Overview of Broadband Technologies

A BROADBAND INTERNET TECHNICAL ADVISORY GROUP
TECHNICAL WORKING GROUP REPORT

A Uniform Agreement Report

Issued:
01/25/2024

Table of Contents

About the BITAG

The Broadband Internet Technical Advisory Group (BITAG) is a non-profit, multi-stakeholder organization focused on bringing together engineers and technologists in a Technical Working Group (TWG) to develop consensus on how the Internet operates including broadband network management practices and other related technical issues that can affect users' Internet experience, including the impact to and from applications, content and devices that utilize the Internet.

The BITAG's mission includes: (a) educating policymakers on such technical issues; (b) addressing specific technical matters in an effort to minimize related policy disputes; and (c) serving as a sounding board for new ideas and network management practices. Specific TWG functions also may include: (i) identifying "best practices" by broadband providers and other entities; (ii) interpreting and applying "safe harbor" practices; (iii) otherwise providing technical guidance to industry and to the public; and/or (iv) issuing advisory opinions on the technical issues germane to the TWG's mission that may underlie disputes concerning broadband network management practices.

The BITAG Technical Working Group and its individual Committees make decisions through a consensus process, with the corresponding levels of agreement represented on the cover of each report. Each TWG Representative works towards achieving consensus around recommendations their respective organizations support, although even at the highest level of agreement, BITAG consensus does not require that all TWG member organizations agree with each and every sentence of a document. The Chair of each TWG Committee determines if consensus has been reached. In the case there is disagreement within a Committee as to whether there is consensus, BITAG has a voting process with which various levels of agreement may be more formally achieved and indicated. For more information please see the BITAG Technical Working Group Manual, available on the BITAG website at www.bitag.org.

BITAG TWG reports focus primarily on technical issues, especially those with the potential to be construed as anti-competitive, discriminatory, or otherwise motivated by non-technical factors. While the reports may touch on a broad range of questions associated with a particular network management practice, the reports are not intended to address or analyze in a comprehensive fashion the economic, legal, regulatory or public policy issues that the practice may raise. BITAG welcomes public comment. Please feel free to submit comments in writing via email at dsicker@bitag.org.

Executive Summary

Broadband internet access is central to our society and economy. Tens of billions of dollars are now being allocated for construction of new last mile connections - to connect the un-served and under-served - as well as to subsidize consumers' subscription to broadband. But these construction grants and subscription subsidies may not always be informed by up-to-date information concerning the technical capabilities of various last mile network technologies.

Indeed, while some stakeholders may believe there is only one best network technology - fiber to the premises (FTTP) via passive optical networking (PON) - there is actually no one single best last mile technology, given the varied climate, terrain, time needs, and budgets for broadband construction and subsidization. This report aims to inform stakeholders about the various current and near-term capabilities of various network technologies so that they can make better-informed decisions about funding to support more and better broadband, given limited time, limited funds, and other factors and constraints.

The report covers in detail Hybrid Fiber Coaxial (HFC) networks, Digital Subscriber Line (DSL), Fiber to the Premises (FTTP), Licensed and Unlicensed Fixed Wireless Access, Mobile, Low Earth Orbit (LEO) Satellite, and Wi-Fi. Home network technology is also briefly explored, since the home network is such a significant factor affecting end user performance.

Bottom line: there is not one "best" technology - as factors like mobility, terrain, installed base, population density, local regulation, time needs, available construction labor and materials, cost, and so on mean that the answer is "it depends". Across a wide geography of a state or the country, that "best" answer is often a technology-neutral approach that selects a mix of technologies that matches the geography, population density, cost constraints, time constraints, and other factors. For example, a state broadband office may find that for a low number of passings in a very remote state forest can rapidly be served with LEO satellite service, while a small town can be served with a mix of Fixed Wireless, and new FTTP construction in the downtown core. Further, passings directly adjacent to or near existing FTTP and HFC networks may be met by these networks edging out with FTTP (for FTTP and HFC) or HFC.

In addition, last mile broadband internet access network technologies cannot be considered on their own, when the goal is to deliver good performance to users, the middle mile and backbone networks' performance is equally important. They determine how well-connected an ISP network is to destination networks that host popular sites and applications (such as video streaming), content delivery networks (CDNs), cloud providers, gaming networks, and others. It is worth noting that there continues to be a trend where content is moving closer to the last mile and that there are opportunities for innovation in these parts of the network that directly and significantly impact the quality of broadband for users.

Finally, it is important to bear in mind that speed (throughput) and (idle) latency are not the sole factors that affect broadband quality - working latency (network responsiveness) is emerging as a key performance factor. BITAG explored that topic extensively in our recent Latency Explained paper [1]. Reliability, consistency, and security are also emerging as key factors - such as routing security as explored recently by the BITAG [2].

1 Introduction

Access to broadband internet access has become a crucial component of modern life, as it is required for education, work, healthcare, and other essential activities. The need for reliable, fast, and responsive internet access has never been more important, particularly in the wake of the COVID-19 pandemic, which prompted many people to work, learn, and socialize from home [3]. To meet the connectivity needs of consumers and businesses, there are a variety of broadband access technologies available, each with its own strengths and limitations. Understanding the technical capabilities and applicability of these technologies can be challenging, particularly for stakeholders who need to make informed decisions about broadband deployment and funding.

This report is motivated by the historically significant tens of billions of dollars being invested by local, state, and federal governments to subsidize subscription costs of broadband [4], and the construction of new broadband networks to connect the unserved and under-served [5], [6]. However, many policymakers that set the criteria for subsidies and grants and the grant-makers that award grants may not be aware of the wide range of broadband access technologies now available or may not be fully aware of the current capabilities of those technologies. This report is intended to inform these audiences so that broadband subsidies and grants will be grounded in accurate, current information concerning various access technologies. The report also attempts to make clear that there is not one "best" technology - factors like mobility, terrain, population density, local regulation, time needs, available construction labor and materials, cost, and other variables means that the answer is "it depends".

We aim to provide a broad overview of current and emergent broadband access technologies. The report does not recommend a particular technology but instead explains the capability and applicability of each technology. This report also shows that there is no one 'best' technology; consumers, businesses, and communities have a wide variety of budgets, requirements, interests, and other needs. This report should appeal to a diverse audience, ranging from policymakers, regulators, and lawmakers to academic researchers, network engineers, historians, and many others.

The report includes an overview of the architecture, network protocols, infrastructure, customer equipment, operation, standards, and future roadmap for each of the following broadband access technologies: Hybrid Fiber Coaxial (HFC), Digital Subscriber Line (DSL), Fiber (primarily Passive Optical Networks, PON), Fixed Wireless Access (FWA - using licensed spectrum - and other fixed wireless - using unlicensed spectrum), Mobile, and Low Earth Orbit (LEO) Satellite.

To present a balanced view of the various technologies, the report will examine key factors that should be considered when choosing a broadband technology, including location, performance, cost, upgradability, and sustainability. We will highlight some of the current misconceptions regarding the technical capabilities of various broadband access technologies, with the goal of providing accurate and up-to-date information. It should be noted that last mile architectures cannot be evaluated in isolation and the entire Internet ecosystem between the communication source and destination must be analyzed to fully understand the impacts of the deployed broadband technology.

In this report we provide a thorough and objective analysis of various factors related to broadband access, drawing on available research and measured data analytics. It is important to note that different technologies may use different measurement and monitoring platforms, making direct comparisons difficult. Nonetheless, our goal is to offer a fair and impartial overview of broadband access technologies, with a focus on assisting stakeholders in making informed decisions based on their individual needs and circumstances. In addition, we identify gaps and potential areas for improvement that may benefit from further research funding.

2 Technology Overview for Main Broadband Access Networks

2.1 Hybrid Fiber-Coaxial (HFC)

2.1.1 Overview

Cable modem technology is used to provide Internet service over hybrid fiber-coaxial (HFC) networks. HFC networks (or, "cable networks") were initially designed for one-way distribution of broadcast television programming, but were upgraded in the 1990s to allow for two-way communication. This enabled new services, such as video-on-demand, voice telephony and broadband internet access, to be provided by cable network operators. Hybrid Fiber Coaxial (HFC) networks have witnessed substantial technological progress, emerging as a cornerstone in contemporary connectivity. Notably, they now support a 10 Gbps link rate with 1 ms Round-Trip Time (RTT) capability. These advancements signify a crucial stride in data transfer capabilities and underscore the network's efficiency in handling real-time communications. These technological advancements address the evolving demands of our connected world, providing a robust framework for enhanced connectivity and communication

The term hybrid fiber-coaxial refers to the physical cabling that connects a customer to the network operator's facility. A fiber optic link is used for a major portion of the distance from the operator facility to the customer, and then metallic coaxial cable (typically copper or aluminum) is used for the remainder of the distance. A device called a fiber node performs the optical-to-electrical conversion between the fiber portion of the path and the coaxial portion.

Like passive optical networks (PON) and wireless networks, HFC networks are a "shared medium" network, where a set of customers (a service group) share the bandwidth of a single fiber link. In the early years of cable broadband service, the majority of the bandwidth shared by a service group was dedicated to carrying linear television programming, and only a small fraction of the total network bandwidth was used to provide internet access. Over time, cable network operators have continuously improved the internet capabilities of the network by allocating a larger portion of the network bandwidth to internet access, and upgrading network equipment to enable more total network bandwidth. Operators have reduced service group sizes down to the range of 100 to 200 customers in a service group, enabling more capacity for each user. Operators are continuously deploying newer generations of cable modem technology, and moving fiber nodes closer and closer to customers (so the coaxial portion of the path is shorter). This ensures leveraging the technology by reducing the serving group size and improving the system performance. At this point, HFC networks are predominantly fiber with the fiber portion greatly exceeding the coax portion in terms of distance covered.

2.1.2 Network Architecture, Protocols and Standards

HFC network architectures are typically described as tree topologies where a cable operator's facility (e.g., headend) is connected to each fiber node via one or more fiber optic cables, and the fiber node is connected to the households via a branching structure constructed from rigid (hardline) coaxial cable (commonly 0.5" to 0.875" in diameter), with splitters creating branches that then pass each household in the service group (Figure 1). At each house, a "tap" on the coaxial line allows a smaller diameter "drop cable" to be connected to a point of entry at the side of the house. Along the coaxial portion of the path, amplifiers are included periodically to boost the signal levels to counteract attenuation. In some areas, this cabling (including equipment such as amplifiers and taps) is attached to utility poles, and in other areas it is buried underground.

At each subscriber household, interior coaxial drop cables connect the point of entry to the customer equipment. At the root end of this tree structure (i.e. the headend or hub location) is a cable modem termination system (CMTS) which is the equipment responsible for providing internet service over the HFC network. At the leaf ends of this tree structure (i.e. the customer house) is a cable modem (CM). The CMTS and the CMs in the service group implement a version of the Data-Over-Cable Service Interface Specifications (DOCSIS) which define how user traffic is encoded for transmission over the HFC network. CableLabs, its member companies (cable network operators globally,) and cable equipment manufacturers jointly draft and maintain the DOCSIS specification. Since its first publication in 1996, the specifications have undergone a series of updates that have extended the capabilities of the technology. Each version provides backward compatibility with the previous versions to enable network operators to incrementally upgrade equipment in their networks.

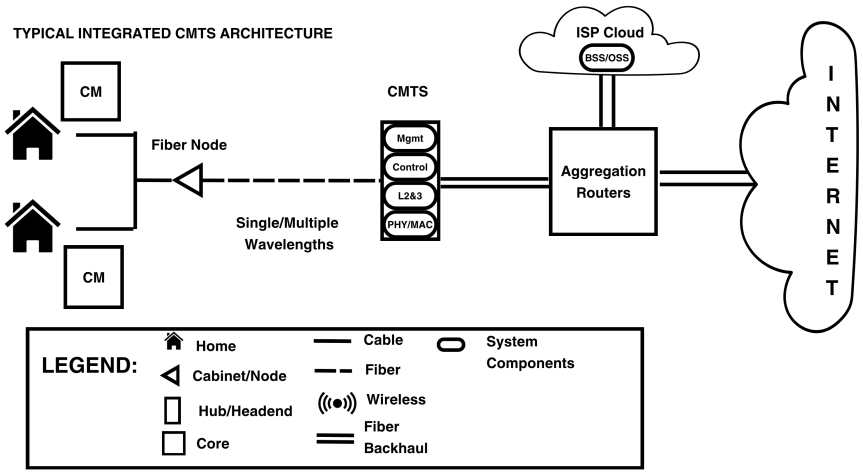

Figure 1: Centralized HFC Network Architecture

Table 1: DOCSIS Specifications Network Architecture

Version	Highlights	Max Speed Down	Max Speed Up	Latency	First Issue Date
DOCSIS 1.0	Initial cable broadband technology, high speed internet access	40 Mbps	10 Mbps	10ms – 1000ms	1996
DOCSIS 1.1	Voice over IP service, gaming, streaming	40 Mbps	10 Mbps	10ms – 1000ms	1999
DOCSIS 2.0	Higher upstream speed, capacity for symmetric services	40 Mbps	30 Mbps	10ms – 1000ms	2001
DOCSIS 3.0	Greatly enhances capacity, channel bonding, IPv6	1 Gbps	200 Mbps	10ms – 100ms	2006
DOCSIS 3.1	Capacity and efficiency progression, OFDM, wideband channel, AQM	10 Gbps	1-2 Gbps	10ms – 100ms	2013
Low Latency DOCSIS 3.1	Dual-queue networking, L4S	10 Gbps	1-2 Gbps	1ms – 10ms	2019
DOCSIS 4.0	Symmetrical streaming and increased upload speeds	10 Gbps	6 Gbps	1ms – 10ms	2019

The DOCSIS protocols utilize frequency-division duplex (FDD) communication, where the “downstream” data (toward the customer) is carried in one or more channels in one frequency band (typically 108 MHz – 1.2 GHz), and the “upstream” data (from the customer) is carried in one or more channels in another frequency band (typically 5 MHz – 42 MHz and extending to 85 MHz). The most recent version, DOCSIS 4.0, extends the spectrum up to 1.8 GHz, allows for a much more flexible allocation of the spectrum between the upstream and downstream bands, and also supports “full-duplex” (FDX) operation (simultaneous transmission in both directions) on a portion of the band, enabling symmetrical multi-gigabit services.

2.1.3 Future Roadmap

HFC networks are continuously evolving as new technologies are developed and new market demands and customer needs arise.
Some of the main evolutions that are underway, and which will continue in the future are:

- Distributed CCAP Architecture. This architecture moves all DOCSIS and digital video physical-layer functionality (modulation, error correction, etc.) that traditionally exists in the headend or hub to a Remote PHY Device (RPD) that is installed in each fiber node. This new architecture provides several key benefits including digital fiber between node and headend, higher RF efficiency, symmetrical multi-gigabit services, ability to implement a virtualized DOCSIS infrastructure using NFV (Network Function Virtualization) and SDN (Software Defined Networks), and the reduction in facility power and space requirements.

- Fiber Deep. Deploying fiber nodes (RPDs) much closer to households to reduce or eliminate the need for coaxial amplifiers, reduce network power consumption, shrink service group sizes, and increase capacity by minimizing RF interference.

- Increased upstream capacity. Allocating more of the coaxial cable bandwidth to upstream transmissions and/or utilizing FDX and the deployment of DOCSIS 4.0 equipment.

- Increased downstream capacity. Extending the useable frequencies on the coaxial cable for downstream transmissions up to 1.8 GHz, and the deployment of DOCSIS 4.0 equipment.

- Software based network optimization techniques. These include actively monitoring the plant conditions, to predict and resolve service degradations (Proactive Network Maintenance), and increasing network capacity and reliability by creating optimized modulation profiles for each customer (Profile Management Application).

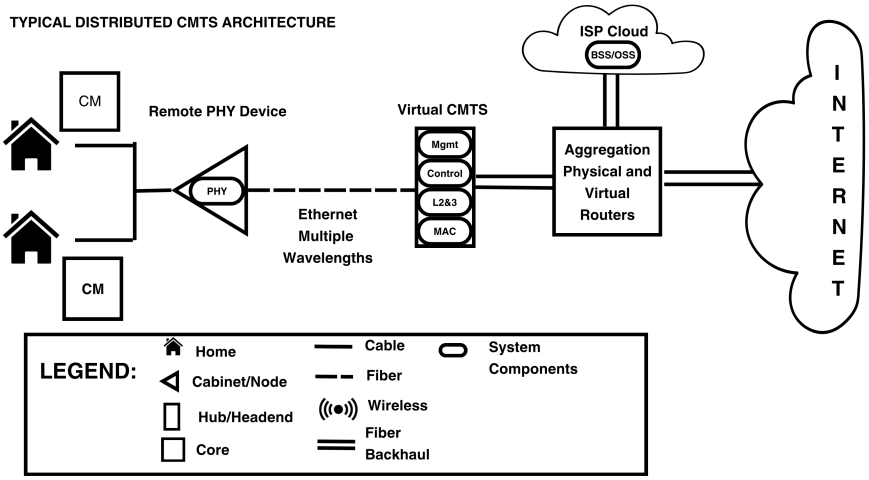

Figure 2: Distributed HFC Access Architecture

2.2 Digital Subscriber Line (DSL)

2.2.1 Overview

Digital subscriber line (DSL) is a family of technologies that use twisted-pair copper telephone lines to transmit high-speed digital data to homes and businesses. The increased available downstream bandwidth make it a widely available and cost-effective alternative to dial-up Internet access. DSL technology is known for reliable connectivity and cost-effective deployment and is a mature technology that has been deployed for over twenty-five years. It continues to be deployed where access technologies such as fiber are cost prohibitive. DSL is available in most areas where there is a telephone network. However, the speed of the connection may vary depending on the distance between the customer and the digital subscriber line access multiplexer (DSLAM).

DSL works by splitting the frequencies used over a standard telephone line into two bands: a low-frequency band for carrying voice traffic and a high-frequency band for carrying data traffic. This allows DSL to transmit data at high speeds without interfering with the telephone service. Signals attenuate over distances, so DSL standards indicate the speed potential up to a maximum distance.

2.2.2 Network Architecture, Protocols and Standards

A typical DSL system consists of a DSL modem at the customer's premises and a DSL access multiplexer (DSLAM) at the telecommunication company's central office or remote terminal. Locating the DSLAM closer to customers at a remote terminal (Fiber to the Node) serving hundreds of homes allows for higher bandwidth speeds. The DSL modem converts digital data into an analog signal that can be transmitted over the telephone line. The DSLAM converts the analog signal back into digital data, aggregates traffic data from multiple modems and forwards it to the Internet. DSLAM traffic is then switched to a Broadband Remote Access Server (BRAS) where end-user traffic is aggregated and routed across the ISP network to the Internet. The BRAS is the first IP hop to the internet from the customer and serves as the interface for authentication, authorization and accounting systems.

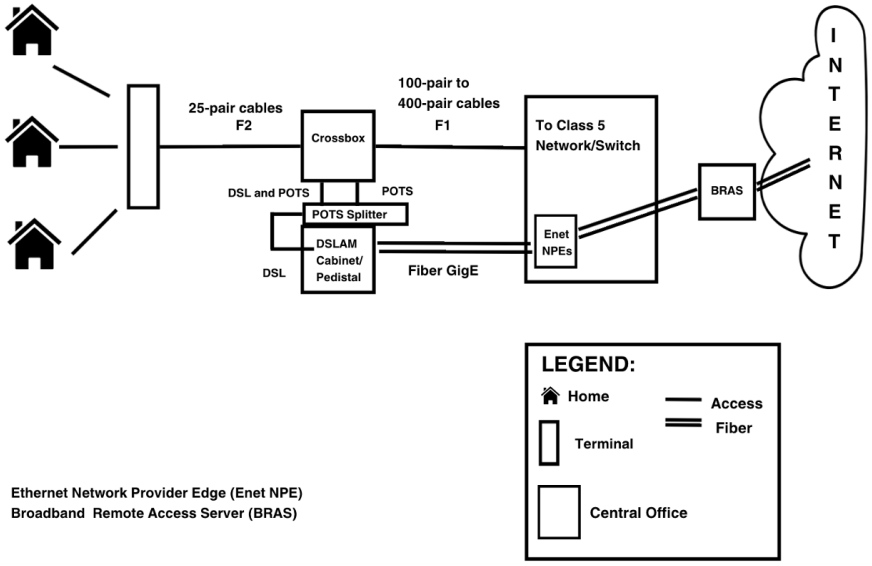

Figure 3: DSL Network Architecture

DSL uses a variety of protocols to transmit data. The most common protocols are:

Symmetric Digital Subscriber Line (SDSL): SDSL provides symmetric speeds, with upstream and downstream speeds that are equal. In general, SDSL is an older standard, with bitrates that are lower than those provided

by asymmetric DSL. Therefore, it is not used as often.

Asymmetric Digital Subscriber Line (ADSL): ADSL is the most common type of DSL. It provides asymmetric speeds, with upstream speeds that are typically a fraction of downstream speeds. There are several ADSL standards.

Very High Bitrate Digital Subscriber Line (VDSL): VDSL is a more recent technology than ADSL that provides much faster speeds than ADSL or SDSL and requires short range links. Again, there are several VDSL standards.

The speed of a DSL connection depends on several factors, including the type of DSL technology, the distance between the customer and the DSLAM, and the quality of the twisted-pair copper lines. SDSL typically offers symmetric speeds of up to 1.5 Mbps. ADSL and VDSL have maximum speeds which vary depending on the standard. ADSL2+ has a maximum of 24 Mbps downstream and a maximum of 3.3 Mbps upstream on a single twisted pair. VDSL Annex Q (mode 35b) can offer downstream speeds of up to 300 Mbps and upstream speeds of up to 100 Mbps on a single twisted pair of very short length.

DSL is standardized by the International Telecommunication Union (ITU). The ITU has published a number of standards for DSL, including:

Table 2: DSL Specifications

DSL Type	Description	Standard	Max Speed Down	Max Speed Up	First Issue Date
ANSI T1.413	asymmetric digital subscriber line	T1.413 Issue 2	8 Mbps	1 Mbps	1998
G.DMT	asymmetric digital subscriber line	G.992.1	8 Mbps	1 Mbps	1999
G.lite	asymmetric digital subscriber line	G.992.2	1.5 Mbps	512 kbps	1999
ADSL2	asymmetric digital subscriber line 2	G.992.3	12 Mbps	3.5 Mbps	2003
ADSL2+	asymmetric digital subscriber line 2 – Extended bandwidth	G.992.5	24 Mbps	3.3 Mbps	2003
Bonded ADSL2+	bonded digital subscriber line	G.998.2	50 Mbps	5 Mbps	2003
VDSL2 (8a)	very high speed digital subscriber line 2 - 8 MHz	G.993.2	50 Mbps	16 Mbps	2006
VDSL2 (12a)	very high speed digital subscriber line 2 - 12 MHz	G.993.2	66 Mbps	22 Mbps	2006
VDSL2 (17a)	very high speed digital subscriber line 2 - 17 MHz	G.993.2	120 Mbps	50 Mbps	2006
VDSL2 (35b)	very high speed digital subscriber line 2 - 35 MHz	G.993.2 Amd 1	300 Mbps	100 Mbps	2006
Bonded VDSL2 (17a)	bonded very high speed digital subscriber line 2	G.998.2	240 Mbps	100 Mbps	2006
Vectoring	Self-FEXT cancellation (vectoring) for use with VDSL2 transceivers	G.993.5 (G.vector)	120 Mbps (17a)	50 Mbps (17a)	2010
G.fast	fast access to subscriber terminals	G.9700, G.9701	1.5 Gbps aggregate (212 MHz)		2014

These values are theoretical maximums and may not be realizable in field deployments. The actual speed obtained is highly dependent on the condition of the twisted-pair line, so estimated distances are quite variable. For the highest speed services, the length of the pair often must be less than 250 meters. For downstream speeds of roughly 10 Mbps, a distance of 2,000 meters is reasonable.

As mentioned in the table above, some of these technologies may be bonded, which uses two copper twisted-pair lines to provide a speed which is roughly double that of a single pair.

2.2.3 Future Roadmap

G.fast and VDSL2 (35b) G993.2 Amd 1 are the current state of the art standards. G.fast at 212 Mhz can achieve stable 1Gbps x 1Gbps speeds out to 500 feet using the technique cDTA (Collective Data Timing Allocation). This allows the technology to dynamically utilize all the available frequencies downstream and upstream as it detects customer usage requests and adjusts which direction to transmit for the best result. G.fast was approved in 2014 and revised in 2019. The standard MG.fast (G.9711) at 424 Mhz, with an approval process that started in 2020, should be able to deliver 5Gbps speeds, however attenuation starts at very short distances (100 ft).

2.3 Fiber to the Premises (FTTP)

2.3.1 Overview

Passive Optical Networks (PON) is the most common Fiber to the Premises (FTTP) technology for the residential market and has been widely deployed for several years across the globe. PON access is a point-to-multipoint (P2MP) technology, meaning a single optical signal from a service provider's equipment is split across multiple points along the fiber path for the most efficient usage of fiber rather than individual fibers between service providers facilities to the customer, commonly known as a point-to-point (P2P) type architecture. P2MP fiber architecture cuts back on the number of optical electronics needed so that only a single optic is necessary at the provider facilities to serve multiple customers instead of one fiber path for each customer when using (P2P) topologies. This reduces costs and saves on power consumption.

On a P2MP network, PON can provide a large range of services to many users. The optical signal uses an unpowered splitter to "passively" transmit to different users for network access. By design, a PON uses no active electronics that require power in the field, making it compelling to service providers operational teams as the associated power expense and potential failure points are reduced. PONs can transmit data in both the downstream and upstream with symmetrical speeds, while allowing for different speed tiers and services to consumers.

PON provides the most efficient option for the use of fiber in the providers' footprint and is thus the most cost and operationally effective. The network architecture consists of an Optical Distribution Network (ODN), which is a single fiber from the service provider's facility that is split into individual fibers that go to the consumer location. From an architecture perspective, there are options for deploying FTTP, such as a centralized deployment option where the single fiber and optical signal are generated from the service provider central offices and then split near the service group area. Another option is to use more of a distributed access architecture to generate the PON signal deeper into the network from a cabinet or hardened strand mount device so that it is closer to the service group area. Also, there are options with the implementation of the splitters within the ODN for a single centralized split with a single splitter, or perhaps cascading splitters if more efficient for the service group geography.

2.3.2 Network Architecture, Protocols and Standards

For PON, one of the primary factors that dictate the ODN network architecture is a design principle known as optical budget. The power of the optical signal degenerates and lowers over distance. With PON ODNs there is a maximum optical budget for the entirety of the PON and the design must consider power loss over the distance across fibers and there is also optical power insertion loss, which is the loss with splitters or fiber splice points. These factors are taken into account when considering the ODN architecture and how to deploy it. Based on these parameters, PON service groups range from 16 to 128 endpoints (ONTs). Depending upon where the PON terminates, the overall system is known as fiber to the curb (FTTC), fiber to the building (FTTB), or for residential service fiber to the premises (FTTP).

There are two main PON technology families: Ethernet Passive Optical Network (EPON) and Gigabit Passive Optical Network (GPON). These protocols use multiplexing techniques (i.e. Time Division Multiplexing and Wavelength Division Multiplexing) to transmit service flow data over the optical fiber. EPON is based upon IEEE 802.3 Ethernet packet switching technology that was modified to support point-to-multipoint connectivity while GPON is a transport protocol, wherein data is carried over an agnostic synchronous

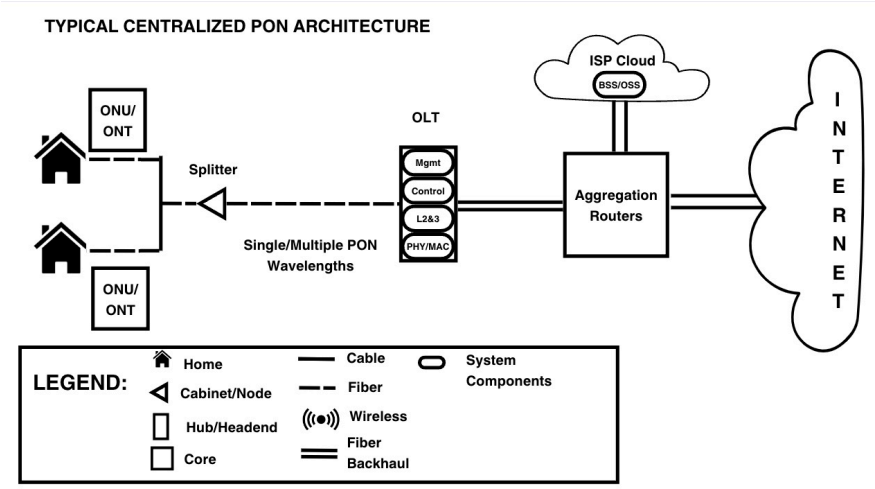

Figure 4: Centralized PON Architecture

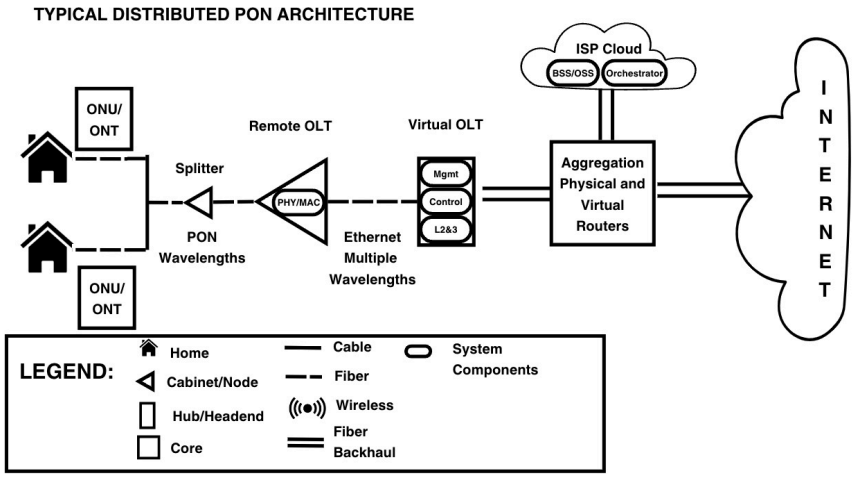

Figure 5: Distributed PON Architecture

framing structure from end to end. Optical Line Terminal (OLT) is the service provider's endpoint that controls the data transmission from/to the customer equipment (ONT/ONU) by assigning unique service flow identifiers for each customer's service (e.g., data, voice, video) and transmitting them using multiplexing techniques. These technologies are equally capable, with Telcos and MSOs preferring one or the other due to legacy compatibility issues [7].

Traditional PON architectures relied on centralized PON setups, employing specialized OLTs that integrated data, control, and management planes. Modern distributed architectures offer superior efficiency, automation, and cost-effectiveness. Technologies like Software-Defined Networking (SDN), Network Function Virtualization (NFV), and cloudification, enable operators to disaggregate data, control, and management planes. This empowers a programmable, scalable, and agile PON network infrastructure.

PON technology was originally proposed by British Telecommunications in 1987. Then in 1995, the International Telecommunication Union (ITU) standardized specifications for the delivery and communication across fiber networks. As with any communication technology, protocols must be agreed upon for proper implementation. The two primary standards bodies in the communication industry are the ITU and the Institute of Electrical and Electronics Engineers (IEEE). As technology with optical signals improves, standards evolve to accommodate and implement in the market.

Table 3: PON Specifications

PON Type	Description	Standards	Max Speed Down	Max Speed Up	First Issue Date
EPON	PON with Ethernet framing	IEEE 802.3ah	1.25 Gbps	1.25 Gbps	2004
10G-EPON	Extensions to EPON with backward compatibility	IEEE 802.3av	10 Gbps	10 Gbps	2009
50G-EPON	Backward compatible with 10G EPON	IEEE 802.3ca	25/50 Gbps	50 Gbps	2020
BPON	PON with framing based on ATM (Asynchronous Transfer Mode)	ITU G.983	622 Mbps	622 Mbps	2005
GPON	Framing based on GPON encapsulation method - Backward compatible with BPON	ITU G.984	2.5 Gbps	1.25 Mbps	2008
XG-PON	Co-existence with GPON through WDM (Wavelength Division Multiplexing)	ITU G.987	10 Gbps	2.5 Gbps	2012
NG-PON2	TWDM (Time and Wavelength Division Multiplexing) – Co-existence with previous standards through WDM	ITU G.989	40 Gbps	10 Gbps	2015
XGS-PON	Backward compatible with XG-PON, co-existence with GPON through WDM	ITU G.9807	10 Gbps	10 Gbps	2016
HS-PON	Backward compatible with 10G GPON	ITU G.9804	50 Gbps	50Gbps	2021

2.3.3 Future Roadmap

The life cycle and current adoption of PON has begun using the 10Gbps technology of XGS-PON and 10G-EPON, where EPON standards have been ratified earlier for higher rates. 10G-EPON was the first symmetrical 10G PON technology standardized and deployed worldwide. Today, XGS-PON replaces lower rate GPON deployments in many markets. 10G technology will continue to be deployed during this current decade with the next evolution beginning to occur in the 2030s. The future of PON is 25Gbps/50Gbps with development gains towards a 100Gbps capable PON.

2.4 Fixed wireless (licensed and unlicensed)

2.4.1 Overview

Fixed wireless has been used for decades to deliver connectivity into areas that have little or no existing wireline infrastructure and as redundant network to back up traditional wired networks. Recently, fixed wireless technology has evolved into a compelling alternative to traditional wireline broadband in areas where cost, right of way and regulatory obstruction have stifled access to broadband. Mobile network operators are able to leverage much of their existing infrastructure to offer fixed wireless on licensed spectrum within their current footprints and there is a large group of independent Wireless Internet Service Providers (WISPs) that primarily use unlicensed spectrum to deliver broadband into unserved and underserved locations. Fixed wireless is often used as part of a hybrid model with fiber networks to extend coverage outside of a wireline footprint or as a regulatory bypass around areas with right of way or competitive roadblocks that prevent wireline deployment.

2.4.2 Network Architecture, Protocols and Standards

Fixed wireless access has several differences compared to mobile cellular broadband. Mobile cellular services utilize a model in which interlocking areas of service coverage are created where an end-user device (such as a mobile phone) can connect with any tower in the coverage area. With FWA, each subscriber has a client device at their location with a fixed, high gain antenna pointed back to a specific access point on the provider network. This simplifies the network architecture since there is no need for the signaling overhead that mobility requires. Fixed, high gain antennas also have the potential for a higher signal-to-noise ratio, which is key to high speeds, low latency and reliable connectivity.

Fixed wireless networks use PTP, PTMP or meshed connections from an access point to a fixed subscriber or client location.

1) Point to point (PTP) utilizes dedicated radios on both sides of a connection with focused antennas on either side. This method is typically used for connections between towers for middle-mile backhaul but can also be used to provide dedicated bandwidth for locations - typically commercial applications - where a shared medium of access is not appropriate. Since PTP is a dedicated connection, it can be customized to meet capacity, reliability and latency objectives and can deliver symmetrical speeds in both upload and download directions.

2) Point to Multipoint (PTMP) utilizes an access point at the provider side of the connection which can deliver service to several client radios. This method is used for delivering service into a wide area using shared medium in the same way that PON and DOCSIS network deployments are shared. Time slots are allocated for all of the client devices on the system and are allocated to meet the user demand. Most user demand is asymmetric - there is more demand for download than upload (need citation) - so PTMP networks are typically optimized for download speeds. PTMP network capacity can be upgraded by increasing channel sizes if more spectrum is available, implementing additional access points at a location with more focused antennas or adding additional cells in areas of higher demand. PTMP is the lowest cost deployment model and is more suited to areas with lower density or a need to cover a large area at a lower cost.

3) Mesh wireless networks utilize access points that also have a backhaul component built in. A mesh network will have at least one point within the footprint that has a direct connection to a middle mile

network where outside access can be injected. From that point, other members of the mesh network can join in using their backhaul component while delivering access to customers on the access point component. This model is suitable for limited size applications such as neighborhoods or subdivisions, but will run into scaling issues as more clients are added and backhaul capacities reach saturation.

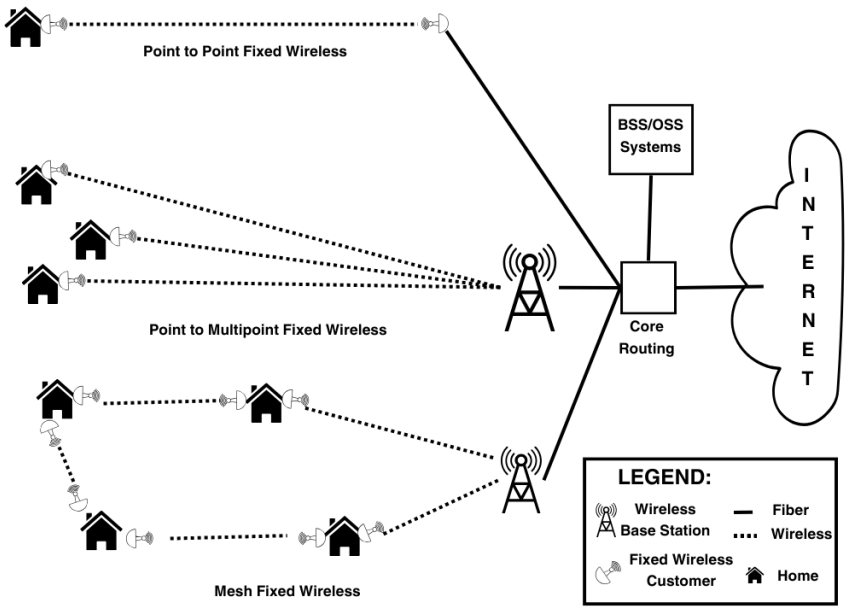

Figure 6: Fixed Wireless Network Architecture

Several spectrum bands are utilized for fixed wireless deployment, both licensed and unlicensed. Each spectrum band has a set of unique characteristics but follows some common rules:

- Lower frequency spectrum has a longer potential coverage range and will go through clutter or terrain obstructions better than higher frequencies.

- Higher frequency spectrum has a smaller coverage area, but can be used to deploy higher speeds through smaller cells and frequency reuse.
- Very high frequencies – such as millimeter wave – have extremely small coverage areas, but utilize very large channel sizes and can reach gigabit speeds to end users.
- Unlicensed spectrum is readily available for any provider. Deployments must be designed to accept interference and congestion within unlicensed spectrum bands can reduce overall network capacity and reliability depending on the type of deployment and equipment used.
- Licensed spectrum for point to multipoint utilization is limited to providers with spectrum licenses. Since the provider has control over the spectrum, there is no interference from other users of the spectrum within the license area. This allows the use of higher power and modulations within the frequency boundaries.

- Lightly licensed spectrum is available to operators that obtain an access license and utilize equipment with the ability to access a spectrum database that determines availability in an area. This spectrum uses priority access grants (PALs) for government and commercial users but also has a general access component that is available for users without PALs.

There is no single spectrum/deployment model for fixed wireless broadband deployment. Each operator can choose the spectrum utilized by availability, terrain, type of deployment and the amount of spectrum available.

Fixed wireless can also be deployed using mobile band spectrum and can coexist with mobile users on the same network.

There are several established models for deployment of fixed wireless. These models often coexist within the same network and can be utilized to meet different requirements according to end-user demand, spectrum access, vertical infrastructure availability and economics.

Macrocells are the most common deployment model in rural areas. A typical microcell consists of access points on a tower or rooftop feeding out over a large geographic area with a radius of two to 20 miles. This model uses less infrastructure to cover more locations but will run into capacity constraints due to the distance from the users, mounting capacity at the tower and limitations on the use of spectrum at a single point. Macrocells primarily utilize lower frequency spectrum usage to maximize coverage.

Microcells are intended to cover much smaller areas than macrocells, typically under two miles in diameter. Microcell deployments are common in suburban and urban areas and developments with higher density of locations served. The smaller coverage area compared to macrocells means that more access points – and therefore more capacity -can be deployed into the same geographic area. Microcells can also utilize frequency reuse and antenna coverage to get more capacity out of limited spectrum resources. The shorter distance between the tower and the end user enables higher signal to noise ratios and use of higher frequency spectrum bands which leads to improved network performance and reliability. The microcell deployment model will scale to higher capacities and performance than macrocells, but can be exponentially more expensive to deploy over the same geographic area.

Femtocells and picocells are designed to cover very small geographic areas less than a few hundred feet. These are not commonly used for outdoor fixed wireless deployments but can sometimes be found in dense urban areas and commonly rely on millimeter wave spectrum to deliver up to gigabit speeds within their limited footprints.

Compared to other broadband delivery types, there is a wide variety of standards based and proprietary platforms for fixed wireless broadband delivery.

Fixed wireless deployment using licensed and mobile network spectrum is almost entirely done using 3GPP standard platforms. The terms of use for licensed spectrum impose stringent technical standards on platforms so innovation is consolidated into the standard based systems. 4G LTE and 5G fixed wireless performance is very similar to mobile broadband with an expectation of improved speed and reliability through use of higher gain antennas.

Early unlicensed fixed wireless deployments were often adapted from indoor access points for outdoor use and operated in the 900 MHz, 2.4 GHz and 5 GHz spectrum ranges. Although manufacturers still use 802.11 standard chipsets in some fixed wireless broadband platforms, several features have been added to the systems to improve performance in outdoor deployments such as schedulers, GPS synchronization, extended distance parameters and noise filtering/cancellation. Although many of these platforms use similar chipsets, the platforms are typically proprietary and not compatible with each other.

2.4.3 Future Roadmap

Recently the introduction of Next Generation Fixed Wireless Access (ngFWA) platforms for use in unlicensed spectrum have initiated the use of advanced noise cancellation methods to deliver performance comparable or superior to licensed spectrum platforms. Advances in 5G/6G and other mobile based standards will migrate to fixed wireless and lead to further speed and capacity increases.

Table 4: Unlicensed FWA Specifications

Platform Type	Description	Standards	Max Speed Down	Max Speed Up	First Issue Date
802.11 DSSS	2.4 GHz 802.11 based Outdoor FWA using Direct Sequence	IEEE 802.11	1 Mbps	1 Mbps	1998
802.11 FHSS	2.4 GHz 802.11 based Outdoor FWA using Frequency Hopping	IEEE 802.11	2 Mbps	2 Mbps	1998
802.11b DSSS	2.4 GHz 802.11b based Outdoor FWA using Direct Sequence	IEEE 802.11b	11 Mbps	11 Mbps	1999
802.11a OFDM	5.8 GHz 802.11a based Outdoor FWA using OFDM	IEEE 802.11a	54 Mbps	54 Mbps	1999
Motorola Canopy	Proprietary Motorola FWA system using FM modulation	None	10 Mbps	10 Mbps	2001
802.11n MIMO-OFDM	2.4 GHz and 5 GHz 802.11n based Outdoor FWA using MIMO-OFDM	IEEE 802.11n	600 Mbps	600 Mbps	2008
802.11ac MUMIMO-OFDM	2.4 GHz and 5 GHz 802.11ac based Outdoor FWA using MUMIMO-OFDM	IEEE 802.11ac	1.6 Gbps	1.6 Gbps	2013
802.11ax MUMIMO-OFDMA	2.4 GHz and 5 GHz 802.11ax based Outdoor FWA using MUMIMO-OFDMA	IEEE 802.11ax	2.3 Gbps	2.3 Gbps	2021
Tarana ng-FWA	Proprietary Tarana FWA system with noise cancelling systems	None	2.4 Gbps	2.4 Gbps	2021

2.5 Mobile Wireless

2.5.1 Overview

Every decade the mobility industry performs a major upgrade to its wireless infrastructure. The 2000s were dominated by 3G, while 4G was used in the last decade in the 2010s. Each cellular generation has been significantly faster than the one before. 4G can currently reach top speeds of up to 100 Mbps, though real-world performance is generally no more than 35 Mbps. 5G has the potential to be 100 times faster than 4G, with a top theoretical speed around 20 Gbps and current, real-world speeds from 50 Mbps to 3 Gbps.

5G enables the mobile wireless networks to handle significantly higher data rates and volumes of data, while improving two other very key capabilities: a) latency/ reliability and b) connection density. The classes of applications enabled by 5G are broadly divided into three different categories based on their requirements:

• eMBB (enhanced mobile broadband): This encompasses applications such as 4K video, augmented reality and tactile internet. These applications typically require very high bandwidth and reasonably low latency. Throughput in Gbps is targeted.

• Massive MTC (machine type communication): This is general category that includes connected devices such as meters, sensors, home security, etc. While most of these applications are not bandwidth intensive they require deep coverage and ability to support battery life up to 10 years.

• Critical MTC: This category of applications includes machine to machine communication that requires ultra-low latency and extreme reliability. Some examples are vehicle to vehicle communications, industrial

automation and robotics, etc.

With such a diversity of requirements, the true challenge for 5G is to be a flexible radio technology and a single network that can efficiently support a vast variety of applications. North America is a leader in the uptake of wireless 5G connections. 5G penetration of the population in the North American market is approaching 32 percent. Overall, a total of 215 million 5G connections are projected to come from North America in 2023, bolstered by strong 5G smartphone shipments in the US. According to Ericsson, total global mobile data traffic reached 118 exabytes (EB) per month by the end of 2022 and is projected to nearly quadruple to reach 325 EB per month in 2028, with 20 GB for North America by the end of 2022 and increasing to 58 GB at end of 2028.

2.5.2 Network Architecture, Protocols and Standards

While traditional mobile implementations consist of centralized and consolidated data, management and control functionality, the new mobile technology benefits from distributed architectures. Virtualization of network elements is a key functionality required to ensure that the 5G network architecture is scalable yet agile at the same time. Concepts such as NFV and SDN will allow the mobile industry to move away from the model where every box in the network has a dedicated role. Instead of deploying a large core network it is possible to shift the core and the content closer to the edge of the network by virtualizing the elements of the core network. Moving the content to edge and utilizing things like mobile edge computing are going to be critical for some of the use cases such as critical MTC that require ultra-low latency. By virtualizing some of the components of the RAN (Radio Access Network), especially the functions at the higher layer, the same efficiency of scale and agility can be obtained in the RAN deployment as well. NFV also allows the industry to implement the concept of network slicing. A network slice is essentially an instantiation of the network that runs on top of a pool of hardware. This enables operators to optimize each slice for delivering a type of service e.g. eMBB, fixed broadband, massive MTC etc.

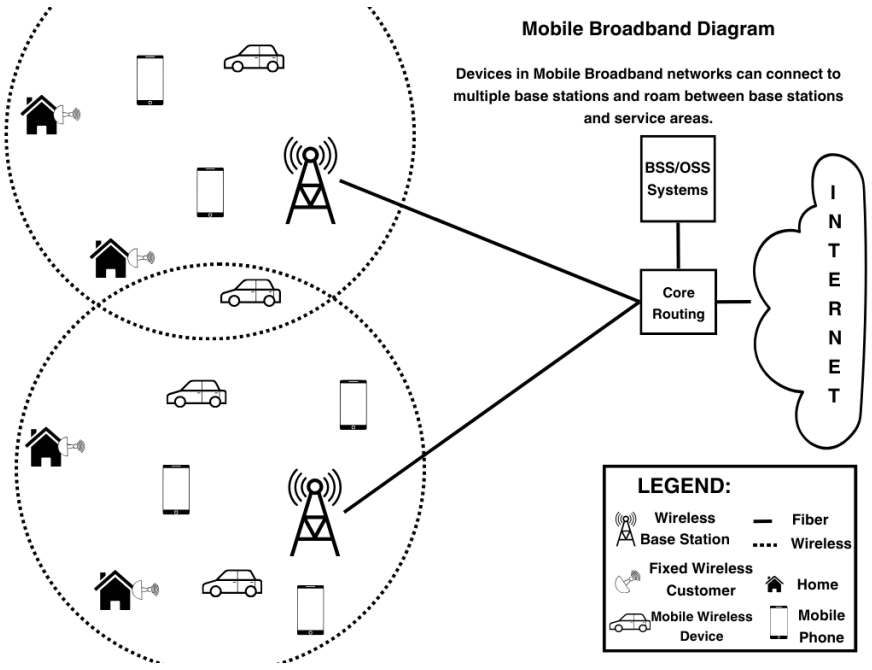

Figure 7: Mobile Wireless Network Architecture

There are several standards bodies and industry forums that continue to work on defining standards pertaining to 5G and 6G. Of these, the two most important organizations are ITU-R and 3GPP. ITU-R is responsible for setting the requirements that a technology must meet in order to qualify as IMT 2020 compliant.

3GPP on the other hand is responsible for developing further releases and the protocol specifications for 5G

and 6G.

Table 5: Mobile Wireless Specifications

ITU-R IMT (Publication date)	Technology	3GPP Standards (Release date)	Operating Frequency Band	Theoretical Peak DL Rate*
IMT-2000 / 3G (May 2000)	UMTS (FDD &TDD), HSPA LTE	UTRA-WCDMA/ LTE (Rel 99) (Mar 2000)	< ~1 GHz	~40 Mbps
IMT-Advanced / 4G (January 2012)	LTE	LTE-Advanced/ LTE Advanced Pro (Rel 10) (Mar 2011)	< ~10 GHz	~1 Gbps
IMT-2020 / 5G (February 2021)	NR & LTE	5G/ 5G Advanced (Rel 15/16) (June 2018/Sept 2020)	< ~75 GHz	~20 Gbps
IMT-2030 / 6G (est 1H2030)	TBD	6G (Rel TBD) (est 2028/2029)	< ~100 GHz & ~100GHz+	est >1000 Gbps

*Relative theoretical peak DL Data Rate trends that represent possible examples applicable for specific scenarios, while other values may also be considered

Mobile Network Evolution from LTE to 5G

Existing LTE network (core + RAN) was the starting point for 5G deployment. Therefore, in the early phases of 5G deployments, a very important question begged itself as to how to evolve the current network to integrate 5G services and the 5G network to interwork with the current platform.

The preferred architecture required the industry to evolve the current LTE RAN to interoperate with the 5G core network. This implies that 5G services will not only be available while the subscriber is on the 5G RAN, but also on the LTE RAN. This is also the best way to ensure that value of the current LTE investment continues in the 5G era by being able to deliver these new capabilities even on the LTE network. The legacy LTE Evolved Packet Core (EPC) will continue to support the legacy devices and legacy services that are currently being offered on the 4G LTE network. Another very important milestone for 5G is the network densification and deployment of small cells. Higher frequencies provide two key benefits that are essential to a 5G network; a) wider spectrum which can support higher data rate, and b) ability to extract high capacity and spectral efficiency [1]. The transition to higher frequencies and wider bandwidth requires a reduction in the cell radius for optimal performance, which makes small cells a natural evolutionary path.

2.5.3 Future Roadmap

Explosive growth in data traffic for mobile networks fueled by applications such as ultra-high definition video, augmented reality, and tactile internet will drive the industry toward the next generation of mobile wireless networks. 5G is also expected to enable a host of new machine centric applications such as IoT, self-driving cars, industrial automation, and eHealth.

With new, flexible radio access technologies and protocols in multiple bands 5G enables extremely high data rates, massive IoT with low cost/low power devices, and extremely low latencies. Such capabilities are necessary to achieve the vision of pervasive connectivity and anytime, anywhere services on any device. On a different front, it is very important for governments around the world to continue auction spectrum for

[1]Spectral Efficiency is the amount of throughput that can be supported per Hz of spectrum. In other words, this is the efficacy of the system in its spectrum utilization.

licensed commercial use and develop a robust pipeline for licensed spectrum for 5G. This will ensure that operators can continue to address data growth and new 5G applications.

2.6 Low Earth Orbit (LEO) Satellite

2.6.1 Overview

Satellites have been providing Internet access for several decades using geosynchronous ("GEO" or "GSO") satellites orbiting the Earth at around 22,236 miles (36,000 km). While these GEO satellites have provided Internet access solutions for remote regions, there is a high degree of latency (or "lag") with the communication to and from the satellites that makes them impractical for communication requirements such as video calls, online gaming, and virtual worlds. These deployments do not provide sufficient broadband performance to meet the needs of users today, with the satellite industry shifting to new technologies.

A new generation of systems using Low Earth Orbit (LEO) satellites have evolved that circle around the earth at an altitude of between 124 miles (200 km) and 1,243 miles (2,000km) [8]. Because these satellites are closer to the Earth, they have a limited coverage area and need a higher number of satellites for complete Earth coverage. A LEO system is referred to as a "constellation" that will have satellites in one or more "shells" at different altitudes. The Starlink system from SpaceX, for example, currently has over 5,500 satellites in orbit, with plans to potentially launch as many as 30,000 satellites. Other examples of LEO systems include Eutelsat OneWeb and the Amazon Kuiper satellite constellations, which are at varying stages of operational deployment.

2.6.2 Network Architecture, Protocols and Standards

The customer premise equipment typically consists of an externally-located phased array panel antenna and is usually combined with a unit that has a Wi-Fi router. The network infrastructure on the access side consists of a constellation of LEO satellites, with corresponding ground stations or gateways. The ground stations are often located near high-bandwidth internet exchange points (IXPs). These are normally data centers where internet service providers locate their core routing equipment and have good connectivity to the internet. Many of the new LEO constellations use inter-satellite lasers (ISLs) between satellites to allow routing of network traffic across the constellation until it can connect to a ground station. This enables connectivity for users who are far away from any local ground stations.

A LEO system, such as Starlink, uses the three main components of the end user terminal, the satellite constellation [9], and the ground station to deliver internet connectivity. The end-user speed varies according to the time and usage of subscribers. According to measurements from Ookla for Q1 2023 the average Starlink download speed in the U.S.A. was 66.59 Mbps and the uplink at 7.74 Mbps [10] with 62ms latency. The user terminals use traditional Ku- and Ka- microwave bands, that operate in the 12-18 and 26.5-49 GHz bands. The dish uses phased array antennas, and electronically controlled dish angles to keep the ground to space link operational.

The internet access provided over a Starlink connection supports all the regular internet standards and protocols that you would expect of any other type of connection. The routing and network protocols used between the satellites, ground stations, and customer equipment used by Starlink are proprietary and not yet well understood. The in-home router provided by Starlink uses Wi-Fi Technology IEEE 802.11a/b/g/n/ac standards, with a chipset supporting Wi-Fi 5, a Dual Band radio supporting 3 x 3 MIMO and WPA2 security.

The advantage of a LEO system is that the coverage is ubiquitous. The ideal use cases for the systems are to bring connectivity to remote regions, airplanes, ships, and mobile vehicles. They are also valuable for disaster response or other situations where existing infrastructure is damaged or unavailable. The fact that terrestrial infrastructure such as fiber optic cable or cell sites are not needed to provide service to the end user is a unique advantage. A disadvantage is that LEO systems, while faster than GEO satellites, are still not as fast as terrestrial systems in terms of available bandwidth and latency. Also, there are capacity limitations in terms of the number of subscribers that can be supported in each geographical area. However, there are situations where it is impractical to connect a user via terrestrial systems due to cost and time to rollout, where a LEO system such as Starlink is a good solution.

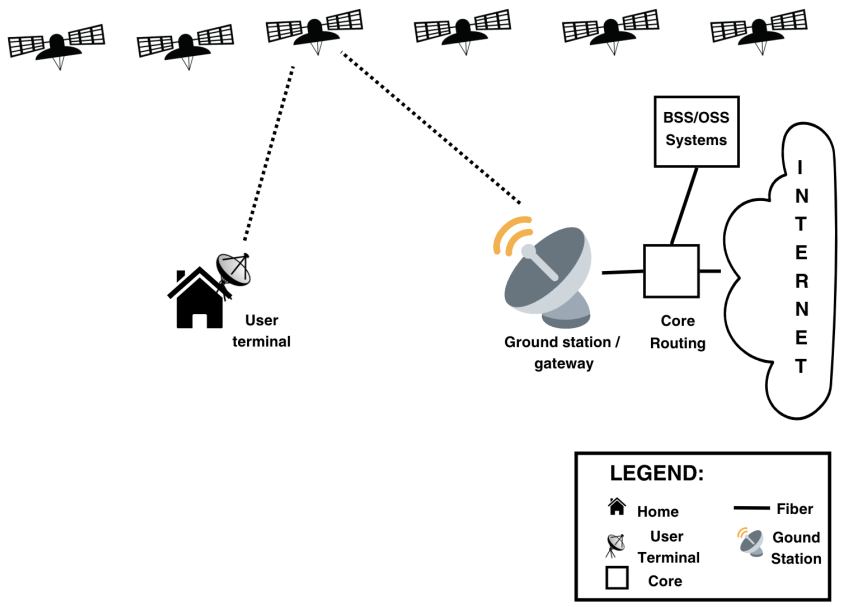

Figure 8: LEO Satellite Broadband Network Architecture

2.6.3 Future Roadmap

Over the next 2-5 years, 50,000 - 90,000 satellites are planned for launch into low Earth orbit, expanding coverage, enabling faster connections, and providing competition for connectivity. SpaceX is continuing to build out their first Starlink constellation planned to be 4,408 satellites. They have started to deploy satellites into their second "Gen2" constellation that will initially have 7,500 satellites with goals to grow to over 30,000 satellites. Eutelsat OneWeb has launched over 600 satellites and plans to launch more. Amazon's Project Kuiper is planning a constellation of 3,200 satellites that it hopes to start launching in 2024 to compete directly with Starlink. The Chinese government is working to launch its Guangwang constellation that is planned to have around 13,000 satellites. The European Union is also proposing an IRIS2 constellation. Many other companies are seeking to provide space-based Internet services. Meanwhile, the traditional GEO satellite providers are seeking to expand their options, and a few companies also have offerings in medium Earth orbit (MEO) between 1243 miles (2,000 km) and 22,236 miles (36,000 km). Some companies are now pursuing "multi-orbit" strategies that combine connectivity between satellites in LEO, MEO, and/or GEO. There are still many questions around the affordability and availability of these LEO-based solutions. As outlined in a report from the Internet Society, there are also concerns around the sustainability of all these separate businesses, environmental and climate impacts, space debris, and impacts on astronomy.

2.7 Wi-Fi

2.7.1 Overview

Wi-Fi is the predominant form of wireless broadband connectivity within homes, offices, and small businesses. The Wi-Fi Alliance® (WFA) commissioned a report in 2021 that estimated Wi-Fi's market value would be $4.9 trillion by 2025[11]. In addition to Wi-Fi's use indoors, it is used by some rural and metropolitan ISPs as a last-hop residential connection to the Internet. These ISPs are often nonprofit organizations formed by the local community, though there are examples of for-profit corporations providing Internet connectivity using Wi-Fi.

This section will discuss Wi-Fi in the context of its use in providing public (free or subscription-based) Internet access. Use of Wi-Fi inside the customer premises is discussed in [Technology Overview for Premises

Networks]. Private hotspots (such as those in coffee shops, hotels, and airports) are not discussed in detail in this report. 3GPP (the organization that defines the 5G and 6G mobile wireless standards) has also defined standards for use of 802.11 technology as a component of a 3GPP network (where end user devices connect to an 802.11 hotspot and authenticate with the same 3GPP core used by cellular wireless technologies). This capability and architecture are often used by mobile carriers to provide hotspots.

2.7.2 Network Architecture, Protocols and Standards

Network architectures used to supply public Internet access via Wi-Fi vary widely. Factors include who controls the network (e.g., local government, for-profit company, individuals in the community), the goals of the network (e.g., provide access to residential areas, to public spaces such as parks and libraries, to people in business districts, or to traffic lights, parking meters, government-controlled cameras, and other capabilities of the municipality), the density of population in the community, funding (sources and amount), and more. There are numerous examples of these Wi-Fi networks in the US and abroad [12] [13].

Some key distinguishing features among the various architectures are how connecting devices are authenticated, use of repeaters, whether Wi-Fi or wired technologies are used to provide backhaul links, and how the network is controlled and operated.

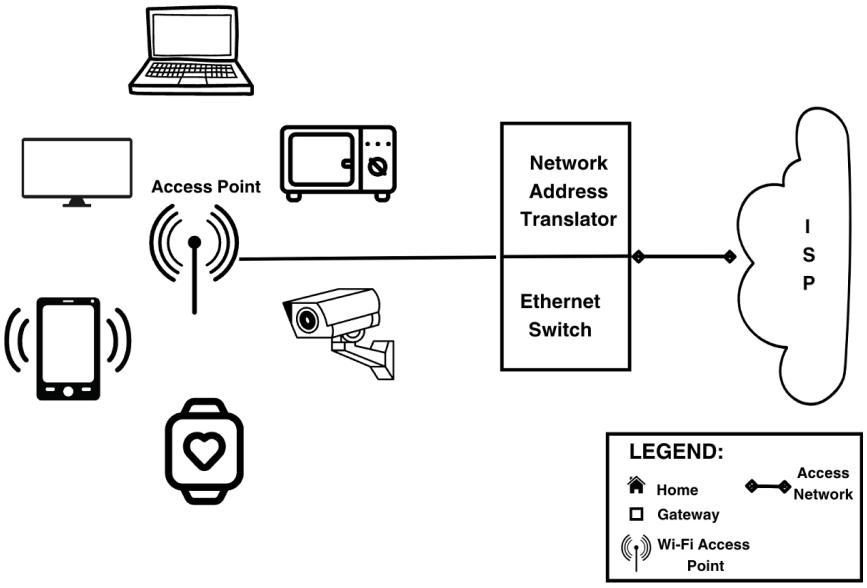

Figure 9: Wi-Fi Network Architecture

The WFA provides certifications for what it calls “Wi-Fi Protected Access” (WPA)[14]. It is currently up to version 3 of this. These certifications are based on IEEE specifications. WPA certifications exist for what WFA calls “Personal” and “Enterprise” usages. The Personal mechanism makes use of a shared secret (passphrase) that is used by all devices connecting to that access point. While this is primarily designed for use by home networks, it is also used by some smaller community-based Wi-Fi networks. The Enterprise mechanism authenticates devices using a centralized authentication database that Access Points (APs) communicate with to determine whether a device should be granted access.

Another authentication mechanism is called “Captive Portal”. This mechanism operates at the Internet Protocol (IP) layer. In this model, the AP uses no security mechanism at the physical or networking layer. Instead, it redirects all IP traffic from the device to a web interface where the user must supply some form of credentials (or policy acknowledgement) before it is granted access to the Internet. This mechanism is very common in hotel networks and some hotspot implementations, and is also used in some municipal networks.

Repeaters are simple devices that relay Wi-Fi signals between devices attached to them and a central Access Point. They are a relatively inexpensive method to "boost" or "extend" Wi-Fi signals.

It is also possible to extend a Wi-Fi network by using additional Access Points that are all configured with the same network identifier and authentication information (e.g., a WPA passphrase). These networks may connect Wi-Fi Access points or Repeaters to other Access Points (APs) or Repeaters to create a network that provides linkage for all devices back to a centralized point that has access to the Internet. Some networks will also use wired technologies (Ethernet, powerline, fiber, Multimedia over Coax Alliance) for backhaul, and some use a combination of Wi-Fi and wired technologies. These Wi-Fi access networks are generally centrally managed. This includes management of authentication mechanisms and configuration of backhaul links. The term "mesh" refers to a network of Access Points with routing capability that are connected to multiple other such Access Points and make their own routing decisions through the use of a routing protocol. There is no centralized control in a true mesh network. Such mesh networks are extremely rare and uncommon.

The software used to centrally manage the devices in a Wi-Fi access network is generally proprietary. Therefore, the Access Points in any particular network tend to be supplied from a single vendor. An exception to this has been networks that make use of APs whose code has been replaced with OpenWRT, and open source AP operating systems [15]. OpenWRT can be loaded on a variety of APs.

Table 6: Wi-Fi Specifications Centralized HFC

"Wi-Fi Certified" program	Based on IEEE standard	Description	Commonly achieved throughput	Nominal Peak Rate	Radio Frequency Used (GHz)	Certification Publication date
802.11b	802.11b	Uses phase-shift keying (PSK) modulation.	2-3 Mbps	11 Mbps	2.4	2000
802.11a	802.11a	Uses orthogonal frequency-division multiplexing (OFDM) modulation.	20 Mbps	54 Mbps	5	2002
802.11g	802.11g	Uses OFDM modulation, like 802.11a	20 Mbps	54 Mbps	2.4	2003
4	802.11n	Uses multiple-input, multiple-output (MIMO) OFDM modulation (64-QAM); introduced use of multiple antennas	40-50 Mbps	600 Mbps	2.4/5	2008
5	802.11ac	Uses multi-user (MU) MIMO OFDM access (OFDMA) modulation (256-QAM)	100+ Mbps	6,933 Mbps	5	2014
6	802.11ax	Uses MU-MIMO OFDMA (1024-QAM)	100+ Mbps	9,608 Mbps	2.4/5	2019
6E	802.11ax	Separate certification for products operating in 6 GHz spectrum.	100+ Mbps	9,608 Mbps	2.4/5/6	2020
7	802.11be	Uses MU-MIMO OFDMA (4096-QAM)	TBD	(est) 46,120 Mbps	2.4/5/6	Est 2024

The original Wi-Fi standard, IEEE SA 802.11, was approved in 1997 after seven years of development. There was no certification program for this standard (to ensure interoperability), its speeds were slow, and there was no significant deployment. It has been followed by a series of updates signified by a postfix letter or pair of letters from 802.11a to 802.11bk (so far.) The most current rolled up (incorporating all approved updates to that point in time) publication of the 802.11 standard is 802.11-2020[16]. Since that publication work

has continued to produce amendments 802.11ax-2021 through the preliminary P802.11bk. Newer standards typically consist of improvements to security, privacy, access to new frequency bands, wider channels, and data transfer efficiency improvements.

Note that due to licensed uses of the 6 GHz spectrum in the US, 6E products are not allowed to be used at standard power in the 6 GHz spectrum without support for an Automated Frequency Coordination (AFC) system. WFA announced in August 2023 a new commercial subsidiary to test AFC compliance.[17]

In addition to the standards from IEEE, specifications have been created by other organizations to provide additional utility and ease of installation. W-Fi Alliance has defined several related to setting up a Wi-Fi AP and network of APs. To better understand the performance of Wi-Fi devices, Broadband Forum has created a testing program to allow ISPs to compare the performance of APs they supply to their customers. There are many trade-offs as to which performance criteria are important in any particular deployment depending on building materials, whether vertical coverage is needed (multi-story premises), density of competing AP networks, and more.

2.7.3 Future Roadmap

Original Wi-Fi was meant to support simple scenarios, such as laptop computers accessing shared printers and supermarket scanners accessing shared databases. Today's Wi-Fi supports high device densities and large numbers of people in shared spaces such as sports arenas. Hence, the most recent major advance in the standard, 802.11ax, focuses on efficiency and performance improvements. Future IEEE standards continue this general trend by permitting aggregation of frequency bands and the use of sub-channels to enable simultaneous data transfer by multiple nodes. Wider channels that will support greater bandwidth are also part of the roadmap[18].

3 Technology Overview for Home Networks

Consumers often have difficulty determining whether a problem with their Internet performance is a result of the ISP's access network or their home network (or some other aspect of the end-to-end service). This section is intended to provide a high-level overview of some of the technologies and architectures (and advancements in technologies) of consumer and small business premises networks (primarily home networks) that are being driven by the need to get very high speed broadband access reliably to the end devices (laptops, smartphones, sensors, cameras. etc.) on these home and business networks.

The home Local Area Network (LAN) architectures described in this section can be used with any of the broadband access technologies of the preceding sections. Many consumers and small businesses choose to use the equipment supplied by their ISP, the devices an ISP offers (and supports) can have a big impact on their customers' experience, but it is not a requirement that consumers use ISP-supplied equipment to extend or operate their premises networks. There are a variety of options available to consumers for devices the consumer can self-manage as well as devices that are purchased or leased as part of a managed service.

3.1 Wi-Fi

A general overview as well as information on Wi-Fi standards, protocols and future roadmap are in the above section on Wi-Fi as an access technology.

3.1.1 Network Architecture and Protocols

Wi-Fi is primarily a hub-and-spoke system in which every device (or "node") connects to a central access point (AP) for access to other nodes, including Internet gateways. It also has a direct connection mode, known as Wi-Fi Direct, that enables nodes to communicate with each other without passing through the AP. The 802.11 standards have also defined mechanisms for mesh networking through constellations of APs.

3.1.2 Infrastructure and Customer Equipment

In a typical configuration the Wi-Fi access point is combined with a Network Address Translator (NAT), a Dynamic Host Control Protocol (DHCP) server, and an Ethernet switch. This combination is commonly known as a home router. Devices that combine home router functionality with cable or DSL modems or fiber optical network terminals are also common.

3.1.3 Wi-Fi

Several Wi-Fi AP vendors offer bundles of multiple APs which they refer to as a "mesh" system. In general, APs marketed as "mesh" typically have a single main AP that is connected to the Internet, and one or more satellite APs. The satellite APs typically have a single backhaul link that connects it either directly to the main AP or to one of the other satellite APs. Sometimes a wired technology such as Ethernet is used to provide the backhaul to the main AP. Range extenders or repeaters are simplified satellite APs that do not support IP routing.

Most consumer AP "mesh" systems have satellite APs establishing a single backhaul connection that is intended to provide the best (highest bandwidth, lowest latency, fewest hops) connection back to the main AP. This is usually accomplished by having the satellite APs provide the main AP with various Wi-Fi statistics. The main AP can then provide some direction to the satellite APs. The WFA EasyMesh specification defines a protocol for providing statistics from satellites to the main AP, by extending the IEEE 1905 protocol for this purpose.

In order to provide even greater control and intelligence (without requiring the main AP to have expensive computing capabilities), there are also Application Service Providers (ASP) who offer management of premises Wi-Fi networks as a service. In these cases, the main AP sends the statistics it collects to the ASP's servers, where the ASP can use more complex algorithms (than the main AP could) to determine how best to configure the premises network. Some providers offer a proprietary "mesh" system of APs that sends a variety of information from the premises network to its servers on the Internet. Unless the user invokes Privacy Mode, this data includes information on the precise location and identifiers of all devices inside the premises, including the movement of mobile devices, DNS requests, browser fingerprints, UNPnP traffic, and more. Some providers list the various data they collect and what the Privacy Mode limits. Some other ASPs provide management of Wi-Fi premises networks using certified WFA EasyMesh devices and the Broadband Forum User Services Protocol.

Modern APs that make use of the 6 GHz spectrum are often capable of Gigabit speeds. Where the speed of the access network is significantly higher than the speed of the LAN network, bufferbloat can be an issue. This topic is discussed further in [1].

See 2.7.2 for a discussion of the various authentication methods that Wi-Fi may support. Inside consumer and small business premises networks, the primary mechanism is a shared passphrase. The current certification for this available from WFA is WPA3-Personal.

3.2 Ethernet

Many newly constructed homes are being built with structured wiring of CAT5 or even CAT6 to provide Gigabit Ethernet connectivity to various points inside the premises. Most people then connect access points or ethernet capable devices to these and use the Ethernet for backhaul to the central AP.

3.3 Powerline

Powerline has never gained great traction, but is widely available for use in creating a wired network inside a premises. While it is sometimes used to directly connect end devices, it is also sometimes used for backhaul of Wi-Fi APs.

4 Operations

Regardless of the specific technology, a network's health hinges on proper maintenance and monitoring. Network Management Systems (NMS) serve a primary role in the network collecting vital performance and usage metrics. These tools are versatile, deployed across various access technologies to provide operators with insights into network performance, usage statistics, and potential issues as well as network and service planning.

Recent advancements in Software-Defined Networking (SDN), Network Function Virtualization (NFV), and cloudification have revolutionized network operations. Automation and programmability have become key components in streamlining maintenance and monitoring tasks. SDN allows for centralized control and management of network resources, enabling dynamic adjustments to meet changing demands. NFV virtualizes network functions, reducing reliance on dedicated hardware. Cloudification leverages cloud infrastructure to enhance scalability and flexibility.

Through automation and programmability, routine tasks are executed efficiently, reducing human error and accelerating response times to network events. These technologies enhance the overall agility and responsiveness of network operations. Convergence platforms are being developed to deploy and operate common components and functionality over multiple access technologies. This framework allows operators to apply common service platforms over different access networks. While all benefit from advancements in SDN, NFV, and cloudification, the specific nuances of each network type require tailored strategies for seamless operations. Each technology presents unique characteristics, necessitating specialized tools and approaches for maintenance and monitoring. This includes regular inspections and maintenance of physical maintenance components, firmware audits, power, capacity and connectivity management, environmental control and other maintenance procedures, some of which are listed below.

· Hybrid Fiber-Coaxial (HFC): HFC networks combine fiber optic and coaxial cables. Signal strength meters and spectrum analyzers are used to maintain signal integrity. Amplifiers and nodes are vital for signal distribution, ensuring consistent quality across the network.

· Passive Optical Networks (PON): PONs leverage fiber optics for data transmission, ensuring high bandwidth capabilities. Monitoring tools like optical power meters and OTDRs are crucial for assessing signal levels and troubleshooting fiber paths.

· Digital Subscriber Line (DSL): Monitoring tools such as line testers and DSL performance analyzers are used to assess signal quality, noise levels, and data rates. Regular line maintenance and periodic testing are essential to ensure optimal DSL performance.

· Fixed Wireless Networks: Fixed wireless relies on wireless links and base stations. Spectrum analyzers and wireless link testers ensure reliable signal strength and interference management. These tools are essential for maintaining stable connections in fixed wireless setups.

· Mobile Networks: Cellular towers and base stations form the backbone of mobile networks. Drive test equipment and network analyzers aid in assessing signal quality, coverage, and performance. This data is crucial for optimizing tower placement and ensuring seamless connectivity for mobile users.

· Low Earth Orbit (LEO) Satellite Networks: LEO satellites provide global coverage. Tracking and monitoring equipment manage satellite communication, ensuring seamless connectivity. Precise tracking of satellite positions is crucial for efficient data transmission across the network.

· Wi-Fi Networks: Wi-Fi networks use access points and routers for local wireless connectivity. Wi-Fi analyzers and network monitoring software optimize signal strength and identify interference for robust wireless connections. These tools are instrumental in creating reliable and high-performing Wi-Fi networks for end-users.

5 Performance

There are many possible ways to measure the performance of a broadband access network. There are many other metrics beyond throughput that can be used to measure the performance of a broadband access network. These include latency, jitter, packet loss, and others. We define and detail some of these metrics below. Beyond these network-level performance metrics, other relevant performance metrics include application-level performance metrics, including those specific to particular applications (e.g., video conferencing, video streaming, gaming).

5.1 Network-Level Performance Metrics

5.1.1 Throughput

The throughput of a broadband access network can be measured in both the upstream and downstream directions. Many network test web sites still report this metric as "speed" which is an ambiguous term [1]. The most common metric is the throughput of the access network, which is typically measured in megabits per second (Mbps) or gigabits per second (Gbps)—specifically, with units of bits transferred per unit time. Downstream throughput is typically quite relevant for user experience, given that most applications are asymmetric, with more data flowing downstream from servers to client applications on a user's access network. Various applications, including file transfer, use more upstream capacity, making upstream throughput a relevant metric to consider. Upstream throughput can also be relevant in the case of networks that have excessive buffering at a bottleneck point, which can lead to bufferbloat (exhibited by high end-to-end latency) and generally poor application performance.

5.1.2 Latency and Jitter

An increasingly relevant network performance metric is latency, which can also be measured in a variety of ways. Whereas throughput refers to the amount of data that can be transferred across a link (or path) in a particular unit of time, latency refers to the amount of time that it takes for a packet to travel across a link (or path). Latency is typically measured in milliseconds (ms). Latency is often measured as round-trip time (RTT), which is the amount of time that it takes for a packet to travel from a source to a destination and back again. Latency can also be measured as one-way delay, which is the amount of time that it takes for a packet to travel from a source to a destination.

When measuring latency, the choice of source and destination are pertinent to the ultimate metric being reported. For example, the source vantage point for latency is typically a client device on an access network; the destination, on the other hand, can vary. One possibility for a destination endpoint is a server on the wide-area network, somewhere at a location in the network. A common wide-area endpoint might be a server in an exchange point or co-location facility, for example. Measuring latency to such a server has some advantages and disadvantages. On the one hand, such a measurement can yield a better understanding of what latency looks like across a "typical" end-to-end path that might traverse several independently operated networks between the client and an Internet server, thus more closely mimicking the experience of a user who is accessing a service on the Internet (e.g., a video streaming service, a website, etc.).

On the other hand, such a measurement may not shed insight into the performance of the access network itself, or other specific locations along the path that may introduce latency (e.g., the interconnect, the network hosting the server). Other network paths, such as the path between the client and their chosen Domain Name System (DNS) resolver, may also be relevant to the user experience. For this reason, it may be appropriate to measure (and report on) latency to multiple network destinations, including various wide-area destinations (both local and further afield), to specific services (e.g., Google, Netflix), as well as to specific DNS resolvers. Measuring the latency of specific services, such as DNS query latency, can also be appropriate, particularly given the variable performance of emerging encrypted DNS resolvers.

Jitter refers to the variability in latency, and can be measured in several ways, including the standard deviation of latency measurements, or a moving average of pairwise differences between latency measurements. Jitter is an important consideration because the variability in latency can affect user experience, particularly for real-time applications that require consistent, predictable latency along a path. High jitter can result

in effects such as large gaps between the arrival of data, resulting in irregular playback of audio or video, inconsistent responsiveness in gaming applications and so forth. A common solution to high jitter is to "smooth" packet arrivals with a client buffer (in the case of video, a playout buffer), but doing so can result in large buffers that ultimately result in high latency, particularly under periods of high traffic load and congestion—leading to high latency under load, a phenomenon we discuss next.

5.1.3 Latency Under Load (Responsiveness)

Another important consideration is how network latency responds to additional traffic load. Specifically, network latency may increase in response to increased traffic volumes on a network link or path. One primary contributor to this phenomenon is bufferbloat, which is the result of excessive buffering at a bottleneck point in a network. Bufferbloat can lead to high latency and jitter, which can negatively impact the performance of interactive applications, such as video conferencing, gaming, and voice over IP (VoIP). Bufferbloat can also lead to poor performance of other applications, such as web browsing, which can be sensitive to latency.

Latency under load is also sometimes referred to as operational latency. Other industry terms for this phenomenon sometimes refer to responsiveness (which is essentially the inverse of latency under load). Occasionally, quality of experience (QoE) is referred to in the context of latency under load, although QoE more often refers to application performance [1].

5.2 Application Performance Metrics

Although lower-level performance metrics can be useful for understanding the basic operation and functioning of the network, as speeds increase and applications become more complex, these lower-level metrics often do not yield a good indication of user experience. For example, a network may have high throughput, yet most applications do not have particularly high throughput demands. For example, a video conference application may require no more than a few megabits per second. On the other hand, a combination of factors, from latency to packet loss, may contribute to a poor user experience. Due to the complexity of the network environment and the architecture of these applications, the best way to understand the performance of these applications under certain network conditions is simply to measure the performance directly.

In such cases, it may be appropriate to design application-specific performance tests, such as a test for a specific video conference or gaming application. Direct measurement in such cases has certain advantages, as specialized tests can often offer a more clear picture of what a user is likely to experience when using that particular application. On the other hand, such tests can be complicated to design and deploy, as they can sometimes require intimate knowledge of how a particular application performs, instrumentation of a proprietary client, access to proprietary and service-specific endpoints, and so forth.

For this reason, sometimes application performance monitoring is performed through "passive" measurements—specifically, measurements that capture ongoing application session traffic and indirectly infer application performance. One such example technology is that which can capture packet traces and infer characteristics such as the frame rate and resolution of streaming video (either on demand or video conference traffic). Such an approach has the advantage of being able to directly measure user experience, for an actual, ongoing user session. The approach, however, is not without its own complications: this approach requires capture of network traffic which can lead to both systems challenges and privacy concerns. Furthermore, with the increasing use of encryption, such approaches may not be able to directly observe application performance characteristics, and may have to rely on indirect inference through statistical machine learning approaches.

5.3 Measuring Network and Application Performance

One challenge that network providers face is measuring this litany of performance metrics, particularly continually over time, and across the expanse of the network. Unfortunately, many leading methods for measuring performance face obsolescence, particularly as access network speeds have increased over the past decade.

A particular area of concern is the use of client-based speed tests to measure (and generalize) network performance. Past research has demonstrated that client-based speed tests face a host of shortcomings,

including but not limited to poor spatial and temporal sampling that reflect biased samples, as well as infrastructure and test implementations that reflect the bottlenecks of client devices, server infrastructure, or other factors that have little to do with network performance.

Recent research has performed the first direct comparison of speed test methods and tools and has discovered that results of these tests can vary not only between successive tests of the same tool, but also between different tools that purport to measure the same network, under the same conditions. This research has demonstrated that some of the speed tests that regulators have relied on in the past face fundamental flaws, from bugs in software to inadequately provisioned infrastructure, that may result in under-reporting of network throughput.

More concerning than the shortcomings of these tools, however, is the fact that "speed" is increasingly an inadequate proxy for the user experience. As access network throughputs continue to increase, the limiting factors for user experience are increasingly the other metrics discussed above (particularly latency and operational latency)—which are not typically the focus of existing speed test tools (or studies that rely on these tests and data).

This evolving landscape argues for a more holistic approach to network performance measurement. Specifically, recent research has demonstrated the value in relying not just on a single speed test (which may reflect biases or characteristics of that test or deployment), but rather a framework that facilitates performing multiple independent tests from the same vantage point that purports to measure the same metric. Furthermore, there is clear value to frameworks that provide the capability to perform not just multiple speed tests, but also latency and other measurements. Emerging open-source measurement frameworks such as Netrics allow network operators to integrate (and schedule) multiple tests across a range of performance metrics. The Netrics framework does not implement (or advocate for) any single test, although the open-source distribution does provide a range of test implementations (including, for example, multiple throughput tests, a latency under load test, a DNS latency test, and a video conference application test). The main value of such a framework is the ease of integrating multiple existing tests and scheduling them in ways that do not interfere with one another—a particularly important capability given the wide range of both metrics and test implementations and the need to both measure many different network metrics and cross-validate different test measurements for any given metric.

6 Cost and Deployment

6.1 Cost and Deployment Practicalities Necessitate a Diversity in Broadband Access Technologies

NTIA's $42.5 billion Broadband Equity, Access, and Deployment (BEAD) program will result in an unprecedented, highly significant deployment of broadband across underserved parts of the US. And while NTIA has hailed fiber broadband as the gold standard for its high speeds and reliability, it is crucial to recognize that it is not a one-size-fits-all solution, particularly when one considers time to deploy, materials and labor cost, materials and labor availability, location (including geography and topological considerations), deployment, and other factors. The availability and deployment figures for ISPs' Internet services, per speed tiers and broadband technologies, can be accessed through the FCC Broadband Data Collection program [19].

When BITAG took on this topic, we observed that some in the policy space may not be fully aware of the current capabilities of broadband technologies. All broadband access technologies have evolutionary paths toward higher data rates and lower latencies (some more limited than others); as such it is important to understand the current and future capabilities of each technology (as described in the previous section of this paper) as well as the associated cost and deployment of these technologies (as described below). In addition, end users ultimately do not care what underlying technologies are used to deliver their broadband service; just the features and pricing of the service.

6.2 Cost Challenges of Broadband Access

When existing broadband infrastructure has a path to higher data rates and lower latency, it's difficult to justify overbuilding new networks; whereas greenfield builds and stranded infrastructure (those unable to be upgraded) should consider the optimal broadband technology for cost and deployability in that circumstance (generally, fiber). However, fiber infrastructure deployment can be time-consuming and costly, with costs of $40,000 or more per mile and years to complete. In dense, high-uptake areas, this cost is readily recoverable; whereas, in rural (and low density suburban) areas, the cost per home-passed increases rapidly (which is why these areas have not been built to date and require grant support to make the economics work). On the other extreme, LEO satellite has a relatively fixed cost (due to the extremely high cost of launching satellites) regardless of the region it serves, making it a less costly option for the most remote areas compared to other broadband access technologies.

6.3 Costs & Timing of Broadband Deployment

Earlier, we described the technical attributes of the various broadband access technologies. However, decisions are typically driven by deployment costs and the ability to leverage existing infrastructure. By leveraging a combination of fiber optic and coaxial cables, HFC broadband provides a balance between cost-effectiveness and performance, by utilizing existing coaxial cable networks, and reducing the need for extensive infrastructure upgrades. This enables a quicker deployment and wider availability of high-speed internet services to sparsely populated or remote residential and commercial areas. DSL broadband provides reasonable broadband connectivity over a combination of traditional copper telephone lines and fiber leverages existing widespread telephone infrastructure, making it accessible and cheap to deploy. FWA offers a reliable broadband solution through wireless using both licensed and unlicensed spectrum. It provides cost-effective deployment options, as it lessens the need for extensive infrastructure and enables swift connectivity to underserved areas. As described above, LEO satellite-based broadband services have the potential to bridge the connectivity gap in remote regions because of their near universal coverage and fixed cost point.

In many cases, a combination of technologies proves to be the most effective approach. By integrating fiber, wireless, and satellite solutions, communities can benefit from a hybrid infrastructure that leverages the strengths of each technology. Technologies like FWA and LEO satellites (if already operational) can be rapidly deployed at a comparatively low cost, providing immediate and affordable connectivity to remote, unserved areas. This speed of deployment is crucial for bridging the digital divide and unlocking economic and educational opportunities in rural communities. When considering the cost of deployment and varied timeline, it is clear that a diversity of broadband access technologies is necessitated by considerations of distance, population density and pre-existing infrastructure.

7 Conclusion and Recommendations

Based on this group's deep industry experience and the topics explored in this paper, it is clear that there is no one best technical solution to delivering broadband internet access service; a wide variety of technologies can serve the needs of users now and in the future. The bottom line for any policymakers or grant makers, is that all of these technologies should be considered; don't leave out any potential tools in the toolbox, so to speak.

The answer to what is the appropriate network technology will depend on a wide range of local, situational factors, especially when new network construction/expansion is being considered. For example, issues of geography and terrain, rights of way and permitting, population density, availability of stable and affordable power at points of access network carriage and aggregation, how quickly connectivity is desired, budgeted cost per passing, the need to maximize passings across a wide area (e.g., state-wide), and so on. For example, a state broadband office may find that a low number of passings in a very remote state forest can rapidly be served with LEO satellite service, while a small town can be served with a mix of Fixed Wireless, and new fiber construction in the downtown core. Passings directly adjacent to or near existing FTTP and HFC networks may be met by edging out with FTTP (for FTTP and HFC) or HFC.

It is also worth noting again that it is typically much faster and more cost-efficient to extend or leverage existing networks rather than building FTTP from scratch. This can be months or even years faster and be done at a significantly lower cost per passing. As states and others determine grant allocations, this can enable a higher number of unserved homes to be served, at a lower overall average cost, connecting more homes more quickly compared to new wireline construction. Given that many of these technologies have robust capabilities now or in the near future, there is also less concern that users will be somehow stranded on outdated technology that will not meet their needs in the future. By extension this means there is not one "best" technology that should be a default choice - but that across a wide geography of a state or the country that the best answer is to select a mix of technologies that matches the geography, population density, cost constraints, time constraints, and other factors. Thus, a technology-neutral approach should be taken.

In addition, last mile broadband internet access network technologies cannot be considered on their own, when considering the goal to deliver good performance to users. The middle mile network and backbone network matter as well. That includes how well-connected an ISP network is to popular destination networks that host popular sites and applications (such as video streaming), content delivery networks (CDNs), cloud providers, gaming networks, and others. It is worth noting that there continues to be a trend where content is moving closer to the last mile and that there remains much innovation in these parts of the network that directly and significantly impacts the quality of broadband for users. The user's home network matters too; we saw this at the start of the pandemic with underperforming Wi-Fi networks [3].

Finally, it is important to bear in mind that speed (throughput) and (idle) latency are not the sole factors that affect broadband quality - working latency (network responsiveness) is emerging as a key performance factor. The BITAG explored that topic extensively in our recent Latency Explained paper [1]. Reliability, consistency, and security are also emerging as key factors - such as routing security as explored recently by the BITAG [2].

Glossary

802.11 A set of standards for implementing wireless local area networking (WLAN) communication.

AFC Automated Frequency Coordination, a system to manage frequency usage in the 6 GHz spectrum.

AP Access Point, a networking hardware device that allows a Wi-Fi device to connect to a wired network.

BEAD Broadband Equity, Access, and Deployment, a program by NTIA aimed at deploying broadband across underserved parts of the US.

BITAG Broadband Internet Technical Advisory Group, an organization that provides technical expertise to address broadband-related issues.

Bufferbloat Delay in network communication due to excessive buffering of data.

CAT5/6 Category 5/Category 6, types of twisted pair cable used for Ethernet connectivity.

CDN Content Delivery Network, a distributed network of servers that work together to provide fast delivery of internet content.

DHCP Dynamic Host Configuration Protocol, a network management protocol used to assign dynamic IP addresses.

DNS Domain Name System, translates domain names to IP addresses.

DSL Digital Subscriber Line, a technology that provides internet access by transmitting digital data over telephone lines.

EasyMesh A Wi-Fi Alliance specification for managing Wi-Fi networks.

FCC Federal Communications Commission, https://www.fcc.gov/

FTTP Fiber to the Premises, a broadband network architecture that uses optical fiber to provide all or part of the local loop used for last-mile telecommunications.

FWA Fixed Wireless Access, a wireless communication technology that delivers high-speed internet access to a fixed location via radio waves.

Gbps Gigabits per second, a unit of data transfer rate.

HFC Hybrid Fiber-Coaxial, a network architecture that combines fiber optic and coaxial cables.

IEEE Institute of Electrical and Electronics Engineers, a professional association that develops standards for various technologies.

IEEE 1905 Standard for a Convergent Digital Home Network for Heterogeneous Technologies.

IETF Internet Engineering Task Force, The international standards development organization that develops and publishes the specifications that define the Internet protocol suite and related applications.

IPTV Internet Protocol Television, a system through which television services are delivered using the Internet protocol suite over a packet-switched network.

ISP Internet Service Provider, a company that provides internet access to customers.

IXP Internet Exchange Point, The sites of Internet bandwidth production, where network operators interconnect to exchange customer routes and traffic. Most IXPs are noncommercial consortia of the participating network operators, and most IXPs exist within single metro areas. As of 2022, there are approximately 750 IXPs active in 151 countries.

Jitter The variability in latency, measured as the standard deviation of latency measurements.

LAN Local Area Network, a network of interconnected computers within a limited area.

LEO Low Earth Orbit, a satellite network providing global coverage.

Mbps Megabits per second, a unit of data transfer rate.

Mesh Network A network of Access Points with routing capabilities that are connected to multiple other Access Points, making their own routing decisions.

NAT Network Address Translator, a method of remapping one IP address space into another.

NMS Network Management Systems, tools used for collecting performance and usage metrics in a network.

NFV Network Function Virtualization, a network architecture that virtualizes network functions, reducing reliance on dedicated hardware.

NTIA National Telecommunications and Information Administration, an agency of the United States Department of Commerce.

OpenWRT An open-source firmware for wireless routers.

Packet The fundamental unit of data communications, each packet contains a *header*, which includes the source and destination addresses and the information necessary to direct and interpret the packet, and a *payload*, which is the data that users or applications are trying to communicate. The Internet's routing system operates on packet headers, and does not examine or act upon information in the payload.

Peering One of the two forms of interconnection between networks, the other being "transit." In a peering relationship, network operators exchange only customer routes (and therefore traffic) but not the routes (and traffic) that they learn via transit. Peering is cost-neutral (no money is exchanged between the parties) and is used at the Internet exchange points at the center of the Internet's topology. Only one peering relationship exists in any routed path between two points in the Internet, at the "center" of that path, while transit relationships lead "downward" in both directions from the peering relationship to each endpoint.

PON Passive Optical Networks, a network architecture that uses fiber optics for data transmission.

Powerline A networking technology that uses existing electrical wiring for data transmission.

QoE Quality of Experience, a measure of overall satisfaction with a service.

QoS Quality of Service, a measure of the overall performance of a network service.

RFC Request For Comments, A series of numbered documents that establish Internet standards; managed by the IETF.

RTT Round-Trip Time, the time taken for a packet to travel from source to destination and back.

SA Standards Association, a group within the IEEE responsible for developing standards.

SDN Software-Defined Networking, a network architecture that allows for centralized control and management.

Throughput The amount of data that can be transferred across a network in a specific unit of time.

Transit One of the two forms of interconnection between networks. In a transit relationship, the "upstream" network operator provides a full set of BGP routes, reflecting reachability for the entirety of the Internet, to the "downstream" customer network, typically in exchange for payment. Peering is the other form of interconnection between networks.

UNPnP Universal Plug and Play, a set of networking protocols that permits networked devices to discover each other's presence on the network.

USDA United States Department of Agriculture, https://www.usda.gov/

WFA Wi-Fi Alliance, a global nonprofit organization that promotes Wi-Fi technology and certifies products.

WPA3-Personal Wi-Fi Protected Access 3 - Personal, a security certification for Wi-Fi networks.

References

[1] "Latency Explained," Broadband Internet Technical Advisory Group (BITAG), 2022 [Online]. Available: http://www.bitag.org/documents/BITAG_latency_explained.pdf

[2] "Routing Security," Broadband Internet Technical Advisory Group (BITAG), 2022 [Online]. Available: https://www.bitag.org/documents/BITAG_Routing_Security.pdf

[3] "Pandemic Report," Broadband Internet Technical Advisory Group (BITAG), 2020 [Online]. Available: https://www.bitag.org/documents/bitag_report.pdf

[4] "Affordable Connectivity Program" [Online]. Available: https://www.fcc.gov/acp. [Accessed: 08-Nov-2023]

[5] "Broadband Equity Access and Deployment Program" [Online]. Available: https://broadbandusa.ntia.doc.gov/funding-programs/broadband-equity-access-and-deployment-bead-program. [Accessed: 08-Nov-2023]

[6] "Rural Digital Opportunity Fund" [Online]. Available: https://www.fcc.gov/auction/904. [Accessed: 08-Nov-2023]

[7] "10G-EPON vs. XGS-PON." [Online]. Available: https://www.cablelabs.com/blog/10g-epon-vs-xgs-pon. [Accessed: 29-Nov-2023]

[8] "Perspectives on LEO Satellites." [Online]. Available: https://www.internetsociety.org/leos/. [Accessed: 08-Nov-2023]

[9] "Enormous ('Mega') Satellite Constellations." [Online]. Available: https://planet4589.org/space/con/conlist.html. [Accessed: 08-Nov-2023]

[10] "Ookla Speed Tests for Starlink." [Online]. Available: https://www.ookla.com/articles/starlink-hughesnet-viasat-performance-q1-2023#:~:text=Speedtest%20Intelligence%20reveals%20that%20Starlink,the%20U.S.%20at%2066.59%20Mbps. [Accessed: 08-Nov-2023]

[11] "Global Economic Value of Wi-Fi® 2021 – 2025," Sep. 2021 [Online]. Available: https://www.wi-fi.org/download.php?file=/sites/default/files/private/Global_Economic_Value_of_Wi-Fi_2021-2025_202109.pdf

[12] "Municipal wireless network." [Online]. Available: https://en.wikipedia.org/wiki/Municipal_wireless_network. [Accessed: 24-Aug-2023]

[13] "List of wireless community networks by region." [Online]. Available: https://en.wikipedia.org/wiki/List_of_wireless_community_networks_by_region. [Accessed: 24-Aug-2023]

[14] "The Differences between WPA-Personal and WPA-Enterprise" [Online]. Available: https://www.tp-link.com/us/support/faq/500/. [Accessed: 01-Jun-2023]

[15] "Welcome to the OpenWrt Project." [Online]. Available: https://openwrt.org/. [Accessed: 24-Aug-2023]

[16] "IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks–Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," Feb. 2021 [Online]. Available: https://ieeexplore.ieee.org/document/9363693

[17] "Wi-Fi® Automated Frequency Coordination: extracting the most value from outdoor and standard power 6 GHz." [Online]. Available: https://www.wi-fi.com/. [Accessed: 30-Aug-2023]

[18] "The Future of Wi-Fi," *In Compliance Magazine* [Online]. Available: https://incompliancemag.com/article/the-future-of-wi-fi/. [Accessed: 01-May-2023]

[19] "FCC Broadband Deployment and Availability Data." [Online]. Available: https://www.fcc.gov/BroadbandData. [Accessed: 29-Nov-2023]

Report Contributors and Reviewers

- Maria Adamcyzk, AT&T
- Richard Bennet, HighTechForum
- Stephen Curran, Cable Bahamas
- Amie Elcan, Lumen
- Hany Fahmy, AT&T
- Nick Feamster, University of Chicago
- Jason Livingood, Comcast
- John Quesenbury, Adtran
- Barbara Stark, unaffiliated
- Rikin Thakker, NCTA
- Greg White, Cablelabs
- David Winner, Charter
- Dan York, Internet Society (ISOC)

Editors

- Matt Larsen, Vistabeam
- Sebnem Ozer, Charter
- Doug Sicker, BITAG