient number of Internet Protocol version 4 (IPv4)

[9] CableLabs, *PacketCable Multimedia Specification*, https://community.cablelabs.com/wiki/plugins/servlet/cablelabs/alfresco/download?id=152f0820-cf0c-4a23-ada3-898746e490c2.

[10] Comcast, "Introducing An Open Source Network Policy Engine," September 20, 2016, https://corporate.comcast.com/stories/introducing-an-open-source-network-policy-engine (viewed Oct 23, 2023). See also IETF RFC 6057, "Comcast's Protocol-Agnostic Congestion Management System," https://tools.ietf.org/html/rfc6057. The RFC states: "If the software determines that a particular subscriber or subscribers have been the source of high volumes of network traffic during a recent period of minutes, traffic originating from that subscriber or those subscribers temporarily will be assigned a lower priority status."

[11] For example, for non-routable IPv4 addresses, see IETF, *Address Allocation for Private Internets*, RFC 1918, https://tools.ietf.org/html/rfc1918.

addresses for all of their customers, forcing customers to either use Internet Protocol version 6 (IPv6), which has many more addresses but is not supported by all internet nodes, or to restrict service to just the IPv4 addresses the ISP can allocate, possibly denying service to customers. NAT also provides a security function because the internal private addresses of customer devices are obscured, thus restricting unsolicited and potentially harmful internet traffic.

14. ISPs also provide IPv4-to-IPv6 gateway functions, interconnecting between IPv4 and IPv6 networks. Further, IPv6 also performs extensive packet processing. For example, the IETF specification RFC 7045, *Transmission and Processing of IPv6 Extension Headers*,[12] explains how IPv6 network nodes, including ISPs' nodes, need to process what are called extension headers, resulting in different routing functions depending on the contents of the header. This extent of processing in IPv6 networks is significantly greater than in IPv4 networks. This function in IPv6–which acquires, stores, processes, and transforms the packets–enables connections that would not otherwise be possible (for example, an IPv4 node communicating with an IPv6 node), or with more efficient routing, decreases latency and increases throughput, enabling real-time applications such as video conferencing and gaming. Network management concerns itself with delivering packets from one node to another. Functions that change the packets themselves, such as encapsulating an IPv6 packet within an IPv4 packet, such that the header data of the IPv6 packet is now the content information of the IPv4 packet, are information processing and transformation steps beyond mere transmission.

15. Recognizing that different traffic flows have fundamentally different requirements, the IETF has developed new specifications for an architecture called Dual Queue Networking. IETF RFC 9330, titled "Low Latency, Low Loss, and Scalable Throughput (L4S) Internet Service,"[13] "enables internet applications to achieve low queuing latency, low congestion loss, and scalable throughput control." Related specifications include RFC 9331, "The Explicit Congestion Notification (ECN) Protocol for Low Latency, Low Loss, and Scalable Throughput (L4S),"[14] and RFC 9332, "Dual-Queue Coupled Active Queue Management (AQM) for Low Latency, Low Loss, and Scalable Throughput (L4S)."[15] Dual Queue Networking will enable ISPs to better support applications such as AR, VR, video conferencing, cloud gaming, and other real-time applications. This and other traffic management approaches involve a deep level of user information

[12] https://tools.ietf.org/html/rfc7045.

[13] IETF Datatracker, RFC 9330, https://datatracker.ietf.org/doc/rfc9330/.

[14] IETF Datatracker, RFC 9331, https://datatracker.ietf.org/doc/rfc9331/.

[15] IETF Datatracker, RFC 9332, https://datatracker.ietf.org/doc/rfc9332/.

processing, improving overall reliability and efficiency while also enabling applications that would not otherwise be possible.

16. ISPs are also investing in internet infrastructure by improving routing security. One example is employing a Resource Public Key Infrastructure (RPKI) to prevent "route hijacks" due to malicious action or routing errors.[16] ISPs are also cryptographically signing Route Origin Announcements (ROAs) and validating Border Gateway Protocol (BGP) route updates.

Caching

17. All major ISPs cache content using caching servers located within the ISP network or through direct connection with content delivery networks. Because the cache stores and retrieves information, it is an information service. Moreover, it also provides functionalities that go well beyond merely facilitating transmission; rather, it affords the customer additional capabilities, taking it outside the scope of network management. With caching, the ISP's DNS servers direct an end user's request for specific content to different cache servers, depending upon the proximity of the end user and/or congestion at a given cache. Thus, content that would normally be delivered from a distant server can simply traverse the ISP-to-user connection. This minimizes distance traveled over the internet and internet bottlenecks, thereby improving users' quality of experience and adding value to their broadband internet access service by providing faster and more dependable service.

18. In some cases, the ISP owns and operates the cache. In other cases, the cache hardware can be provided or managed by a third party but is still operated at the ISP location.[17] Alternatively, many ISPs have collaborative direct connections to content delivery networks. In all cases, the cache is a part of the broadband internet access service offered by the ISP, working hand-in-hand with the ISP's DNS servers. Users cannot directly opt out of the caching component of the offering, but using third-party DNS would functionally prevent users from being directed to the ISP's cache, resulting in a degradation of service. Thus, the caching of information and transmission are inextricably linked.

19. Put simply, today's high-quality streaming content relies heavily on caching and direct connectivity to ISPs. Increasingly, internet content is bulking up. Streaming has already

[16] Supported by Mutually Agreed Norms for Routing Security (MANRS), a global initiative focused on reducing the most common routing threats. https://www.manrs.org/.

[17] For example, see Akamai, "Akamai Network Partnerships," https://www.akamai.com/solutions/industries/network-operator/akamai-network-partnerships (viewed Nov. 3, 2023). See also Netflix, "Welcome to Open Connect." https://openconnect.netflix.com/en/ (viewed Oct 23, 2023).

transitioned from standard definition to high definition, and the industry is currently providing an increasing amount of content in ultra-high definition. Virtual reality will impose even greater bandwidth demands on network operators.[18] Caching substantial portions of the internet's massive and growing content is essential to ensure that users' ability to access, retrieve, and manipulate information is not degraded. The volume of streaming content is so great that the internet backbone could not handle the traffic if it weren't for distributed caching of the content, particularly through direct ISP connections with Content Delivery Networks (CDNs). While most impactful for static content like streaming video, caching is also widely used for dynamic content that varies over time or by user, such as news websites or social media. Dynamic content is cached either through scripts running within the cache (for interactive or personalized content) or through regular purging and updating of the cache (for rapidly updated content such as news stories, inventory, or pricing data).[19]

20. Companies such as Akamai operate CDNs both outside and inside ISP networks. As the IETF has summarized:

> Content Delivery Networks (CDNs) provide numerous benefits for cacheable content: reduced delivery cost, improved quality of experience for End Users, and increased robustness of delivery. For these reasons, they are frequently used for large-scale content delivery. As a result, existing CDN Providers are scaling up their infrastructure, and many Network Service Providers (NSPs) are deploying their own CDNs.[20]

At ¶ 78 of the NPRM, the FCC states: "In addition, should the Commission distinguish between caching by ISPs and the kind of caching that third-party content providers use to keep copies of content (such as videos and images, but possibly also web pages) closer to users? We preliminarily conclude that caching of this kind is not provided by ISPs and thus is not a part of BIAS, and as such does not transform BIAS into an information service." From a technical

[18] For a discussion of the enormous bandwidth requirements of virtual reality, see ABI Research/Qualcomm, *Augmented and Virtual Reality: the First Wave of 5G Killer Apps*, 2017, https://www.qualcomm.com/documents/augmented-and-virtual-reality-first-wave-5g-killer-apps. Six degrees of freedom virtual reality consumes 200 Mbps to 1,000 Mbps.

[19] For example, *see* Cloudflare, "Caching static and dynamic content: How does it work?" (viewed December 5, 2023), https://www.cloudflare.com/learning/cdn/caching-static-and-dynamic-content/; Akamai Techdocs, "Cache Strategies" (viewed December 5, 2023), https://techdocs.akamai.com/purge-cache/docs/cache-strategies.

[20] Internet Engineering Task Force (IETF), *Request for Comments: 6707, Content Distribution Network Interconnection (CDNI) Problem Statement,* 2012. https://www.rfc-editor.org/rfc/rfc6707.

perspective, however, the cache that an ISP operates is indistinguishable from such third-party services. Whether the ISP manages caching infrastructure itself or contracts for this service, what improves the BIAS offering is the tight integration of caching with the ISP's DNS infrastructure. Even for caching operated by third party content providers, integration with ISP DNS is a must to efficiently deliver content from geographically close replicas of the contents.

21. Some have argued that caching does not work with encrypted traffic, as is common nowadays with encrypted web traffic using the Secure Hypertext Transfer Protocol (S-HTTP).[21] This is simply incorrect. Even if the content server delivers encrypted traffic, DNS can direct the client to the appropriate caching server, such as a streaming server, whether located remotely or close by in a content delivery network. The transmission is then encrypted between the destination server and the user.[22] As discussed in the next section on the Domain Name System, an ISP-provided DNS, in combination with a content delivery network hosted by the ISP, provides users an optimum internet experience.

Domain Name System (DNS)

22. DNS provides the processing capabilities that allow subscribers to visit a website without inputting an IP address. Users seeking information on the internet do not think of communicating between or among specific points, as required by the formal definition of a "telecommunications service."[23] When a subscriber types a domain name into a browser, the browser typically queries the ISP's DNS service for the proper IP address to send that information. The DNS service is typically implemented in two components: a DNS resolver (also referred to as a DNS recursive server) that receives the query and caches DNS information, and

[21] For example, in her concurrence in the *Mozilla* opinion from the United States Court of Appeals for the District of Columbia Circuit (October 1, 2019), Judge Millett stated "… caching has been fundamentally stymied by the explosion of Internet encryption." https://www.cadc.uscourts.gov/internet/opinions.nsf/FA43C305E2B9A35485258486004F6D0F/$file/18-1051-1808766.pdf.

[22] The one exception is when a user employs a virtual private network (VPN) connection, in which case the DNS server may be operated by the VPN provider, and the VPN DNS may not have any knowledge about the ISP CDN.

[23] 47 U.S.C. § 153(50) (definition of "telecommunications"); id. at § 153(53) (definition of "telecommunications service"). Citation appears in footnote 69 ¶ 18 of the NPRM.

an authoritative server that has more complete DNS information and can provide the resolver information it needs.[24]

23. DNS also provides a wide range of other services. For example, DNS can also be used for reverse lookups, with which a user queries DNS with an IP address to determine the domain name associated with the IP address. DNS operates in a similar mode when it provides an error-page-assist function for a user who has supplied an invalid address and DNS suggests similar pages the user may have been intending to reach.

24. In each of these cases, DNS service exhibits all of the hallmarks of an information service. A DNS server processes information when it receives DNS queries; it generates information when it delivers a response to an end user or queries an authoritative server; it stores domain name information in its cache; it transforms information when it takes a query from a user and sends it upstream (for information not in its cache); it retrieves information when it obtains domain name data from the internet; it utilizes information that it has stored in its cache; and it makes information available when it responds to DNS queries.

25. Most ISPs implement an advanced version of DNS called EDNS Client Subnet (ECS), with EDNS referring to Extensions for DNS, an approach specified in RFC 7871.[25] Using ECS, the resolver can provide client subnet information to the Authoritative server, which identifies the location of the client. In cases where a content delivery network may be distributed across multiple locations, the authoritative server can respond with the IP address optimal for the client, such as the closest or the least loaded. Many ISPs host content delivery networks within their network, and by integrating these with ECS on their ISP-managed DNS systems, the ISP can optimize the user experience. As further explained in paragraph 28, this approach does not work with third-party DNS servers.

26. Previously,[26] the FCC analogized DNS to a 411 telephone lookup service, but the two services are profoundly different. Using a 411 service, a user has a mindset of connecting to a phone number and knows only the name of person that they intend to call. The user then obtains a phone number through a separate call to the 411 service and then makes a phone call using that number. In contrast, with DNS, the process happens inline, automatically and as part of the

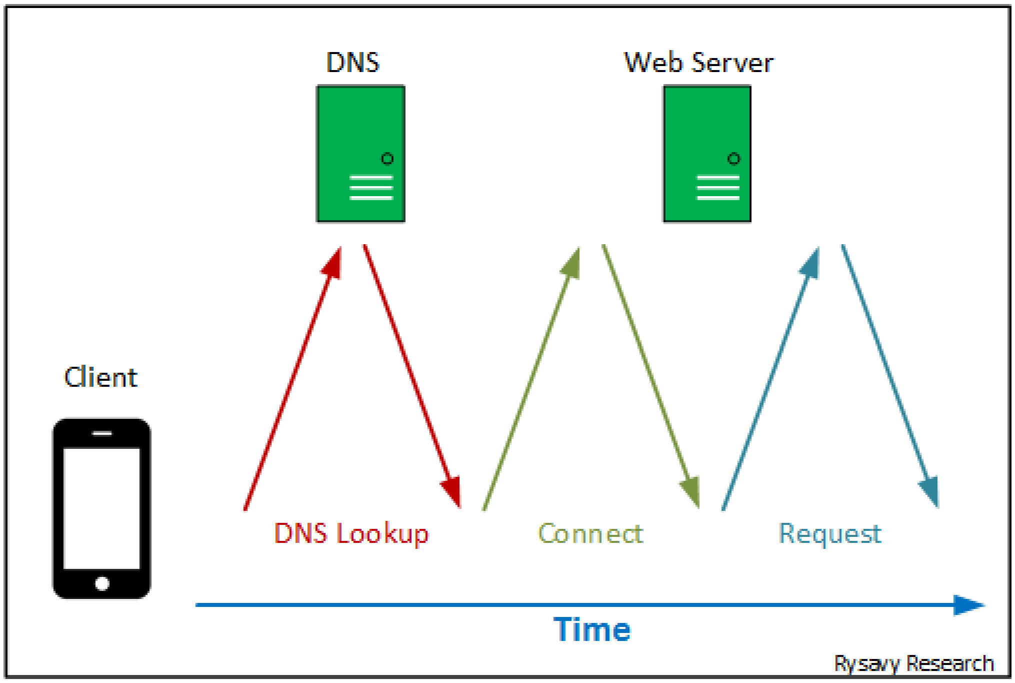
[24] For further explanation, see Cisco, "What is the difference between authoritative and recursive DNS nameservers?" Aug. 2023. https://umbrella.cisco.com/blog/what-is-the-difference-between-authoritative-and-recursive-dns-nameservers.

[25] IETF, *Client Subnet in DNS Queries*, https://datatracker.ietf.org/doc/html/rfc7871.

[26] 2015 Title II Order at ¶ 370.

internet query, without any involvement by the user other than the initial request. A user entering a search term into a web page, for example, does not think about needing to get an IP address first. He or she enters the term and the client software, if it does not already have the IP address of the search engine, performs a DNS query. Then, after obtaining the IP address, the client software connects to the desired server. Furthermore, as shown in Figure 1, the DNS query is one step in a multi-step communications process. Across time, a request to a DNS server is followed by a response from the DNS server (with a resolving DNS server possibly making an additional request to an authoritative DNS server); which is then followed by a connection request to and a response from the web server; which is then followed by a request for information from the web server. In addition, with an internet service facilitated by DNS, the user obtains desired information regardless of its location or endpoints, whereas with a telephone 411 lookup service, all the user obtains is a phone number. Calling that number provides no assurance of reaching the desired person.

Figure 1: DNS as an Integrated Step in Network Access



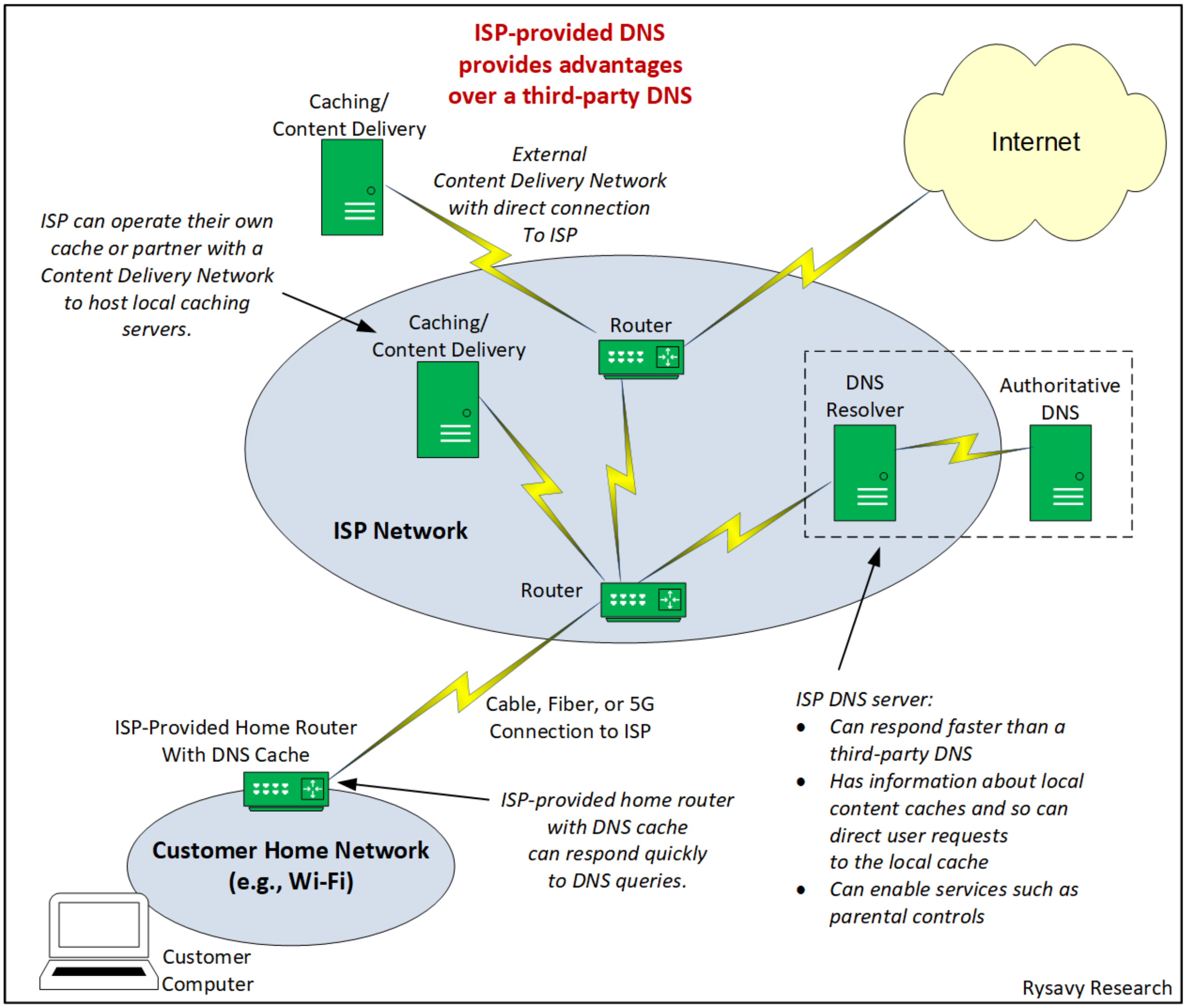
27. The DNS query is not an “adjunct-to-basic” service, as the NPRM states in ¶ 75. The 2015 order, referenced in the NPRM at footnote 269, stated that an adjunct-to-basic function must be incidental to the underlying telecommunications service. The only perspective that warrants DNS being “incidental” is one in which users view themselves as communicating with IP addresses. But users seek answers to questions, to communicate with their loved ones, and to engage in myriads of other activities, none of which include wanting to know the IP addresses

of the services with which they are communicating. Indeed, if IP addresses were so important, wouldn't business cards, in addition to listing the telephone numbers of a user, also include the IP address of their organization? IP address information is integral to supporting users' information processing objectives. The ISP and other internet infrastructure constitute a complex and distributed information service to efficiently and most effectively provide this IP address information.

28. Although third-party DNS servers are available, using an ISP-provided DNS service offers many advantages to subscribers, as depicted in Figure 2. As discussed above, DNS architecture is distributed, and the resolving DNS server within the ISP network can be located close to the user, resulting in faster response times than is possible with a third-party DNS server, which requires traffic to traverse across multiple hops. Another major advantage of ISP-provided DNS service is when the ISP caches internet content, for example streaming content on a content delivery network that it hosts, or when an ISP has a direct connection to a content delivery network, an increasingly common configuration. In this case, the DNS, using ECS (described in paragraph 25), can resolve to the closest caching server while also optimizing load balancing. A third-party DNS doesn't have knowledge of the ISP caching content or CDN with a direct ISP connection and will instead direct the user to an external site, creating unnecessary internet traffic, slowing response time, and undermining the user experience. Similarly efficient mechanisms in use are ISP-provided routers that cache DNS information right at the user home location, which provide extremely fast response times for frequently used internet destinations.[27] Using a third-party DNS service bypasses this efficient architecture. Yet another advantage of ISP-provided DNS is that some ISP-provided services are intertwined with the DNS service, such as optional filtering of adult content, in which case the DNS server itself blocks internet sites. This parental feature becomes unavailable with a third-party DNS service.

[27] ISP-provided routers can also manage radios in customer premises, such as choosing Wi-Fi channels that do not overlap with nearby access points. ISPs are motivated to supply these full-service gateways because often the home network is the bottleneck for internet connectivity. See Cornell University, "Measuring the Prevalence of Wi-Fi Bottlenecks in Home Access Networks," Nov. 2023. https://arxiv.org/abs/2311.05499.

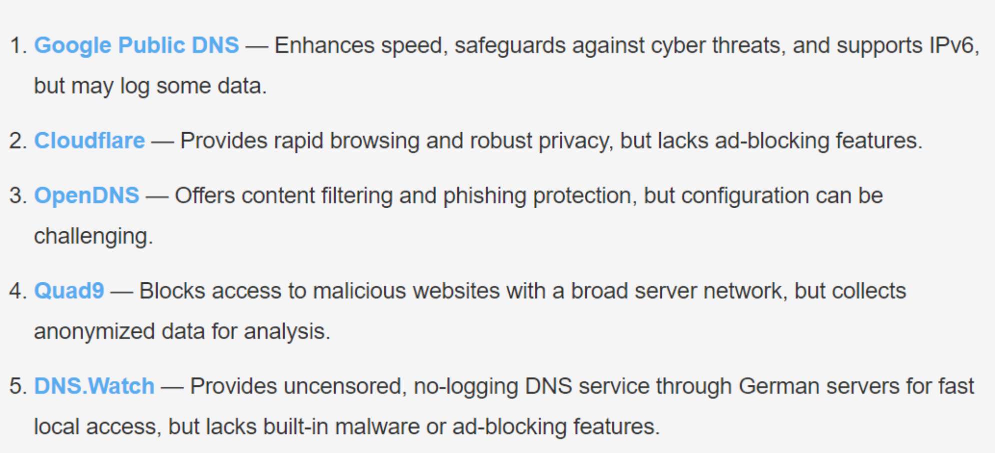
Figure 2: Advantages of an ISP-Provided DNS Service.


ISP-provided DNS provides advantages over a third-party DNS
Internet
Caching/ Content Delivery
External Content Delivery Network with direct connection To ISP
ISP can operate their own cache or partner with a Content Delivery Network to host local caching servers.
Caching/ Content Delivery
Router
DNS Resolver
Authoritative DNS
ISP Network
Router
Cable, Fiber, or 5G Connection to ISP
ISP-Provided Home Router With DNS Cache
ISP-provided home router with DNS cache can respond quickly to DNS queries.
ISP DNS server:
Can respond faster than a third-party DNS
Has information about local content caches and so can direct user requests to the local cache
Can enable services such as parental controls
Customer Home Network (e.g., Wi-Fi)
Customer Computer
Rysavy Research

29. Given the advantages of using the ISP-provided DNS server, it comes as no surprise that the overwhelming majority of DNS queries are made using the ISP-provided DNS service. Quite simply, the ISP-provided service addresses user needs. It also simplifies configuration of user devices. Using a third-party DNS requires a user to manually configure low-level communications settings, and so most users do not make this change. Though this change is relatively straightforward for a tech-savvy user, and such a user may have valid reasons for desiring a third-party DNS, the change is not one that an average user understands or is inclined to pursue. And even if a user decides to use a third-party DNS service, the user is confronted

with confusing tradeoffs between the third-party providers. For example, one website characterizes common third-party DNS services as follows:

Figure 3: Example of Complicated Tradeoffs for User Choosing a Third-Party DNS[28]



1. Google Public DNS — Enhances speed, safeguards against cyber threats, and supports IPv6, but may log some data.
2. Cloudflare — Provides rapid browsing and robust privacy, but lacks ad-blocking features.
3. OpenDNS — Offers content filtering and phishing protection, but configuration can be challenging.
4. Quad9 — Blocks access to malicious websites with a broad server network, but collects anonymized data for analysis.
5. DNS.Watch — Provides uncensored, no-logging DNS service through German servers for fast local access, but lacks built-in malware or ad-blocking features.

30. Some have cited a high usage of third-party DNS servers.[29] These numbers, such as 180 billion queries per day, have to be treated in context. While 180 billion queries may sound large in the abstract, it is actually relatively small—major ISPs process trillions of DNS queries every day.[30] Moreover, most IoT devices, such as doorbell cameras and internet-connected thermostats, which number in the many millions, are hard-coded to use a particular third-party DNS service. Researchers found that Google DNS and OpenDNS servers are the most prevalent choices for hard-coded smart assistants, connected TVs and other IoT devices.[31] Therefore third-party DNS query numbers are generally not representative of choices made by an ISP customer.

[28] WizCase, "21 Best Free & Public DNS Servers (for Every Country) in 2023," https://www.wizcase.com/blog/best-free-public-dns-servers/ (viewed Nov. 2, 2023).

[29] For example, Judge Millett of the United States Court of Appeals for the District of Columbia Circuit, in the *Mozilla* opinion of October 1, 2019, stated "By 2015, OpenDNS and Google were processing over 180 billion queries every day." https://www.cadc.uscourts.gov/internet/opinions.nsf/FA43C305E2B9A35485258486004F6D0F/$file/18-1051-1808766.pdf.

[30] For example, I understand that AT&T and Verizon each process over a trillion inquiries per day. Disclosed 11/17/2023 in direct communication with network engineers.

[31] M. Hammad Mazhar & Zubair Shafiq, "Characterizing Smart Home IoT Traffic in the Wild," *2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation* (2020),

31. DNS technology is evolving, and ISPs continue to invest in their DNS systems to improve the customer experience. Recently implemented enhancements include support for new encrypted DNS communications protocols, including DNS over Hypertext Transfer Protocol Secure (DoH), DNS over Transport Layer Security (DoT), and DNS over Quick UDP Internet Connections (QUIC) (DoQ).[32] The IETF has also approved new secure discovery protocols for finding and assigning encrypted DNS servers from the ISP network. Specifications include RFC 9460 (Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records), RFC 9461 (Service Binding Mapping for DNS Servers), and RFC 9462 (Discovery of Designated Resolvers). These specifications are from the Adaptive DNS Discovery (ADD) working group.[33]

32. If users were better served by a third-party DNS, then ISPs would make the rational business decision to direct users to these third-party services and save themselves the cost of deploying and maintaining expensive infrastructure. ISPs do not make money offering DNS capabilities, but ISPs and their customers alike perceive significant value in ISP-provided DNS service, which thus remains inextricably intertwined with their ISPs' broadband internet access service offerings.

Many Bundled Offerings Are Inherently Intertwined with Broadband Internet Access

33. ISPs offer numerous services that are part and parcel of the broadband internet access service. Many include one or more characteristics of information service and do not merely facilitate transmission, nor are they stand-alone offerings. A few examples follow.

34. ISPs may provide user-directed content filtering as part of their broadband internet access offering. These services do not merely facilitate transmission. Rather, they involve the processing of information that results in the change of form and content of information sent over networks. One example of user-directed filtering is Web Guard, which is a free service that

https://doi.ieeecomputersociety.org/10.1109/IoTDI49375.2020.00027, stating that 98% of smart assistants and 72% of smart TVs [for example] use hard-coded Google DNS servers to resolve DNS queries instead of using the default DNS server configured at the home gateway.")

[32] For background, see NextDNS, "What is DNS over TLS (DoT), DNS over Quic (DoQ) and DNS over HTTPS (DoH & DoH3)?" https://help.nextdns.io/t/x2hmvas/what-is-dns-over-tls-dot-dns-over-quic-doq-and-dns-over-https-doh-doh3 (viewed Nov. 17, 2023).

[33] IETF Datatracker, "Adaptive DNS Discovery (ADD)," https://datatracker.ietf.org/wg/add/about/ (viewed Nov 17, 2023). The working group charter states, "Clients adopting encrypted DNS protocols need to determine which DNS servers support those protocols, and which server to use for specific queries if multiple servers are available. These decisions can vary based on the network environment, and also based on the content and purpose of the client queries."

T-Mobile makes available to its broadband customers to help restrict adult content from being seen or accessed by family members under eighteen years old.[34] This is a service a subscriber opts into for particular access lines, such as for his or her children. Because the filter processes information sent by the user in accessing web sites and because the user does not necessarily receive the requested page, the filtering is an information service. And because network management concerns itself with enabling transmission, a service that selectively makes information available (or, in other words, prevents certain transmissions) is not a network management function. Moreover, all of these services add value to the customer experience beyond mere transmission by making the internet safer for families.

35. Another form of content modification that mobile broadband providers employ is video optimization. To reduce the demand of high-resolution video on mobile devices with small screens, mobile operators optimize the content so as to consume less bandwidth. Such functionality benefits customers on usage-based plans (or plans that offer a set amount of high-speed data), allowing them to consume more video for the same amount of data consumption. One example is AT&T's Video Management capability that "applies automatically and strives to render streaming video in standard-definition (SD), with a max speed of 2Mbps if you have both a 5G-enabled device and rate plan, or 1.5Mbps if you don't. This speed is perfect for streaming video on a smartphone and may help control data usage."[35] Another is T-Mobile's "Binge On" service, whereby "[a]ll detectable video streaming is optimized for your mobile device so you can watch up to 3 times more video using the same amount of high-speed data."[36] Verizon also manages video streaming quality.[37] Optimization of video resolution, particularly if done by video transcoding, is a complex algorithmic process that processes and transforms the content, making it more than transmission.

[34] T-Mobile, "Web Guard," https://www.t-mobile.com/support/plans-features/web-guard-device-content-filter (viewed Oct. 24, 2023). AT&T offers a similar service called "AT&T Secure Family," which can filter online content. https://www.att.com/security/secure-family-app/ (viewed Oct. 24, 2023). See also Comcast's parental control, "Manage People With Xfinity xFi," https://www.xfinity.com/support/articles/xfinity-xfi-manage-profiles (viewed Oct 24, 2023)," and Cox, "Parents' Ultimate Guide to Parental Controls," https://www.cox.com/residential/articles/parents-ultimate-guide-parental-controls.html (viewed Oct. 24, 2023).

[35] AT&T, "Learn about Video Management," https://www.att.com/support/article/wireless/KM1169198/ (viewed Oct 24, 2023).

[36] T-Mobile, "Binge On," https://www.t-mobile.com/tv-streaming/binge-on (viewed Oct. 24, 2023).

[37] Verizon, "My Verizon Website - Manage Video Streaming Quality," https://www.verizon.com/support/knowledge-base-233798/ (viewed Oct 24, 2023).

36. Many ISPs also provide malware detection and alerting services for their customers in accordance with recommendations developed by the FCC's CSRIC III, Working Group 7[38] on Botnet Remediation, including the Anti-Bot Code of Conduct,[39] which typically covers all customers on a network rather than just those that have opted into a service. ISPs, using their routers or other security nodes, can also perform additional security functions, such as protecting web servers and end users against denial of service, detecting viruses, and distributing virus signatures to client systems. All such security functions relate to an information service that processes information that is beyond transmission. Simple transmission would mean that all traffic addressed to a user would be delivered. But instead, the ISP's security system processes the traffic addressed to a user and transforms it by delivering only a subset of the traffic that it deems safe, making the internet a safer place for subscribers.

37. Despite the popularity of email services from companies such as Google, many ISPs provide email service, which is an information service that acquires, stores, processes, and retrieves information. For many ISPs, this email service is bundled with internet access.[40] ISPs that offer email generally also provide an option for a web interface so users can interact with their email without needing an email client program, and many also offer an app for smart phones and tablets. Using a web interface or an app adds the functions of generating and transforming information. ISPs that offer email generally also offer spam filtering. This additional offering is an information service, because the spam filter must: (1) retrieve spam-processing criteria; (2) store this information; (3) process the user email by applying it against the criteria; and (4) then transform the content by marking spam messages as spam. Additional information processing associated with email accounts includes blocking email addresses, blocking email domains, white-listing email addresses, white-listing email domains, and forwarding emails to another email address.[41] These ISP email accounts may also have the ability for users to store contact information. Again, these capabilities are not simple transmission, nor do they facilitate transmission.

[38] See https://transition.fcc.gov/bureaus/pshs/advisory/csric3/WG%207.pdf.

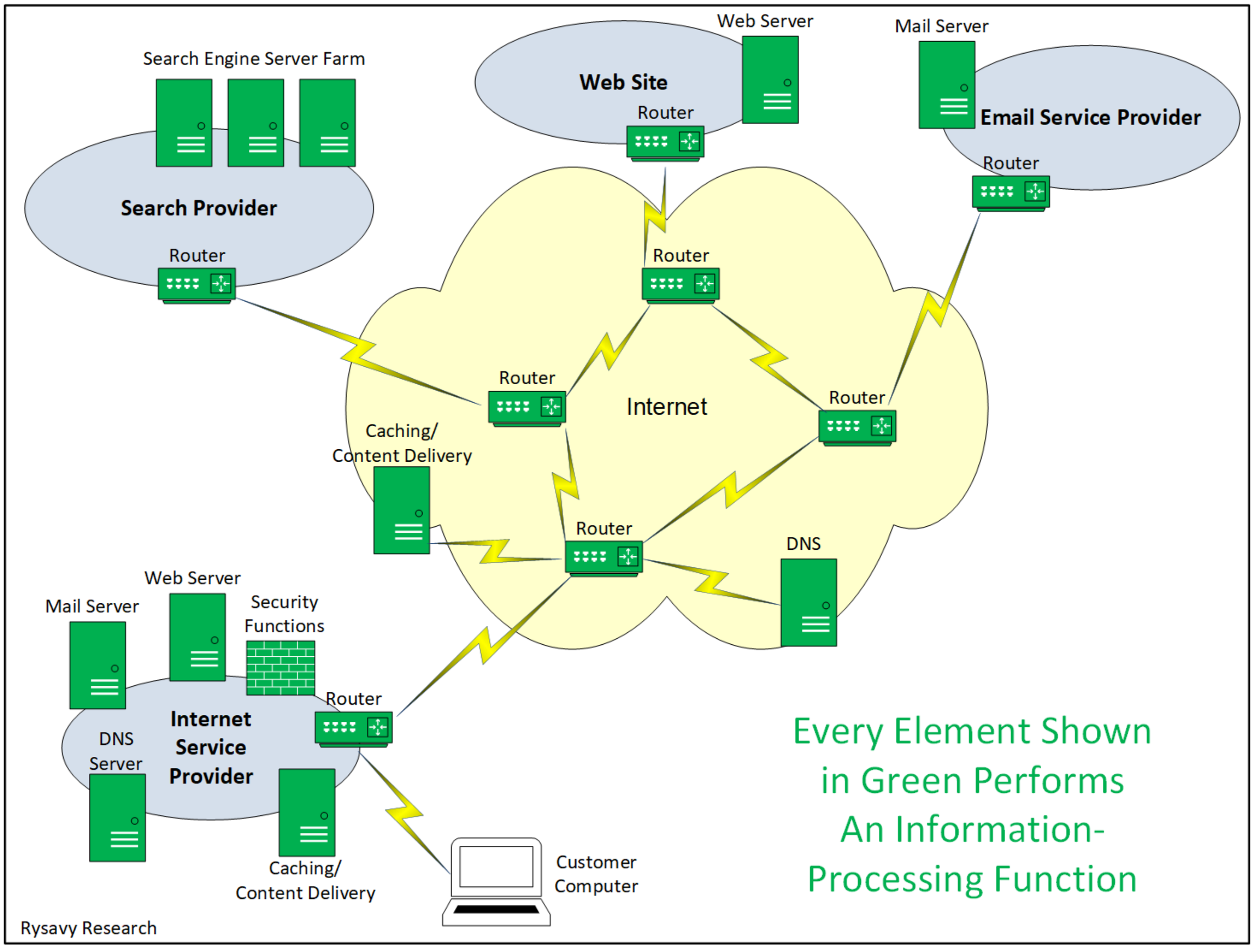
[39] See https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf and https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf.

[40] See Xfinity, "Manage Your Xfinity Email," https://www.xfinity.com/support/articles/stay-connected-with-email (viewed Nov. 24, 2023).

[41] For example, see Charter Spectrum, "Email Security," http://www.spectrum.net/support/internet/email-security/ (viewed Oct. 24, 2023).

38. Figure 4 depicts the elements of the internet discussed above, including routing, mail servers, web servers, DNS, routing, search engine, and the customer's computer. Every element in this diagram shown in green performs an information processing function.

Figure 4: Information Service Nature of the Internet



The Internet and the PSTN are Distinct Platforms

The Internet and PSTN are Separate Networks

39. The internet and the PSTN are two fundamentally different networks, using different architectures and protocols, and providing different capabilities. At the very heart of the PSTN is circuit-switching. On an end-to-end basis (telephone on one end to telephone at the other end), multiple circuits must be set up in series across different nodes before the phone call can occur. The purpose of the PSTN has always been to create a connection between two points of the users choosing for the transmission of telephone calls using a set of protocols called

Signaling System 7 (SS7). The International Telecommunication Union (ITU), which maintains the SS7 standards, states: “Signaling System No. 7 (SS7) is a set of telephony signaling protocols developed by ITU-T since 1970s, which is used to set up and tear down most of the world’s telephone calls.”[42]

40. This contrasts with the internet, which was developed for general purpose data-networking and uses packet-switching instead of circuit-switching. With packet-switching, individual packets traverse from node to node to reach their destination, with no connection setup beforehand. Each router that receives the packet makes a decision on how to forward the packet based on the IP address and other information contained in the header. At the end points, TCP handles items such as retransmission of packets and the pace at which it transmits packets so as to reduce network congestion. In contrast, with circuit-switching, the network creates an end-to-end connection using SS7 protocols, potentially across multiple paths, before any telephone communication can ensue. By way of analogy, packet switching is like traveling from one place to the next without making arrangements for the next leg of the journey until arriving at a destination. In contrast, circuit-switching is like making reservations in advance for every leg of a journey before embarking on the trip.

41. The two approaches could not be more different. The PSTN uses a control architecture that employs the SS7 protocol stack, which is fundamentally different than the TCP/IP protocol stack. Table 1 shows the corresponding protocols relative to the International Organization for Standardization (ISO) Open System Interconnection (OSI) model.[43] The OSI model provides a methodology for characterizing networks. Because the set of protocols differs at every single networking layer, the two networks are completely incompatible with each other and cannot directly interoperate.

[42] ITU, “ITU Workshop on SS7 Security,” 2016, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Pages/default.aspx (viewed Nov. 8, 2023). Note that 4G and 5G systems use the Diameter protocol for telephony signaling.

[43] International Organization for Standardization, *Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model*, ISO/IEC 7498-1:1994, https://www.iso.org/standard/20269.html. This model provides a methodology for characterizing packet-switched networks.

Table 1: TCP/IP Protocol Layers Versus SS7[44]

OSI Layer and Name	Internet: Transmission Control Protocol/Internet Protocol	PSTN: Signaling System 7 Protocol
7: Application	Application	Transactions Capabilities (TC), TUP, ISDN-UP. Also Mobile Application Part (MAP) for cellular networks.
6: Presentation		TUP, ISDN-UP
5: Session		TUP, ISDN-UP.
4: Transport	Transmission Control Protocol (TCP) or User Datagram Protocol (UDP)	Signaling Connection Control Part (SCCP). Also Telephone User Part (TUP) and Integrated Services Digital Network (ISDN) User Part (ISDN-UP).
3: Network	Internet Protocol (IP)	MTP-3
2: Data Link	For example, Ethernet or LTE	MTP-2
1: Physical	For example, Ethernet or LTE	Message Transfer Part-1 (MTP-1)

42. Beyond protocols, the nodes in these networks also differ. In the internet, the interconnecting nodes are routers, which process IP packets and determine which routes to use. In contrast, the telephony network uses the following nodes: Service Control Point (SCP), Signal Transfer Point (STP), and Service Switching Point (SSP).[45] An SCP controls the service in telephone systems, originating and terminating control (signaling) messages; an STP routes SS7 control messages; and SSPs are switches that originate and terminate calls. These nodes are all fundamentally different from the routers used in the internet and perform different functions for a different purpose (as explained above).

[44] SS7 layering source: Figure 2/Q.700, International Telecommunication Union, *Specifications of Signalling System No. 7, Introduction to CCITT Signalling System No. 7 No. 7*, ITU-T Recommendation Q.700, 3/93, http://www.itu.int/rec/T-REC-Q.700-199303-I/e.

[45] For a further description, refer to Performance Technologies, *Tutorial on Signaling System 7 (SS7)*, https://www.scribd.com/doc/201641316/Tutorial-on-Signaling-System-7-SS7.

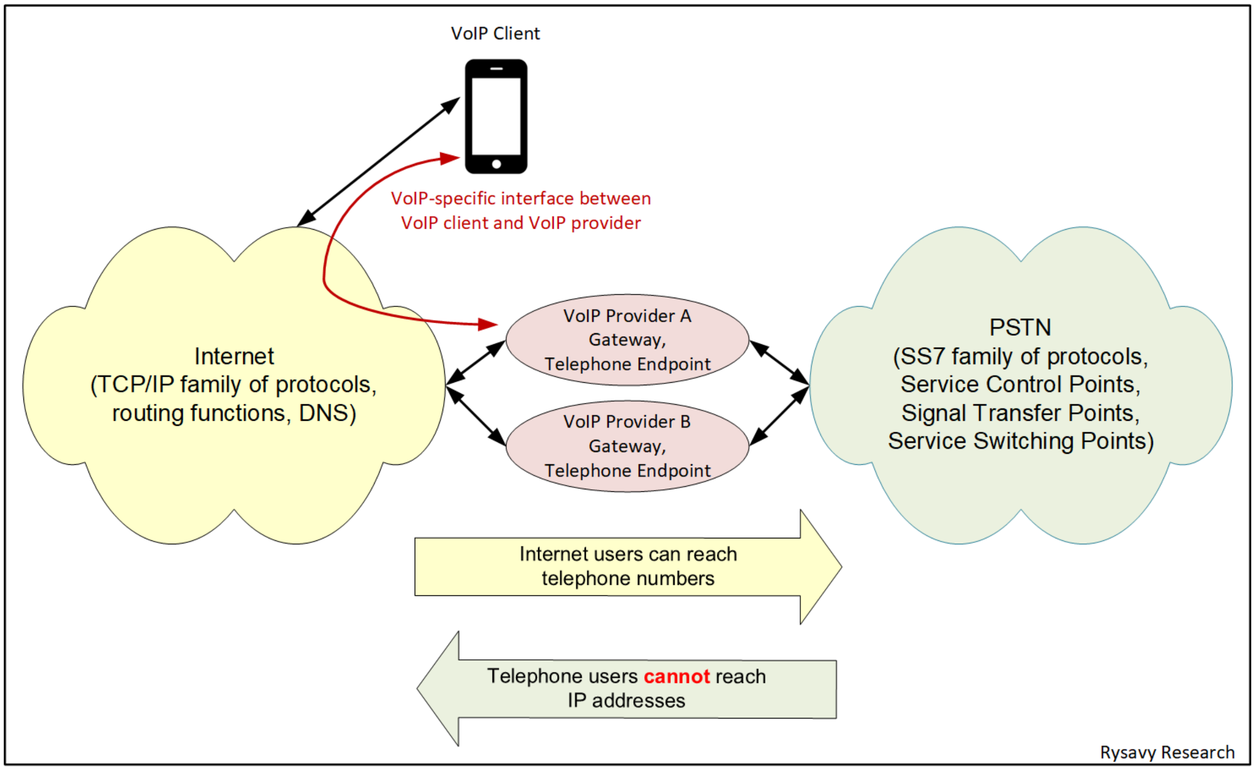
Interconnection of Internet and PSTN

43. The internet and the PSTN, as discussed in the preceding paragraphs, are separate networks that are operated in fundamentally different ways. While it is true that third-party VoIP applications and services enable a limited form of interconnection, these services do not create an integrated network between the internet and PSTN. With a VoIP service, such as from Vonage or a cable operator, a user can make a telephone call from the internet to a phone number on the PSTN, as shown in Figure 5. Such capability, however, is achieved by the VoIP provider (or a service provider on behalf of the VoIP provider) acting as a gateway to translate the different protocols. To the telephone network, the VoIP provider appears as a telephone network node. To the internet, the VoIP provider appears as an internet node. Without the gateway and protocol conversion functions of the VoIP provider, the two networks would not be able to communicate with each other. This protocol conversion is not trivial and includes interfaces to the VoIP application (or VoIP gateway device) and PSTN signaling (control) capability. In addition, because internet nodes do not have telephone numbers, the VoIP provider must act as a telephone-number proxy on behalf of the internet node. Customers of these VoIP services may use a telephone number, but the VoIP provider acts as the end point for the voice calls and relays the call through its data (non-telephone) interfaces to the VoIP application, as shown in Figure 5. Over the internet, the call is carried as TCP/IP data traffic, not as a telephone call.

44. An analogy is transporting an automobile on a train car, which allows the passenger and the automobile to travel over the rail system.[46] Such capability does not transform the rail system and road system a single network. Nor does it permit perfect interoperability: Even though this system allows cars to reach any location that trains can go, it doesn't allow trains to go to places that cars can go by road. The same is true of the telephone network and the internet.

[46] For example, see Amtrak, "Auto Train," https://www.amtrak.com/auto-train (viewed Oct. 24, 2023).

Figure 5: VoIP Operators Providing Gateway Function between the PSTN and the Internet


VoIP Client
VoIP-specific interface between VoIP client and VoIP provider
Internet (TCP/IP family of protocols, routing functions, DNS)
VoIP Provider A Gateway, Telephone Endpoint
VoIP Provider B Gateway, Telephone Endpoint
PSTN (SS7 family of protocols, Service Control Points, Signal Transfer Points, Service Switching Points)
Internet users can reach telephone numbers
Telephone users cannot reach IP addresses
Rysavy Research

45. Although internet users, with a subscription to a VoIP service, can make telephone calls to telephone numbers, the reverse is not true, as depicted in Figure 5. Telephone users cannot make connections to IP addresses, nor even to Session Initiation Protocol (SIP) Uniform Resource Identifiers (URIs), which is the most typical form of addressing for VoIP. The concept does not even make sense. Telephones are designed to connect with other telephones using the telephone number. A telephone, for example, cannot send an email or browse a web site. This inability further demonstrates how the existence of VoIP providers does not create an integrated network between the internet and PSTN.

46. The view that mobile voice and data networks have converged is simply not correct. Even within the infrastructure of a modern mobile network, such as a 5G network, different infrastructure handles voice than data, and separate gateways handle the interconnections to the internet and the PSTN. Voice in a 5G network is transported over IP packets within the operator infrastructure, but it remains a voice service designed to interconnect with the PSTN. When a user is on a voice call, that voice call does not provide the user with any avenue to reach internet end points.

47. For these reasons, mobile broadband internet service and mobile telephony are distinct services that use different infrastructure, different protocols, and different interconnections.

Evolving Mobile Networks and Differentiated Offerings

48. Traditional telecommunications networks, such as telephony networks, are static entities whose functionality does not change over time. In contrast, 5G networks are software-based, and intended to flexibly respond to rapidly changing demands through service orchestration, a distributed core, and features such as edge computing. Operators are already using AI to improve network efficiency and reliability, and AI and machine learning will play an ever more important role in network operations, service offerings, and user applications. A keynote presentation at the 2023 5G Americas annual analyst meeting characterized the interconnected global 5G networks as the most complex machine ever built, one that is programmable and that provides a platform for innovative information processing.

49. 5G, as well as 4G LTE, networks implement a sophisticated QoS architecture to manage data flows. Traffic-flow parameters include whether bit rates are guaranteed, their priority relative to other traffic flows, the maximum amount of packet delay that can be tolerated, and the extent of permissible packet loss. 5G specifications define thirty-two quality indicators,[47] each with unique parameters. In contrast, LTE specifications define thirteen quality-class identifiers,[48] demonstrating the evolving sophistication of wireless networks and the importance of differentiated traffic flows. Voice over 5G New Radio (VoNR), based on voice-over-IP protocols, uses these QoS mechanisms to provide carrier-grade voice service. Without this control, a 5G voice call would disintegrate if surrounding users were consuming large amounts of data. The network prioritizes voice as higher priority than data. The same prioritization of voice over data also occurs in 2G, 3G, and 4G networks.

50. Many other applications could benefit from prioritization. Certain applications work better (or can only function) with network management, including live streaming, gaming, telemedicine, video conferencing (in which video and voice have different requirements[49]), and autonomous vehicles. Different applications, however, have different QoS requirements. Streaming music

[47] 3GPP, *Technical Specification 23.501, System architecture for the 5G System*. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144. See Section 5.7, “QoS Model,” and “Table 5.7.4-1: Standardized 5QI to QoS characteristics mapping.”

[48] For details about LTE QoS, refer to 3GPP TS 23.203, *Technical Specification Group Services and System Aspects; Policy and charging control architecture*, http://www.3gpp.org/DynaReport/23203.htm. Specifically, see Table 6.1.7, “Standardized QCI characteristics.”

[49] For instance, users can tolerate momentary video degradation, but voice must remain intelligible.

and video, for example, requires high throughput but can tolerate delay and some packet loss. A health-monitoring device might consume only small amounts of data but requires high reliability and minimal delay. Background processes such as application or operating system updates can run at lower priority. As wireless networks are used for ever more time-sensitive and critical applications, they must provide needed reliability and performance; an entertainment video stream in a car should not delay an urgent message about a pedestrian in the middle of the road around a blind corner.

51. A common misconception about traffic prioritization is that prioritizing one traffic stream will harm another. The NPRM, at ¶ 158, perpetuates this misconception by wrongfully concluding that the availability of priority treatment will degrade the experience of other users. The truth of the matter is that traffic differentiation is not a zero-sum game, because selective application of QoS can increase the quality-of-experience across the entire subscriber base.[50] In addition, QoS markings are not simply used to ensure performance of one traffic type over another at times of congestion. QoS can also be used simply to classify certain traffic types differently so that a particular routing or security policy can be applied to particular traffic types.

52. The ITU 5G use-case model defines three usage categories for 5G: (1) enhanced mobile broadband; (2) massive-machine type communications; and (3) ultra-reliable and low-latency (URLLC) communications.[51] While 4G networks can handle the first two categories, URLLC , also referred to as mission critical, opens cellular networks to capabilities never before possible, such as advanced industry automation, telemedicine, and drone control. Mission-critical communications depends on traffic prioritization.

53. Beyond the content filtering and video processing already mentioned for wireless networks, 5G networks will take advantage of Multi-access Edge Computing (MEC),[52] a technology that provides a programmable application environment within the radio access network. This approach, standardized by the European Telecommunications Standards Institute (ETSI),[53] processes information to support applications such as augmented reality, distributed AI

[50] For an analysis of this topic, see Rysavy Research, *How "Title II" Net Neutrality Undermines 5G*, Jun. 26, 2019, https://rysavyresearch.files.wordpress.com/2019/06/2019-06-06-how-title-ii-net-neutrality-undermines-5g.pdf.

[51] ITU, *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*, Recommendation M.2083-0, http://www.itu.int/rec/R-REC-M.2083-0-201509-I.

[52] Previously called Mobile Edge Computing.

[53] ETSI, "Multi-access Edge Computing," http://www.etsi.org/technologies-clusters/technologies/multi-access-edge-computing (viewed Oct 24, 2023).

processing, connected cars, and intelligent video processing.[54] MEC is premised on the fact that simply transporting packets between users and centralized sites does not address all use cases. Consider augmented reality (AR), a new application category with tremendous upside that many large companies are now pursuing.[55] AR depends on the superposition of computer data on images that the user is viewing on his or her mobile device; thus, the user experience is vastly improved by minimizing the delay of the computer data. MEC, a capability provided by the ISP, will provide the processing at the edge that enhances the AR experience.[56]

Appendix: Summary of Technical Specifications

This declaration refers to a number of standards and specifications that relate to internet access being an information service. Table 2 summarizes these standards.

Table 2: Summary of Standards and Other Documents That Relate to Internet Access As an Information Service

Technical Standards Impacting Internet	Description
IETF RFC 1034, Domain Names – Concepts and Facilities, 1987.[57]	An introduction to the Domain Name System.

[54] For example, see Verizon, "5G Edge with public MEC," https://www.verizon.com/business/solutions/5g/edge-computing/public-mec/, (viewed Nov. 8, 2023).

[55] See for example Apple's extensive work in this area. Apple, Augmented Reality, https://www.apple.com/augmented-reality/ (viewed Oct 24, 2023).

[56] For further discussion, see IEEE, "How Mobile Edge Networks Can Enhance Augmented Reality," Jun. 2022. https://innovate.ieee.org/innovation-spotlight/how-mobile-edge-networks-can-enhance-augmented-reality/ (viewed Oct. 24, 2023).

[57] https://www.ietf.org/rfc/rfc1034.txt.

Technical Standards Impacting Internet	Description
IETF RFC 1918, Address Allocation for Private Internets.[58]	Use of private addresses to extend the range of internet addresses.
IETF RFC 2475, An Architecture for Differentiated Services.[59]	Means for differentiating traffic flows to enable QoS management.
IETF RFC 6057, Comcast's Protocol-Agnostic Congestion Management System.[60]	Application of QoS to prioritize (acquire, process, transform) packets based on the information they contain.
IETF RFC 7045, Transmission and Processing of IPv6 Extension Headers.[61]	How routers process extension headers in IPv6 for complex routing functions.
IETF RFC 7234, Hypertext Transfer Protocol (HTTP/1.1): Caching.[62]	Standardizes internet content caching.
IETF RFC 7567, IETF Recommendations Regarding Active Queue Management.[63]	Congestion mitigation methods for the internet.
IETF RFC 7754, Technical Considerations for Internet Service Blocking and Filtering, 2016.[64]	Informational purposes document that "examines several technical approaches to Internet blocking and filtering in terms of their alignment with the overall Internet architecture."
Named Data Networking (NDN) and Information Centric Networking (ICN)[65]	In development by IETF and The Named Data Networking Project. This architecture emphasizes information

[58] https://datatracker.ietf.org/doc/html/rfc1918.

[59] https://datatracker.ietf.org/doc/html/rfc2475.

[60] https://datatracker.ietf.org/doc/rfc6057/.

[61] https://tools.ietf.org/html/rfc7045.

[62] https://tools.ietf.org/html/rfc7234.

[63] https://datatracker.ietf.org/doc/html/rfc7567.

[64] https://tools.ietf.org/html/rfc7754.

[65] IETF, Information-Centric Networking, https://datatracker.ietf.org/rg/icnrg/about/. Named Data Networking, https://named-data.net/.

Technical Standards Impacting Internet	Description
	retrieval based on desired content and deemphasizes internet endpoints.
Multi-Access Edge Computing (MEC)[66]	MEC adds information processing at the edge of the network, within the ISP realm, to better support applications such as augmented reality and distributed AI processing. Applicable to 4G and 5G mobile networks. Being standardized by the European Telecommunications Standards Institute (ETSI).

About Rysavy Research

Rysavy Research LLC is a consulting firm that has specialized in computer networking, wireless technology, and mobile computing since 1993. Projects include spectrum and capacity analysis, reports on the evolution of wireless technology, network security assessment, strategic consultations, system design, articles and reports, courses and webcasts, network performance measurements, and working as a testifying expert in patent-litigation. Peter Rysavy has written more than 190 articles and reports. Clients include more than one hundred organizations.

From 2000 to 2016, Peter Rysavy was the executive director of the Wireless Technology Association, an industry organization that evaluated wireless technologies, investigated mobile communications architectures, and promoted wireless-data interoperability.

Peter Rysavy graduated with BSEE and MSEE degrees from Stanford University in 1979. More information is available at https://www.rysavy.com.

[66] Standards http://www.etsi.org/technologies-clusters/technologies/multi-access-edge-computing.