New IP

ICANN Office of the Chief Technology Officer

Alain Durand

OCTO-017
27 October 2020

TABLE OF CONTENTS

This document is part of ICANN’s Office of the Chief Technical Officer (OCTO) document series. Please see the OCTO publication page for a list of documents in the series. If you have questions or suggestions on any of these documents, please send them to octo@icann.org.

Executive Summary

Network 2030 was a focus group (FG) created by the Telecommunication Standardization Sector (ITU-T) Study Group 13 “to carry out a broad analysis for future networks towards 2030 and beyond. In order to formulate a right vision, this FG is expected to identify the gaps and challenges based on the latest networking technologies, and derive fundamental requirements from novel use cases.” The Network 2030 Focus Group concluded in July 2020, envisioning a number of futuristic use cases, ranging from “holographic communications” to “tactile Internet,” “Digital Twins,” and “Industrial IoT.” The requirements perceived for these use cases demand bandwidth on the order of one terabit per second per-flow, sub-millisecond latency, and zero packet loss. These requirements seem unlikely to be ubiquitously realizable in the assumed timeframe of ten years from now.

New IP is driven by Huawei and its subsidiary, Futurewei. New IP’s relationship to Network 2030 is unclear because New IP proponents tend to use the two names interchangeably. At best, New IP can be seen as a set of desired features to implement the use case described in Network 2030. However, there are no publicly available, definitive, and complete descriptions of what New IP is. As such, it can only be seen at best as “work in progress” and cannot be fully analyzed and compared to a standard such as the TCP/IP protocol suite. Hints can be found in Huawei blogs, a Futurewei Internet Draft submitted to the Internet Engineering Task Force (IETF), slides from a guest talk at an Institute of Electrical and Electronics Engineers (IEEE) conference, and in an ITU-T liaison statement to the IETF. At a high level, New IP architecture introduces variable length addresses; reintroduces circuit-switched-like principles in what is dubbed “better than best effort networking”; suggests an approach to enable packets to embed contracts to be enforced by intermediary network elements in a way that is reminiscent of active networks where packets contain code to be executed by routers and switches; and presents the concept of “ManyNets” where instead of a single network, the Internet would become a patchwork of networks loosely interconnected via gateways. New IP advances the idea of a strong regulatory binding between an IP address and a user. If deployed, such techniques could make pervasive monitoring much easier because it would allow any intermediary element (router, switch, and so on) to have full access to exactly which user is doing what. Similarly, content providers would have access to the identity of every user connecting to them. This could dramatically increase the oversight of published content.

Although New IP can use a new variable length addressing type, IPv4, IPv6, or any combination of the above, it cannot be compatible with the existing deployed IPv4- or IPv6-based infrastructure. As such, New IP would have to be deployed in parallel with the current Internet infrastructure, interconnecting via gateways. Any significant deployment would probably face decades-long timelines.

1 Introduction

Network 2030 was a focus group created by ITU-T Study Group 13 at its meeting in Geneva, 16-27 July 2018[1] “to carry out a broad analysis for future networks toward 2030 and beyond. In order to formulate the right vision, this FG is expected to identify the gaps and challenges based

[1] “Focus Group on Technologies for Network 2030”, https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx

on the latest networking technologies, and derive fundamental requirements from novel use cases."

New IP, which is driven by Huawei and its subsidiary Futurewei, can be seen as a set of desired features to implement the use case described in Network 2030. New IP has emerged recently in the context of technology battles, competition among standard bodies, and international geopolitics.

This document provides a technical analysis of New IP and the related Network 2030 work. In particular, this document will focus on the elements that are germane to ICANN's mission (identifiers) and will address the question of compatibility of New IP with the current Internet. The question of compatibility is essential to understanding the challenges potentially facing any deployments of New IP, either as a general replacement of IP, or as an ad-hoc solution in private networks.

The first part of this document (sections 2 and 3) is a survey of available documents related to Network 2030 and New IP. The second part (section 4) analyzes the various claims made.

This study was started under the ICANN 2021-2025 Strategic Plan, Objective 3, that requires ICANN to "embrace the rapid evolution of emerging technologies, business, and security models*"* in order to maintain its agility as the Internet evolves.[2] Not all technology proposals are equal. Some may provide benefits for certain users but put the security, stability, or resiliency of the system of unique identifiers that ICANN helps coordinate at risk. As such, understanding the impact of emerging technologies is required to recommend if they should be embraced.

2 ITU-T Study Group 13 Focus Group Network 2030

Note: This section is provided for background purposes. A technical reader interested solely in the details of New IP might want to skip it. Unlike subsequent sections which provide the outcomes of the author's research, descriptions provided in this section are not the opinions of the author, rather they are either direct quotes from the Network 2030 Focus Group documents or summaries of those documents.

The Network 2030 Focus Group was an activity of Study Group 13 of the International Telecommunications Union Standardization Sector (ITU-T). The leadership, structure, and remit of ITU-T Study Groups are determined at the World Telecommunications Standardization Assembly (WTSA[3]), which is held every four years. The next WTSA meeting was scheduled for November 2020 but is, as of this writing, delayed to 2021 as a result of the COVID-19

[2] "ICANN Strategic Plan for Fiscal Years 2021- 2025," June 2019, https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf

[3] World Telecommunication Standardization Assembly (WTSA-20), https://www.itu.int/en/ITU-T/wtsa20/Pages/default.aspx

pandemic. Each study group submits a report to WTSA and an outline of its proposed work plan for the next four-year study period with its suggested terms of reference. These reports and plans are discussed and ultimately agreed to by consensus of the ITU-T member states in an ITU resolution.

2.1 ITU-T Study Group 13

The remit of ITU-T Study Group 13 (SG13) is "Future networks, with the focus on IMT-2020, cloud computing and trusted network infrastructure."[4] [5] [6] This study group has led ITU's standardization work on next-generation networks – in effect, the market-driven global move away from circuit-switched to packet-switched networking. SG13 is divided into thirteen "questions." (A "question" would be the equivalent of a working group or special interest group in other standard bodies.) The ITU-T's usage of the term "question" designates "a statement of a technical, operational, or procedural problem, generally seeking a recommendation, handbook or report."[7] In the context of SG13, these questions consider various aspects of future networking and cloud computing: software-defined networking (SDN) and network function virtualization (NFV); quality of service; network slicing; fixed/mobile telephony convergence, among other related topics.[8]

2.2 Network 2030

SG13 created the ITU-T Focus Group on Technologies for Network 2030 (FG NET-2030) in July 2018[9]. The Focus Group, often referred to as "Network 2030," was set up as "a platform to study and advance international networking technologies, and investigate the future network architecture, requirements, use cases, and capabilities of the networks for the year 2030 and beyond." These networks are expected to support novel scenarios, such as holographic type communications, haptic sensing, remote surgery, extremely fast response in critical situations and high-precision communication demands of emerging market verticals. The focus group description claimed that "Network 2030 based systems shall ensure they remain fully backward compatible, supporting both existing and new applications."[10]

FG NET-2030's Terms of Reference[11] say the objectives of the Focus Group (FG) are:

> "to carry out a broad analysis for future networks toward 2030 and beyond. In order to formulate the right vision, this FG is expected to identify the gaps and challenges based on the latest networking technologies, and derive fundamental requirements from novel use cases. In addition, the FG intends to formulate an overall framework of Network

[4] Study Group 13 at a Glance, https://www.itu.int/en/ITU-T/about/groups/Pages/sg13.aspx

[5] Focus Group on IMT-2020, https://www.itu.int/en/ITU-T/focusgroups/imt-2020/Pages/default.aspx

[6] Study Group 13 at a Glance, https://www.itu.int/en/ITU-T/about/groups/Pages/sg13.aspx

[7] ITU Recommendation A.23 Annex A (01), 1.5.1.7, https://www.itu.int/rec/T-REC-A.23

[8] Study Group 13 at a Glance, https://www.itu.int/en/ITU-T/about/groups/Pages/sg13.aspx

[9] Focus Group on Technologies for Network 2030, https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx

[10] Focus Group on Technologies for Network 2030, https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx

[11] "Terms of Reference: ITU-T Focus Group on "Technologies for Network 2030," Focus Group NET-2030, https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/ToR.pdf

> 2030, while innovative technical enablers are expected to be proposed. Furthermore, this FG also can serve as an open platform for experts representing ITU members and non-members to quickly move forward the standard develop [sic] of future networks at ITU-T, mainly targeting future networks in the coming decade.

More precisely, the objectives include:

- Study, review and survey existing network technologies, network platforms, and network standards to identify the gaps and challenges towards Network 2030 which are not supported by the existing and near future networks like 5G/IMT-2020.
- Formulate all network aspects of Network 2030, which include but are not limited to vision, requirements, architecture, novel use cases, and evaluation methodology, as related to the fixed network.
- Provide guidelines for network standardization roadmap.
- Establish liaisons and relationships with other SDOs such as ITU-R WP 5D for addressing radio access network aspects.

FG NET-2030 met for the first time in October 2018. It did not complete its work by the end of 2019 and was given a one year extension by SG13. The FG submitted new documents in June 2020 that are now available on the FG web page[12]. FG NET-2030 concluded its work in July 2020.

In the rest of this document, we will use the term FG NET-2030 to identify the actual Focus Group and Network 2030 to designate its work product.

2.3 FG NET-2030 Documents

The major publicly available documents produced by this Focus Group will be referenced according to the terms, [Blueprint] and [Requirements]:

- [Blueprint]**:** "A Blueprint of Technology, Applications and Market Drivers Toward Year 2030 and Beyond."[13]
- [Requirements]**:** "Representative Use Cases and Key Network Requirements for Network 2030"[14]

Additional documents that were subsequently published are:

- "New Services and Capabilities for Network 2030: Description, Technical Gap and Performance Target Analysis[15]

[12] "Focus Group on Technologies for Network 2030", https://www.itu.int/en/ITU-T/focusgroups/net2030/

[13] "A Blueprint of Technology, Applications and Market Drivers Towards the Year 2030 and Beyond," FG-NET-2030, https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/White_Paper.pdf

[14] "Representative use cases and key network requirements for Network 2030," January 2020, https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-NET2030-2020-SUB.G1-PDF-E.pdf

[15] "New Services and Capabilities for Network 2030: Description, Technical Gap and Performance Target Analysis," January 2020, https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-NET2030-2019-SUB.G2-PDF-E.pdf

- "Network 2030 - Gap Analysis of Network 2030 New Services, Capabilities and Use cases" (June 2020)[16]
- "Network 2030- Additional representative use cases and key network requirements for Network 2030" (June 2020)[17]
- "Network 2030 Architecture Framework" (June 2020)[18]
- "Network 2030 - Terms and Definitions" (June 2020)[19]
- "Network 2030 - Description of Demonstrations for Network 2030 on Sixth ITU Workshop on Network 2030 and Demo Day, 13 January 2020" (June 2020)[20]

FG NET-2030 was concluded in July 2020. Other documents produced by the FG include:

- “Gap Analysis of Network 2030 New Services, Capabilities and Use Cases” (June 2020), Doc-O-039[21].
- Additional representative use cases and key network requirements for Network 2030” (June 2020), Doc-O-040[22]
- “Network 2030 Architecture Framework” (June 2020), Doc-O-038-R1[23].
- “Description of Demonstrations for Network 2030 on Sixth ITU Workshop on Network 2030 and Demo Day, 13 January 2020” (June 2020), Doc-O-037[24]
- “Terms and Definitions” (June 2020), Doc-O-041-R1[25].

[16] “Gap Analysis of Network 2030 New Services, Capabilities and Use cases,” Focus Group NET2030, June 2020, https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Gap_analysis_and_use_cases.pdf

[17] “Additional Representative Use Cases and Key Network Requirements for Network 2030,” Focus Group NET2030, June 2020, https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Additional_use_cases_and_key_network_requirements.pdf

[18] “Network 2030 Architecture Framework,” Focus Group NET2030, June 2020, https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Network_2030_Architecture-framework.pdf

[19] “Terms and Definitions for Network 2030,” Focus Group Network 2030, June 2020, https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Network_2030_Terms_and_Definitions.pdf

[20] “Description of Demonstrations for Network 2030 on Sixth ITU Workshop on Network 2030 and Demo Day, 13 January,” Focus Group Network 2030, June 2020, https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Description_of_Demonstrations%20.pdf

[21] “Gap Analysis of Network 2030 New Services, Capabilities and Cases,” Focus Group Network 2030, June 2020, https://extranet.itu.int/sites/itu-t/focusgroups/net-2030/_layouts/15/WopiFrame.aspx?sourcedoc=%7B45C332C0-DEC4-4E29-B2B4-A389B13B5681%7D&file=NET2030-O-039.docx&action=default

[22] “Gap Analysis of Network 2030 New Services, Capabilities and Cases,” Focus Group Network 2030, June 2020, https://extranet.itu.int/sites/itu-t/focusgroups/net-2030/_layouts/15/WopiFrame.aspx?sourcedoc=%7B45C332C0-DEC4-4E29-B2B4-A389B13B5681%7D&file=NET2030-O-039.docx&action=default

[23] “Gap Analysis of Network 2030 New Services, Capabilities and Use Cases,” Focus Group Network 2030, June 2020, https://extranet.itu.int/sites/itu-t/focusgroups/net-2030/_layouts/15/WopiFrame.aspx?sourcedoc=%7BDA10EB7F-6B7D-449B-BCA2-402C89359FB7%7D&file=NET2030%20-O-038-R1.docx&action=default

[24] “Description of Demonstrations for Network 2030 on Sixth ITU Workshop on Network 2030 and Demo Day,” Focus Group Network 2030, June 2020, https://extranet.itu.int/sites/itu-t/focusgroups/net-2030/_layouts/15/WopiFrame.aspx?sourcedoc=%7B4808778B-8DDA-4148-B0C1-7CC17DE654C6%7D&file=NET2030-O-037.docx&action=default

[25] “Terms and Definitions,” Focus Group Network 2030, June 2020, https://extranet.itu.int/sites/itu-t/focusgroups/net-2030/_layouts/15/WopiFrame.aspx?sourcedoc=%7B53A61CB6-0823-4BE8-A66B-DBBF7E9853F1%7D&file=NET2030-O-041-R1.docx&action=default

2.4 Network 2030 Use Cases

The major use cases in Network 2030 are found in [Requirements]. They include:

- Holographic Type Communications (HTC) in [Requirements] section I.1.
  These communications are expected to deliver three-dimensional images and allow interaction between multiple sources and destinations, for instance, for advanced electronic conferencing or immersive virtual reality.

  Requirements:
  - "Gbps for highly immersive augmented reality/virtual reality (AR/VR) and light-field 3D scenarios, and may further reach terabit per second (Tbps) level for true hologram transmission at normal human-size."
  - "Ultra-low latency is crucial for truly immersive scenarios to alleviate simulator sickness."
  - "Multiple transmission paths or data streams with diverse geo-locations are expected to be synchronized appropriately with limited arrival time differences, usually at the level of milliseconds (ms) time interval."

- **Tactile Internet for Remote Communications (TIRO)** in [Requirements], section I.2. Future networks might support haptic communication to provide remote sensing of the human body's movement or muscular effort. The Focus Group has identified two possible use cases: remote surgery and real-time monitoring and control of industrial infrastructure. These use cases might also involve robotics so that real-time visual feedback and haptic information can be communicated between a remote robot and a human operator.

  Requirements:
  - "Bandwidth is especially important in the case of remote monitoring as the increase in complexity of the visual feed (from a traditional 2D image, to 360° video, up to holograms) means that the bandwidth requirements grow drastically. For instance, bandwidths up to 5 gigabits per second (Gbps) might be required for VR feeds, increasing up to 1 Tbps for large sized holograms."
  - "Latency is most crucial for high precision applications such as those described in the above use cases (latency is expected to be ultra-low). The maximum delay that goes unnoticed by the human eye is about 5 ms. Moreover, for the operation to be smooth and immersive, the new paradigm even demands end-to-end latency at sub-ms level for instantaneous haptic feedback in tactile cases."
  - "The human brain has different reaction times to different sensory inputs, for example tactile (1 ms), visual (10 ms) and audio (100 ms). Thus, in tactile cases, the real-time feedback from hybrid sensory inputs, which possibly arise from different locations, must be strictly synchronized."

- **Intelligent Operation Network (ION)** in [Requirements], section I.3. It is suggested that future networks will apply artificial intelligence, machine learning, and neural networks to identify and locate malfunctions in the network. A comprehensive and deeply correlated analysis of measurements would be needed to allow the network to accurately pinpoint root causes of alarms and automatically invoke recovery mechanisms.

Requirements:

- “This capability in future networks enables the advanced intelligent operations described previously. The network requires instantaneous collection of network statistics with low latency.”
- “The network will need to report network monitoring information to the intelligent control functionalities from diverse discrete events... Such information should be given a higher priority, as a need for extremely low latency is expected, at millisecond level.”

⦿ **Network and Computing Convergence (NCC)** in [Requirements], section I.4. Future networks may require multiple distributed network edge sites to interconnect and collaborate with each other to exploit the full potential of cloud computing. Instead of the conventional client-server model, applications would be able to dynamically schedule computing tasks to corresponding computing nodes at different locations according to specific service requirements. These networks are expected to support computing-aware network capabilities that can offer unified management, control, and operation in order to guarantee differentiated service experience with much higher granularity than what is available at present.

Requirements:

- “As networks and computing converge, future networks should support controllable in-time computing power allocation, including modelling, measuring, sensing, advertising and operation of computing power, with prescribed time limitations.”
- “Future networks should also support joint network and computing resource scheduling.”
- “Based on ubiquitous computing resources, every network node can become a resource provider. Flexible addressing capability is thus needed in order to optimally address computing sites and to avoid wasting network resources.”

⦿ **Digital Twins (DT)** in [Requirements], section I.5. This is usually defined as a real-time representation of a physical entity in the digital world. It is thought that DT will add value to traditional analytical approaches by improving situational awareness, and enable better responses for physical asset optimization and predictive maintenance. Digital twins can be applied to various scenarios with physical objects, including cars, buildings, factories, digital twin cities (DTCs), environment, as well as processes and people. These may well be used for the management and monitoring of resources in a smart city.

Requirements:

- “In some cases, the sensory data exchanged between digitized objects or between physical and virtual objects, is quite small, however, in other cases, such as when AR/VR is used to visualize a large-size digital twin entity (e.g., buildings, factories, etc.) for data exchange, high bandwidth is required, similar to HTC. Furthermore, in the case of applying sensory entities for alarming, it demands a guaranteed bandwidth for instant low-volume data transmission with a relatively high priority. Therefore, highly diversified bandwidth on-demand is a key network requirement for DTC.”

- “Data exchange between a DTC and a real city, needs to be as fast as possible, down to the ms level in the case of critical services, hence requiring extremely low-latency data transmission.”
- “In a DTC, some entities (e.g. buildings, water systems) are static, whilst others (e.g., citizens, cars, subways) have high mobility or group mobility. Thus, the network needs to flexibly support mobility on-demand and virtualized entity transition in the DT world.”
- “Since most of the data in a DTC will be associated with citizens or public facilities in the real world, the information exchanges in the digital world must be secure enough to avoid attacks and must be well protected to maintain data privacy. Thus, new security frameworks, such as intrinsic security, binding with digital objects, and novel privacy protection mechanisms should emerge in order to achieve end-to-end security and privacy in an integrated cyber-physical world.”

⦿ **Space Terrestrial Integrated Network (STIN)** in [Requirements], section I.6. STIN is expected to integrate space and terrestrial Internet infrastructure so that low earth orbit (LEO) satellites and other non-terrestrial networking nodes are able to seamlessly internetwork with their terrestrial counterparts. Unlike current satellite network infrastructure, edge devices in these new networks would be able to directly communicate with locally accessible LEO satellite(s), but without necessarily relying on traditional ground station infrastructure.

Requirements:

- “Flexible addressing and routing: Nowadays, allocation of IP prefixes is typically done through major Regional Internet Registries (RIRs) according to specific geographical locations. Consider the IP addressing issue on potentially thousands of LEO satellites with their constellations, the interoperations with the terrestrial Internet infrastructure will incur new challenges, as the IP addresses in space will dynamically interconnect to different domains (autonomous systems) on the ground with different IP prefixes. The new feature of allowing mobile devices to directly connect to local satellites also requires a cost-efficient addressing scheme for mobile devices to communicate with local satellites without necessary address translation operations. The IP addressing strategy will also have direct implications to the routing mechanism both within the LEO satellite network and across the network boundaries between it and the terrestrial network infrastructure. The mobility characteristic of LEO satellite networks is that the movement of the satellites are dynamic but predictable. The vast majority of network links connecting them are statically configured, while a small number of links can be established and torn down on the fly when two satellites on different orbits meet/depart from each other. Thus, an integrated routing mechanism is highly demanded, with the consideration of unique features in STIN.”
- “Compared to the high-capacity fibre optical links that constitute the traditional Internet infrastructure backbone as well as cutting edge access networks, the links connecting LEO satellites in space and terrestrial Internet infrastructure may become a significant bottleneck in terms of bandwidth capacity. In this scenario, the requirement is to increase the capacity in space, including peering links between satellites and also between satellites and ground stations or user devices in order to match the terrestrial capacity for future STIN-based applications.”

- ⦿ Industrial IoT with Cloudification (IIOT) in [Requirements], section I.7. It is anticipated that future industrial networks will move towards the close integration of all components of the manufacturing process: IoT sensors, robots, automated production lines, logistics, cloud computing resources and enterprise business systems. These developments are expected to result in the automatic operation and control of industrial processes without significant human intervention.

  Requirements:

  - "IoT systems contain many control subsystems that run at cycle times ranging from sub-ms to 10 ms."
  - "It is a fundamental requirement for multiple-axis applications to have time synchronization in order to permit cooperation between various devices, sometimes remotely."
  - "In order to recover the clock signal and reach precise time synchronization, the machine control, especially the motion control sub-system, requires very small jitter at sub-microsecond level, and such a small jitter is expected to have bounded limits under some critical situations."
  - "IIoT systems demand high reliability and high security to avoid any potential risk of interrupting production. Specifically, the service availability requirement typically ranges from 99.9999% to 99.999999% for IIoT applications."

Network 2030 also introduces the concept of "ManyNets" in [Blueprint] section 3.2, *"Gaps & Challenges in Today's Communication Services"*[26] Network 2030 also introduces the concept of ManyNets is described as: "*...a* seamless coexistence of heterogeneous network infrastructures: Networks overall, not only at the edge, have become increasingly richer in terms of technology, ownership, and end user participation. Quite likely there will not be just one, but many public Internets. New technologies further widen the constraints for transmitting packets through the utilization of infrastructure-based wireless, wireless mesh, satellite, fixed line technologies (such as fibre optics), all of which must be accompanied by the fundamental packet transfer solution, while adhering to the underlying ownership relations when traversing those different networks."

3 New IP

New IP is a concept proposed by Huawei and Futurewei, a subsidiary of Huawei.[27] This is referred to in this document as [HuaweiBrief]. As described in the "About Us" section of Futurewei's home page, "Futurewei Technologies, Inc., founded in 2001 is a US corporation and an affiliate of Huawei Technologies Company Ltd. engages in research and development of information and communication technologies (ICT)." There appear to be no publicly available documents completely describing what New IP is. As such, there is some degree of confusion, first about its relationship with Network 2030, then about what New IP technically is. In particular, to date, it has been impossible to determine whether New IP is meant for deployment

[26] "New Services and Capabilities for Network 2030: Description, Technical Gap and Performance Target Analysis," January 2020, https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-NET2030-2019-SUB.G2-PDF-E.pdf

[27] "A Brief Introduction about New IP Research Initiative," Huawei Technologies, Co., Ltd., https://www.huawei.com/en/industry-insights/innovation/new-ip

in specific verticals or it is intended to be a full-blown replacement of the existing IP (IPv4 and/or IPv6) for the Internet.

3.1 New IP vs Network 2030

The SG13 Chairman, Leo Lehmann, stated “New IP is not a deliverable of Focus Group Network 2030 studies, but might supply solutions for scenarios considered by the Focus Group. … Network 2030 and New IP are related but two independent streams of work.”[28]

One of the Contributions to FG NET-2030, NET2030-I-115[29] analyzes the relationship between Network 2030 and New IP. (Contribution is an ITU term of art to formally submit a document prior to a meeting.) The Contribution examines the various use cases of Network 2030 and states in Section 4 “Potential Questions for next study period: A high level protocol framework New IP is thus highly needed.”

The boundaries between Network 2030 and New IP have been blurred, both in FG NET-2030 and SG13. One, perhaps overly simplistic, way to differentiate between the two would be to view Network 2030 as identifying use cases and defining requirements which sets the stage for New IP as a technical solution to implement them.

3.2 New IP Documents

At present, the clearest public description of New IP’s characteristics is provided by [HuaweiBrief]. This article states that New IP is a technology study initiative, “driven by a vision on scenarios for utilizing Internet technologies in many facets of the future digital industry and society... centered on study areas that address aspects of the Internet data plane as well as its associated architecture, technologies and protocols... Instead, New IP addresses the study of technologies that fulfil the need for increased flexibility, determinism, and security & privacy, while also ensuring the continued need for ever-increasing throughput (over a plethora of multi-access technologies) as well as catering to very user-specific in-network data plane operations to achieve maximum Quality of Experience (QoE).”

A liaison statement from ITU-T to the Internet Engineering Task Force (IETF) was sent in September 2019.[30] For the purposes of this document, this statement will be referred to as [ITUtoIETF]. It includes a set of slides presenting a tutorial entitled “New IP: Shaping the future

[28] “Lehmann, Leo, “SG13 Chairman’s blog: Network 2030 and New IP based Networks: Is there a Difference?” March 2020, https://www.itu.int/en/ITU-T/studygroups/2017-2020/13/Pages/CB-Future-Networks.aspx

[29] “New IP concept and relationship with Network 2030,” Focus Group Network 2030, January 2020, https://extranet.itu.int/sites/itu-t/focusgroups/net-2030/_layouts/15/WopiFrame.aspx?sourcedoc=%7B33D98FD8-942D-4868-8F1E-872DD188A964%7D&file=NET2030-I-115.docx&action=default&CT=1593465439441&OR=DocLibClassicUI

[30] “New IP: Shaping the Future Network: Tutorial,” Telecommunication Standardization Advisory Group, ITU-T Liaison to IETF, September 2019, https://datatracker.ietf.org/liaison/1653/, https://www.ietf.org/lib/dt/documents/LIAISON/liaison-2019-09-30-itu-t-tsag-ietf-iab-ls-on-new-ip-shaping-future-network-attachment-3.pptx

network." The IETF also issued a liaison statement in response, referred to here as [IETF ITU].[31] Among other points, [IETFtoITU] mentions:

- "In reviewing the proposals included with your liaison statement, we find that there are several statements that are unsupported or incorrect. 'Firstly, due to historical reasons, the current network is designed for only two kinds of devices: telephones and computers.' The fundamental design of the IP protocol stack is not limited to telephones and computers, but encompasses a very broad range of devices, including many that the proposals consider as future work."
- "Disjoint addressing systems necessarily require independent routing to ensure reachability in each system. While these may be layered (as SR-MPLS, documented in RFC 8660, is layered on IP routing), using heterogeneous address spaces without a common substrate implies complex translation to achieve interchange among the different domains. Such translation likely increases fragility and latency while requiring additional network state to achieve interoperability."
- "We see no evidence that the challenges described in the proposals cannot be met by continuing to evolve the existing IP protocol suite."

Further technical detail on New IP, can be found in the IETF Internet Draft, "Forwarding Layer Problem Statement,"[32] written by employees of Futurewei and submitted in March 2020. For the purposes of this document, this Internet Draft will be referred to as [Forwarding]. The document discusses new use cases for the Internet together with an outline of the requirements for the network capabilities and services that are needed to address them.

There is a large overlap in the set of use cases and general directions for solutions in [HuaweiBrief], [ITUtoIETF], and [Forwarding]. [Forwarding] goes into significantly more technical details and will be used as the basis for the analysis in section 4.

Another paper entitled "New IP: A Data Packet Framework to Evolve the Internet"[33] has been presented at IEEE "High Performance Switching and Routing" 2020 as an invited paper. For the purposes of this document, this paper will be referred to as "framework." This is far from a formal description of New IP or its packet format: it does not show the complete New IP header, but only some of the fields; however, it gives some indications on how it is structured. Similar information can be found in the document referred to as [WhatIsNewIP].[34] Several other details can be found here.[35]

[31] "Liaison Statement: Response to LS on New IP, Shaping Future Network," IETF liaison to ITU, March 2020, https://datatracker.ietf.org/liaison/1677/

[32] "Forwarding Layer Problem Statement, https://tools.ietf.org/html/draft-bryant-arch-fwd-layer-ps

[33] Richard Li, Kiran Makhijani, Lijun Dong Futurewei Technologies, "New IP: A Data Packet Framework to Evolve the Internet", invited paper, May 2020, IEEE 21st International Conference on High Performance Switching and Routing (HPSR) 2020

[34] Richard Li, "What is New IP," Industrial Keynote Speech, July 2020, IEEE Infocom 2020

[35] Zhe Chen, Chuang Wang, Guanwen Li, Zhe Lou, Sheng Jiang (HUAWEI) and Alex Galis (University College, London) "NEW IP Framework and Protocol for Future Applications," April 2020, https://ieeexplore.ieee.org/document/9110352

3.3 New IP Architecture Elements

It is worth re-stating that there appear to be no publicly available, specific design documents describing the New IP architecture. Only a glimpse of that architecture can be found by reading [HuaweiBrief], [ITUtoIETF], and [Forwarding].

3.3.1 Use Cases

New IP use cases and background are best found in the section 2 of [Forwarding]. This includes:

- **Audio/Video Streaming and Virtual Reality**
  The authors of [Forwarding] state that these applications are likely to place demands that will challenge the capabilities of current protocols, particularly on bandwidth, as well as stricter latency and jitter requirements. In brief, the authors' view is today's best-effort for streaming with adaptive video and no service guarantees, and is unlikely to be sustainable in the next 10 years.
- **Fixed Networks in 5G and Beyond 5G**
  The authors of [Forwarding] claim that although the protocol stack for the radio component of 5G networks has evolved to provide per-frame reliability and latency guarantees, the "backhaul" IP/MPLS transport network by and large remains a best-effort delivery. In the authors' opinion, "it is no longer possible to solve the corresponding network problems simply by increasing capacity."
- **Industrial control networks**
  Controllers for high-precision machinery and equipment, such as robotic arms and manufacturing equipment for the assembly of electronic components require the delivery of packets with very precise and deterministic performance characteristics. In these settings, the control functions have very exacting timing requirements that are not tolerant of packet loss, latency variations, or jitter. The authors claim that the work of the IETF on deterministic networking alone is not sufficient to meet all of these emerging needs, for which not only maximum latency should be controlled, but also minimum latency, to ensure packets arrive within a certain time frame.

After describing these three use cases, [Forwarding] further points to the other use cases described in Network 2030.

3.3.2 3.3.2 Architecture Elements

New IP architecture elements can be best found in the section 5 of [Forwarding]. In this section, the New IP architecture is based on "Foundational Services" that include:

- High-Precision Communications Services:
  - In-time services specifying maximum latency
  - On-time service specifying minimum and maximum latency
  - Coordinated services such as multiple flows to be delivered under the same end-to-end latency
- Qualitative Communication Services:

- Network elements downgrade elements of the communication and "suppress retransmission of less relevant portions of the payload in order to meet requirements on latency by applications that are tolerant to this."

Section 6 of [Forwarding] lists a number of issues with the current Internet Protocol that the authors of [Forwarding] believe need to be addressed:

- IPv6 does not offer easy to use hop-by-hop options, enabling special treatment of packets by intermediary routers. Similarly, there are no ways for intermediate routers to insert new headers into the packets.
- IPv6 has a fixed address length. The authors of [Forwarding] note that header compression techniques as specified by the IETF IPv6 over Low power WPAN (6LoWPAN) Working Group,[36] are too CPU intensive for presumably current battery-powered IoT devices.
- IPv6 does not offer "better than best effort" services. The authors of [Forwarding] note that some applications require service delivery involving, "stringent end-to-end (E2E) latency with no retransmission and no packet loss." A specific need and requirement is "Need for determinism on E2E throughput and latency. The current TCP/IP is hence not-suitable for Mission-critical and real-time E2E applications."
- The authors of [Forwarding] comments on the lack of a standardized solution for adaptive bit rate video streaming. They note that solutions like RFC 2205[37] RSVP rely on router alerts and do not scale well. (Router alerts are special options in IPv6 packets to signal routers to perform specific treatments.) They also note that there is room for improvement on congestion management where routers could make better informed decisions when dropping packets if they were aware of the minimum acceptable bandwidth those applications require, such as degrading the flow quality from excellent to acceptable but no further.
- The efforts in the IETF Deterministic Networking (DetNet) Working Group[38] are only examining maximum latency, not bounded latency. The authors of [Forwarding] also criticized the DetNet Working Group's efforts: "DetNet is also far from attempting to identify if or how the services it plans to introduce could be made to operate over the Internet in general; instead, it focuses mostly on the shorter-term goal to enable them in controlled networks within a limited domain."
- The authors of [Forwarding] observed that routers have evolved to include a very fast, hardware accelerated forwarding plane performance (NFVI FP), but the same routers have not included fast CPUs to similarly accelerate the treatment of control plane messages. They suggest "redesigning control plane protocols such that they are lighter weight in their signaling and state machinery, and can therefore be completely implemented in the hardware accelerated forwarding plane."
- The authors of [Forwarding] believe a user-to-network API is necessary. They observe that "Some of the deployment models need specific signaling mechanisms from users/applications." They add "These are needed for an E2E service offering for better than best effort or high-precision networking. These may involve new transport mechanisms at hosts, middle-boxes, and routers to meet the E2E service requirements

[36] J. Hui, Ed, P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," September 2011, https://tools.ietf.org/html/rfc6282

[37] "Resource ReSerVation Protocol (RSVP)," https://tools.ietf.org/html/rfc2205

[38] "Deterministic Networking," Deterministic Networking (DetNet) Working Group, https://datatracker.ietf.org/wg/detnet/about/

> in these limited domain deployments." The authors continue, "Here one of the functional requirements is to signal the service level objectives (SLOs) dynamically for a particular service from the network. This signaling includes the service description, the service negotiation with the network, the service setup or modification, or the need to execute some functions at [the] network device and send the results back to the sender. However, the current IP was not designed for this. For example, the result of SLO negotiation, every hop needs to be updated in the IP packet at the router and returned back to the sender (originating host or gateway device for a Service Provider)."

Section 7 of [Forwarding] points to claims on how New IP might solve the above problems:

- Variable length addresses
- Address semantics
- Multiple instructions: a packet should include a list of instructions to be executed in sequence by intermediary routers. Note: this is known as "active networking", a form of programmable networking.
- Node and Path Specific Processing Instructions. These are the capabilities for routers to execute the code included in packets.

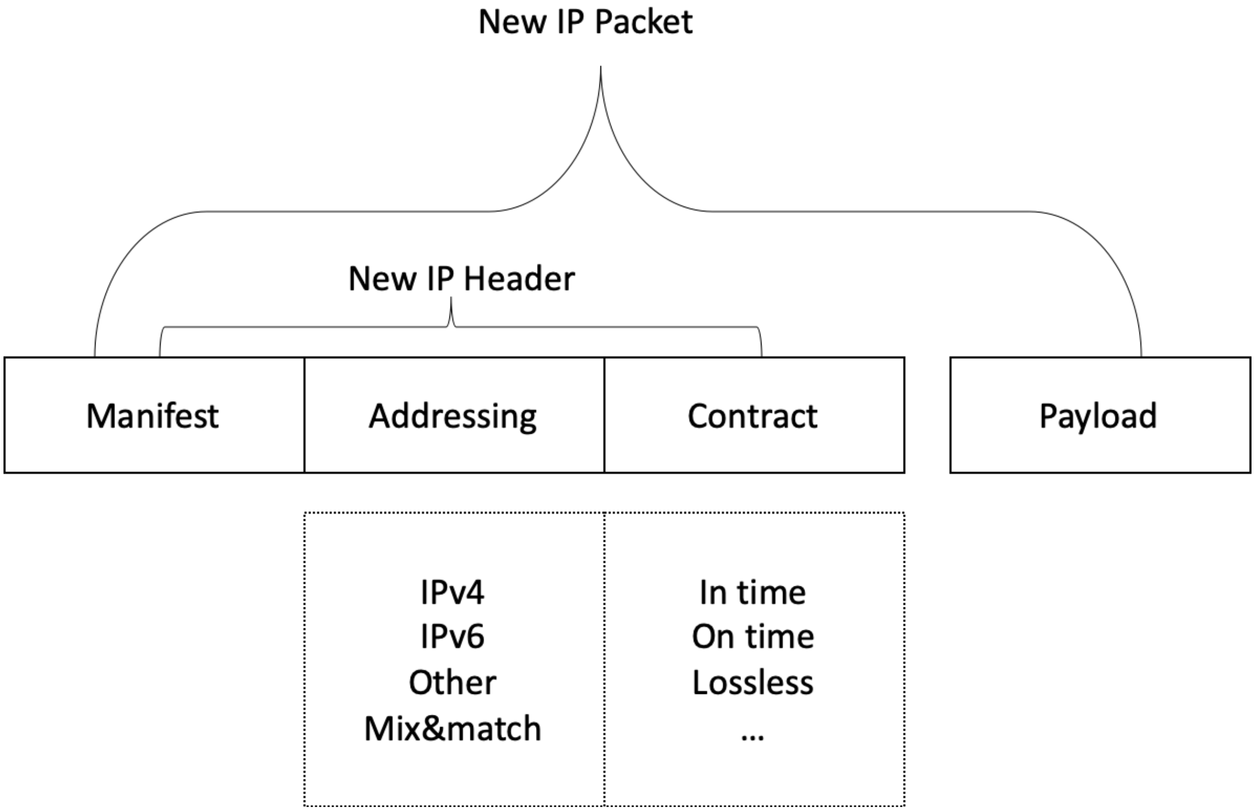
Section 10 of [Forwarding] expands on the notion of ManyNets found in [Blueprint]. It states: The "manyNets concept aims to support flexible methods to support communication among such heterogeneous devices and their networks." In the view of the authors of [Forwarding], this statement is supported by the analysis that "satellite and the terrestrial networks adopt different protocol architecture, which causes the difficulty to internetwork between them, yet the common goal is to provide access to the Internet. Secondly, there will be a massive number of IoT-type devices connecting to the networks but the current interconnection schemes are too complex for these services. There are further trends in 5G, Beyond 5G (5G/B5G) back-haul infrastructure, requiring diverse sets of resource guarantees in networks to support different industry verticals."

3.4 New IP Header to Carry Packets with Different Address Families

As mentioned earlier, some indications on the structure of the New IP header can be found in the framework[39] and [WhatIsNewIP] documents.

[39] Richard Li, Kiran Makhijani, Lijun Dong Futurewei Technologies, "New IP: A Data Packet Framework to Evolve the Internet", invited paper, May 2020, IEEE 21st International Conference on High Performance Switching and Routing (HPSR) 2020

As seen in framework, a New IP packet can be represented as:



One of key suggestions here is that the header will have extra fields when compared to the IP header. One of these fields will indicate the address families of the source and destination addresses. This way, a New IP packet could use IPv4 addresses, IPv6 addresses, or a new type of variable length addresses. It could be possible to mix and match address families in the source and destination addresses. This feature is suggested to allow for seamless interoperability between various networks using different formats of IP addresses.

Another New IP header field will include a contract to specify the type of service requested, such as in-time, on-time, lossless, and the associated parameters.

3.5 From New IP to Future Vertical Communication Networks and Protocols at ITU-T

Based on their actions, it appears that one of the goals of Huawei at ITU-T was to use the outcome of FG NET-2030 to include New IP in questions for the ITU-T Study Group 13 and Study Group 11 at the upcoming World Telecommunication Standardization Assembly (WTSA) meeting. This effort is running into strong opposition from a number of countries.40

[40] For example, "Contribution SG13-C915 at the same meeting," Japan, July 2020, https://www.itu.int/md/T17-SG13-C-0915/en

At the July 2020 ITU-T Study Group meeting, Huawei presented two sets of new contributions, one in ITU-T Study Group 13 (SG13) and one in ITU-T Study Group 11 (SG11). In SG13, the contributions (SG13-C99441 and SG13-C99542) proposed to modify the terms of references of two questions of SG13 during the upcoming WTSA meeting. The supporting contribution (SG13-C99643) introduces the concept of “Future Vertical Communication Networks & Protocols” (FVCNP) which would support:

- Semantic addressing
- Flexible length addressing
- ManyNets
- Deterministic services
- Intrinsic security and privacy
- High throughput
- Endpoint-definable forwarding operations

In SG11, Huawei proposed modifying the terms of references of two questions of SG11 during the upcoming WTSA meeting in contributions SG11-C551[44] and SG11-C552,[45] using SG11-C553[46] as a supporting contribution.

These two sets of contributions appear to be almost identical, albeit with minor changes to adapt to the context of each study group. SG13-C994 is similar to SG11-C552; SG13-C995 is similar to SG11-C551, and SG13-C996 is virtually indistinguishable from SG11-C553. In each set of Contributions, the list of desired properties overlaps entirely with what can be found in Network 2030 and New IP. This suggests that FVCNP is simply a rebranding of New IP that does not include IP in its name.

[41] “Proposal of text amendments to the Terms of Reference of the proposed new Question F (Q.F) for the next study period of SG13,” Internet Area (INTAREA) Working Group, September 2020, https://www.itu.int/md/T17-SG13-C-0994

[42] “S. Bryant, U. Chunduri, T. Eckert, A. Clemm, “Proposal of text amendments to the Terms of Reference of the proposed new Question G (Q.G) for the next study period of SG13,” Futurewei Technologies Inc., March 2020, https://www.itu.int/md/T17-SG13-C-0995

[43] “Supporting contribution to the two contributions submitted into the July 2020 SG13 meeting which propose text amendments to the Terms of Reference of, respectively, draft Questions F and G of SG13 (Q.F/13 and Q.G/13) for the next study period of SG13,” China Mobile Communications Corporation, China Telecommunications Corporation, Huawei Technologies Co., Ltd. (China), Huawei Technologies Düsseldorf GmbH (Germany), July 2020, https://www.itu.int/md/T17-SG13-C-0996

[44] “Proposal of text amendments to the Terms of Reference of draft Question O of SG11 (QO/11) for the next study period of SG11,” https://www.itu.int/md/T17-SG11-C-0551

[45] “ITU-T SG 11 (Study Period 2017),” Beijing University of Posts and Telecommunications (China), China Mobile Communications Corporation, China Telecommunications Corporation, Huawei Technologies Co., Ltd. (China), Ministry of Industry and Information Technology (MIIT) (China), July 2020, https://www.itu.int/md/T17-SG11-C-0552

[46] “Supporting contribution to the two contributions submitted into the July 2020 SG11 meeting which propose text amendments to the Terms of Reference of, respectively, draft Questions P and O of SG11 (Q.P/11 and Q.O/11) for the next study period of SG11,” Beijing University of Posts and Telecommunications (China), China Mobile Communications Corporation, China Telecommunications Corporation, Huawei Technologies Co., Ltd. (China), Ministry of Industry and Information Technology (MIIT) (China), Huawei Technologies Co., Ltd. (China) July 2020, https://www.itu.int/md/T17-SG11-C-0553

SG11 and SG13 were unable to agree on these Contributions. There was therefore no consensus to adopt the proposed modifications. At the time of writing, the following documents remain subject to further discussion in their respective study groups:

- SG11-TD1459/GEN[47] to introduce a study of new layer 4 transport protocols in SG11
- SG13-TD290/PLEN[48] to introduce the study of ManyNets and FVCNP in SG13

Those two documents will certainly be the topic of further discussions before the WTSA meeting.

4 Analysis of Network 2030 Requirements and New IP Architecture Elements

At a very high level, the two previous sections can be summarized by pointing to the following elements promoted by Network 2030 and New IP:

- Ultra-high throughput and ultra-low latency
- In-time services: guaranteed minimum and maximum bounded latency
- Active networks for bandwidth reservation: intelligent network elements that can execute code included within packets. Examples would be synchronization of flows or intelligent content adaptation by routers when the required bandwidth is not available
- Variable-length addresses
- ManyNets

New IP does not explicitly call for active networks. The “*contracts*” however placed in New IP headers, as seen in section 3.4, are pointing in the same general direction: dynamic configuration of intermediary active elements based on instructions found inside packets.

4.1 Ultra-high Throughput and Ultra-low Latency

Network 2030 envisions holographic transmissions requiring bandwidth reaching 1Tbps per flow. Today's fastest interfaces commercially available are 400Gbps to carry aggregates of large numbers of flows. In early 2020, Nokia set the world record with a speed of 1.52 Tbps over 80km of standard single mode fiber.[49]

Sub-millisecond latency requirements need to reconcile with the laws of physics: one millisecond round trip represents a distance of approximately 100km at the speed of light in a fiber, not taking into account the time to process the optical signal. While this may be an issue for industrial type applications that are bound to a single geographic site, or for smart city type projects, the latency incurred from distance would place serious limitations to any general public

[47] “Tentative Questions O/11, P/11 and Revised Q8/11 (H/11) for next Study Period (2021-2024),” Chairman SG11, July 2020, https://www.itu.int/md/T17-SG11-200722-TD-GEN-1459/en

[48] “Tentative ToRs of Q.F and Q.G,” NSP ad hoc convenor, July 2020, https://www.itu.int/md/T17-SG13-200720-TD-PLEN-0292/en

[49] Alan Weissberger, “Nokia Bell Labs sets world record in fiber optic bit rates,” IEEE Communications Society, March 2020, https://techblog.comsoc.org/2020/03/14/nokia-bell-labs-sets-world-record-in-fiber-optic-bit-rates/

end-to-end deployment across the planet, or impose serious logistical requirements such as replicating data/compute closer to the requesting device for client/server type applications.

Network 2030 calls for an increase in the bandwidth for the communication of LEO satellites to ground stations in order to integrate space and terrestrial networks. Satellites are a very interesting approach to providing connectivity in places where fiber is not available. LEO satellites can also be used to lower latency on some long-haul communications. The available bandwidth on satellites, however, does not compare with the one available on fiber, neither now nor in the foreseeable future:

- Geostationary satellites (GEO) operate in the Ku (12 to 18 GHz) or Ka band (26.5 to 40GHz)[50]. Satellites with the highest bandwidth in the Ku band have a maximum aggregate bandwidth of about 25-30Gbps. Those operating in the Ka band have a maximum aggregated bandwidth of about 70 to 75 Gbps.[51] ("Eutelsat Konnect was launched in January 2020 with a throughput capacity of 75Gbps.") These data rates are close to the maximum theoretical bandwidth[52] for either band. Moving to higher frequencies in the V band (40-75Ghz) would only double the maximum theoretical bandwidth up to about 150Gbps, but would be susceptible to serious rain fade and radio absorption issues.
- Low Earth Orbit (LEO) satellites provide an even lower per-satellite bandwidth, because they are very small and do not have enough power to transmit a higher bandwidth and stronger signal. The total achievable bandwidth when at full scale of the now defunct OneWeb constellation was estimated to reach 20Tbs for 2,862 satellites.[53] That was an aggregated bandwidth of about 7Gbps per satellite operating in the Ku band.

As can be seen in comparison with the Nokia demonstration cited above, all these numbers are a far cry from what a single fiber can do today. There are physical underlying reasons for this bandwidth disparity: fiber and copper guide an entire spectrum of signal from source to destination in a predictable medium. Radio, even directional, spreads the unprotected-from-the elements signal over a wide range at distance.

4.2 In-time Service Delivery: Guaranteed Minimum and Maximum Bounded Latency

Providing a quality of service (QoS), with a minimum and maximum latency that is longer than the normal transit delay though the network would require active elements to store the data and release it at the right time. Because of the variability in network congestion, this buffer would have to be located relatively close to the destination; thus, in practice there would need to be two buffers, one close to each end of the communication. It is unclear how such buffers would

[50] "Satellite Frequency Bands," European Space Agency, https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Satellite_frequency_bands

[51] "Eutelsat Konnect Satellite, Built By Thales Alenia Space, Now In Orbit," Thales Group, https://www.thalesgroup.com/en/worldwide/space/press-release/eutelsat-konnect-satellite-built-thales-alenia-space-now-orbit

[52] "Shannon-Hartley theorem," Wikipedia, https://en.wikipedia.org/wiki/Shannon–Hartley_theorem

[53] "Low-Earth Orbit satellites: Spectrum access," Digital Transformation Monitor, July 2017, https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_LEO%20-%20Spectrum%20access%20v1_0.pdf

scale. At 1Gbps, it would take 1.25MB per flow to cache 10 ms of network traffic. On a provider edge device that manages 100,000 subscribers with a single flow each, this means 125GB of memory scaling up to 1.25TB of RAM to store up to 100ms. Also, it is unclear what to do once those buffers are consumed. Some packets would have to be discarded, defeating the entire stated purpose of loss-free networks. Also, it is important to note that large buffers have sometimes been proven to be counterproductive, as seen in "bufferbloat."[54]

One of the key design principles of the Internet was to have 'dumb' intermediary network elements and smart edges[55]. Introducing large, intelligent buffering systems into the data transmission path to provide minimum latency guarantees is an unproven technology and a major departure from that principle, with no guarantees for success.

4.3 Active Networks for Bandwidth Reservation

The idea of end user applications programming intermediary network elements is nothing new. One can find a description in IEEE P1520 (P1520[56]) published in 1998, referencing the international research and industry community known as OPENSIG created in 1995. P1520 describes a programming interface for SS7 switches, ATM switches, and IP routers. This interface was proposed as an out-of-band mechanism.

In-band mechanisms embedding code within packets to be executed by intermediary network elements are called active networking. The Active Networks Program was a DARPA-sponsored research program seeking to sharply increase the programmability of computer networks and network components. Many scientific papers were published in the late 1990s on the subject.[57] [58] [59] [60] [61] A book covering this topic was published in 2002.[62]

Active networks never transitioned from the academic world to the commercial world. Perhaps one of the reasons is that explicit requests for quality of service (QoS) are based on the notion

[54] "Bufferbloat", Wikipedia, https://en.wikipedia.org/wiki/Bufferbloat

[55] "Smart and stupid networks: Why the Internet is like Microsoft," Odlyzko, A., http://www.dtc.umn.edu/~odlyzko/doc/stupid.networks.pdf

[56] Biswas J, Lazar AA, Huard JF, Lim K, Mahjoub S, Pau LF, Suzuki M, Torstensson S, Wang W, Weinstein S. The IEEE P1520 standards initiative for programmable network interfaces. IEEE Communications Magazine. 1998 Oct;36(10):64-70. http://www.ee.columbia.edu/~aurel/papers/programmable_networks/comm%20magazine98.pdf

[57] Wetherall, D. J. and Tennenhouse, D. L. 1996. The ACTIVE IP option. In Proceedings of the 7th ACM SIGOPS European Workshop, ACM Press, New York, NY.

[58] Tennenhouse, D. L. and Wetherall, D. J. 1996. Towards an active network architecture. SIGCOMM Comput. Commun. Rev. 26, 2, 5-17.

[59] Tennenhouse, D., Smith, J., Sincoskie, D., Wetherall, D., and Minden, G. 1997. A survey of active network research. IEEE Commun. Mag. 35, 1, 80-86.

[60] Calvert, K. L., Bhattacharjee, S., Zegura, E. W., and Sterbenz, J. P. G. 1998. Directions in active networks. IEEE Commun. Mag. 36, 10, 72–78.

[61] Schwartz B, Jackson A, Strayer T, Zhou W, Rockwell D, Partridge C (BBN Technologies)
Smart packets: applying active networks to network management
ACM Transactions on Computer Systems, February 2000. http://www-unix.ecs.umass.edu/ece/wolf/courses/ECE697J/Fall2002/papers/AN_smart_packets_network_management.pdf

[62] Bush F, Kulkarni A, Active Networks and Active Network Management, Springer 2002

that bandwidth is an expensive and scarce resource that must be managed. The last twenty five years have shown that this is not necessarily the case.[63] Wireline bandwidth has been plentiful. It has dramatically increased year after year, both in the last mile or residential access and in data center or core networking. We went from Ethernet (10mbps) to Fast Ethernet (100mbps) to 1GE (1Gbps), 10GE (10Gbps), 40GE (40Gbps), and now 100GE (100Gbps) and 400GE (400Gbps). In the wireless world, spectrum is limited. Still, wireless bandwidth has also increased generation after generation, and 5G now promises bandwidth up to 1Gbps for individual end stations.

On a separate, but related topic, the Internet Architecture Board (IAB) issued RFC 7305,[64]"Report from the IAB Workshop on Internet Technology Adoption and Transition." One of the case studies was a multi-path TCP (MPTCP) deployment. MTCP's purpose was to send TCP packets from the same connection along multiple paths to improve resource usage. It was observed that "First and foremost, increasing bandwidth within the network seems to decrease the attractiveness of MPTCP," and later, "not all parties may agree on the benefits." For an application that is bandwidth hungry, simply waiting for the next generation of Ethernet networks has generally been a much simpler and more cost effective solution than engineering complex mechanisms to reserve guaranteed bandwidth. In other words, the business case for complex mechanisms such as explicit QoS has never been clear.

There are also intrinsic security challenges to active networking. Some of these challenges were discussed back in 1999.[65] How does one know that the code embedded in the packet is harmless and does not contain viruses? Who or what decides if that code is authorized to run on the router? How does one know that it has not been tampered with en route? Some of these questions are generic and apply to any kind of code. In a traditional client-server model, potential damages due to bad code are limited to the end-points. In an active network, the potential for collateral damage is much higher. Cryptographic techniques, such as trusted parties cryptographically signing code, might help, but the cost of deploying them on routers to check every single packet might be prohibitive, especially at the packet transmission rates suggested by the use cases in Network 2030. It is worth remembering that BGPsec, a proposal to secure Internet routing defined in RFC 8205[66],has been very difficult to deploy at scale. One of the reasons often mentioned for this difficulty is that it would require every ISP's peering routers to perform cryptographic checks of BGP announcements, a task that can be too CPU intensive for many routers. Doing the same type of checks for QoS on every single packet in an active network would be many orders of magnitude more difficult. BGP announcements typically come at a frequency of a few hundreds per second. A terabit-per-second router would see about one billion packets per second. That is seven orders of magnitude more.

Section 7.4 of [Forwarding] hints at active networks as a way to achieve two things: flow coordination and seamless degradation of performance up to a certain threshold in case of congestion. It suggests to include "contracts" within IP headers that would have to be enforced by intermediary routers. From an ISP perspective, such contracts set by an end point have to be

[63] "Over-provisioning, the only solution to QoS and Traffic Engineering", http://www.ipam.ucla.edu/abstract/?tid=1517&pcode=CNTOP

[64] "Report from the IAB Workshop on Internet Technology Adoption and Transition (ITAT)," Internet Architecture Board (IAB), July 2014, https://tools.ietf.org/html/rfc7305

[65] Alexander S, Arbaugh W, Keromytis A, Smith J, Bell Labs, Lucent Technologies, "Security in Active Networks," https://www1.cs.columbia.edu/~angelos/Papers/SIP99-anets.pdf

[66] M. Lepinski, K. Sriram "BGPsec Protocol Specifications," Internet Engineering Task Force, September 2017, https://tools.ietf.org/html/rfc8205

treated with some skepticism. The typical application behavior is to mark every flow with a tag “important, do not drop.” Unless some form of authentication, accounting, and billing is implemented, ISPs tend to configure routers to ignore such tags in the general case. At a local scale, configuring routers to act on those tags is achievable. ISPs have typically deployed an edge router, re-marking packets containing application-level tags with new tags based on specific user-level contracts. This works while the traffic remains within the ISP network. Doing so across independently managed networks remains an open issue.

4.4 New IP Addresses

4.4.1 Semantic Addresses

Semantic addresses are presented in [ITUtoIETF], slide 18. They introduce the concept of “Resource ID,” “Service ID,” and “Content ID.” The rationale given is: *“Instead of mapping all information into network addresses, the diverse IDs are used to indicate the destination, which improves routing capabilities.”*

Using IP addresses to map out services or resources has been successfully used on the Internet for many years. For example, the well known IPv4 address 8.8.8.8 is the Google open recursive DNS resolver. Similarly, DNS root servers have been using anycast IP addresses to horizontally scale their services. Other interesting developments at IETF include work on Segment Routing (SR) RFC8402[67]. Recent Internet drafts from the Source Packet Routing in NetworkinG (SPRING) Working Group include work on a new IPv6 Segment Routing Header (SRH) to program SR networks[68].

[ITUtoIETF] is silent on what possible benefits these new identifiers would have and, in practice, what differences would there be with IP addresses used as described above.

4.4.2 Variable Length Addresses

The rationale presented by New IP for variable length addresses is that battery powered IoT devices can not handle 128-bit IPv6 addresses. One could make several observations:

- Tiny, low cost IoT devices exist today that have no problems dealing with IPv6 packets. Even if this assertion were true for some categories of devices, Moore’s law[69], which has addressed many limitations in cost and computing power for a number of decades, can be expected to continue to hold (at least for a time) to solve this problem before 2030.
- If no translational gateway is assumed, New IP packets need to carry a short, variable-length address of the IoT device and a long, variable length address of some server in the cloud or other end-point. Thus, only half of the saving would be achieved.

[67] C. Filsfils, S. Previdi, B. Decraene, S. Litkowski, R. Shakir, “Segment Routing Architecture, Internet Engineering Task Force,” July 2018, https://tools.ietf.org/html/rfc8402

[68] C. Filsfils, P. Camarillo, D. Voyer, S. Matsushima, Z. Li, “SRv6 Network Programming draft-ietf-spring-srv6-network-programming-02,” March 2020 https://tools.ietf.org/html/draft-ietf-spring-srv6-network-programming-02

[69] Gordon E. Moore, “Cramming more components onto integrated circuits, April 1965, https://newsroom.intel.com/wp-content/uploads/sites/11/2018/05/moores-law-electronics.pdf

- Similarly, for the exact same reason, the IoT device would still need to have to code to deal with the long, variable length address of the server, defeating entirely the purpose of having small addresses.
- According to forecasts, there should be more than 20 billion IoT devices by 2030[70]. Some forecasts even call for one trillion IoT devices[71]. Given these numbers of devices, and assuming there are no translational gateways, it would be impossible to number all of them using very small length addresses: a minimum of 40 bits (2^40=1,099,511,627,776) would be necessary to number them all in a flat space, and a lot more in a hierarchical space, which would be required to do any kind of routing at the scale of the Internet.
- Regular servers using IPv4 or IPv6 would not be able to communicate directly with such IoT devices. All of those servers would need to be upgraded to the New IP addressing scheme.

This last point is a major hurdle. It demonstrates clearly that the New IP variable length addresses cannot be backward compatible with IPv4 or IPv6. As such, New IP has to be seen as a complete replacement of IP, not just an add-on. As we've seen with the challenges in IPv6 deployment, complete replacements have very long transition times, often measured in decades. If New IP were to somehow interoperate with IP, it would require some form of gateway. This defeats the stated goal of FG NET-2030 and its terms of references "It should ensure that the future network systems and applications remain fully backward compatible."[72] The introduction of these gateways will mean increased operating and capital costs and added complexity to network operations.

To claim that New IP can easily interoperate with IP, New IP proponents point to the New IP header structure described in section 3.4 and the fact that a New IP header can use either an IPv4 address, an IPv6 address, or a variable length address independently as the source and destination addresses of the packet.

Mixing and matching the IP address family in an IP header is a novel approach; however several points should be considered:

- Any intermediary device receiving a datagram with mixed address families would need to understand both related protocols, if only to return Internet Control Message Protocol (ICMP) control messages or apply proper treatment. In practice, it means that there is a need for a middle box performing network address translation between the two address families somewhere at the edge of both networks.
- This mechanism does not take into account payloads that may carry IP addresses. Which IP address families should those inner addresses be? The framework[73] does not mention this case, which is fairly common. Typical examples of such applications are

[70] "Number of active IoT devices expected to reach 24.1 billion in 2030," Help Net Security, May 2020,https://www.helpnetsecurity.com/2020/05/22/active-iot-devices/

[71] "One trillion new IoT devices will be produced by 2035," Arm Technologies, https://learn.arm.com/route-to-trillion-devices.html

[72] "Terms of Reference: ITU-T Focus Group on "Technologies for Network 2030" (FG-NET-2030)," Focus Group Net 2030, https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/ToR.pdf

[73] Richard Li, Kiran Makhijani, Lijun Dong Futurewei Technologies, "New IP: A Data Packet Framework to Evolve the Internet", invited paper, May 2020, IEEE 21st International Conference on High Performance Switching and Routing (HPSR) 2020

network management, routing protocols, any multimedia application using the Session Initiation Protocol (SIP, RFC 3261[74]) and any other applications that make a referral to a third party. Those applications would require application level gateways to work across a New IP to IP boundary. Such gateways come with their own set of complexities and issues.

- IPv4, IPv6, and variable length addresses are not encoded in the same number of bits: 32 for IPv4, 128 for IPv6, and a variable number for variable length addresses. Using one format in the header has consequences on the payload. Because of the fixed Maximum Transmission Unit (MTU), usually set to 1500 on any given link, the maximum payload of the packet is equal to the difference of the MTU and the header size. If address families are changed anywhere en route, there is a chance that the payload will no longer fit, and the packet would have to either be discarded, in the case of the IPv6 protocol, or fragmented, in the case of the IPv4 protocol. This would have an adverse effect on end-to-end traffic. This situation is well known with the current translation of IPv4 packets to IPv6 packets. There are ways to mitigate this effect when using the TCP transport protocol, but none are satisfying when using the UDP transport protocol, which is the default for applications such as DNS.

As such, this New IP feature of being able to carry IPv4, IPv6, or mix and match types does not guarantee interoperability. At best, it can be conceived as a hybrid between tunneling and network address translation (NAT). Trying to interoperate New IP and IP would face similar challenges to the interoperability between IPv4 and IPv6: there is no smooth transition path, and a co-deployment of these protocols that could potentially span multiple decades would have to be taken into account.

4.5 ManyNets

The Internet is defined as a “network of networks,” which seems to be, at least at a high level, identical to the notion of ManyNets defined as “seamless coexistence of heterogeneous network infrastructures” as seen in Section 4. Unfortunately, the definition and explanations of the concept of ManyNets, as described in [Blueprint] and [Forwarding], is not detailed enough to provide a clear understanding of what it entails.

One can still glean some hints in the [Blueprint] with the sentence “Quite likely there will not be just one, but many public Internets.” This seems to hint at a fragmented public Internet, potentially using different sets of unique identifiers and addresses. If and how these ManyNets would be interconnected is not explained in the current sets of documents.

Section 4.3 of [Blueprint], provides another hint: “The fact that global scale connectivity must go through public infrastructure now remains an outdated conjecture.” That section then goes on to mention “the proliferation of ‘private transits,’ ‘space communications,’ and the ‘Densification of distributed edges’ and concludes “it is difficult to think in terms of a single backbone.” It is worth remembering that the Internet is not, and has never been, a single backbone. It is a collection of backbones operated by independent entities, with independent, and sometimes conflicting, business models, and relying on different technologies.

[74] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, “SIP: Session Initiation Protocol,” June 2002 https://tools.ietf.org/html/rfc3261

[Blueprint], section 4.3 goes further. It states "The challenge is in finding innovative ways to solve accounting, diverse capability, and reachability problems, providing classes of citizenship, and a safe harbor to users and their assets. Emergence of such federated networks will be imminent, and Network 2030 undertakes this challenge in order to identify requirements in network technologies, understand this behaviour, and provide dynamic regulatory-binding mechanisms." The key point in this paragraph appears to be the notion of a federated set of networks ruled by regulatory binding mechanisms.

This Network 2030 concept of ManyNets is expanded on in New IP in [IETFtoITU]: "The network needs to provide specific QoS and security policies based on user identity." How exactly this would be achieved is unspecified.

In the current Internet, the binding between an IP address and the user is a private contract between the user and its ISP. (In the case of Carrier-grade NAT, the binding is between a user and an IP address/port number.) Outside of the perimeter of that ISP, that binding is invisible. Users are simply seen as customers of that ISP. They are free to access any content of their choosing in keeping with the agreed-upon contractual terms. Law enforcement authorities can request the ISP to disclose that binding, but usually only on a case by case basis, in accordance with local requirements and regulations. Including in the Internet architecture a strong regulatory binding of user identity to a New IP address can have far reaching consequences and would appear to run against efforts to increase privacy of Internet communications. Because there would be a strong regulator binding of user identity to the New IP address, in theory any intermediary system on the Internet could have access to anyone's real identity and browsing habits simply by observing the New IP addresses of their traffic as it passes through intermediary networks. This binding would certainly make the work of law enforcement agencies to fight crime a lot easier, but at the price of obvious privacy, including those associated with the European General Data Protection Regulation (GDPR) and similar laws around the world, and control implications. It would also carry the risk of making pervasive monitoring much easier and potentially increasing oversight of the publication of content.

Furthermore, such an architecture, which does not exist in the current Internet, would open the door for regulations that could force application and content developers to first adhere to a regulatory framework mandating the reporting and tracking of all users' identities (in fact, the identities of all users browsing free content) and activities in order to get authorization to provide content and services. This would be a clear and complete departure from the permissionless innovation model, in which protocol developers can implement new technologies without needing to understand the myriad laws and regulations that may impede the use of those technologies in particular jurisdictions, that has been the characteristic of the Internet in the last several decades.

4.6 Internet TCP/IP Protocol Suite Track Record

Unsubstantiated claims that TCP/IP can't work for new applications or higher bandwidth have repeatedly been made every time a new access technology has arrived. One can remember Asynchronous Transfer Mode (ATM) (Ethernet can't go to 100Mbps), 3G (TCP/IP not suitable for handheld devices), and similar claims suggesting new technologies, particularly those championed by specific vendors or standards groups, were required. However, the track record of TCP/IP has been remarkable: it has been nimble enough to adapt every time a new underlying network technology has emerged. For example, Voice over IP (VoIP) was generally thought to be unrealistic in the late 1990s, but it has now largely displaced traditional telephony.[75] Similar considerations apply to video applications, as demonstrated by the success of video on demand (VoD) platforms such as Netflix and the many conferencing systems that have replaced physical meetings during the COVID-19 pandemic. In both cases (VoIP and VoD), the applications evolved to adapt to the variable network conditions and have resulted in a push for faster residential and Internet core bandwidth. Network deployment models also evolved at the same time to include content delivery network (CDN) caches. Another example of modular Internet evolution is the use of the QUIC[76] protocol by the YouTube web application. This evolution did not change the TCP/IP protocol suite. It was made possible by the open and modular nature of the Internet model.

Discarding or ignoring such a track record would be possible if a disruptive change in the underlying networking fundamentals were to dramatically alter the way the network is used in a positive way. Among the various use cases brought forward, the idea of using artificial intelligence to create self managing and self healing networks (such as described in [Requirements], section I.3) is the one that could be the most disruptive. However, this is an area that remains work in progress. It is too early to see if it could (or not) be retrofitted into the current Internet architecture.

4.7 Internet Architecture Board Criteria for Protocol Success

IP has evolved over the years and still needs to evolve. However, not all ideas or research proposals are successful. The Internet Architecture Board (IAB) published RFC 5218[77], "What makes for a Successful Protocol." This document mention a list of basic success factors that include:

- Positive Net Value (meets real need)
- Incremental Deployability
- Open Code Availability
- Freedom from Usage Restrictions
- Open Specification Availability
- Open Maintenance Processes
- Good Technical Design

Remembering that New IP has no complete, publicly available, specific design documents to review at this time, it is unclear that **any** of the above criteria are met by New IP.

5 Conclusion

Speed of light limitations could effectively limit some of the described use cases of Network 2030 to short distance deployments less than 100km. As such, efforts like New IP may be better

[75] "VOIP Adoption Statistics for 2019 & Beyond", https://wisdomplexus.com/blogs/voip-adoption-statistics-2019-beyond/

[76] J. Iyengar, M. Thomson, "QUIC: A UDP-Based Multiplexed and Secure Transport draft-ietf-quic-transport-29," June 2020, https://tools.ietf.org/html/draft-ietf-quic-transport-29

[77] Thaler D, Aboba B, IAB, "What Makes for a Successful Protocol?," RFC 5218, July 2008, https://tools.ietf.org/html/rfc5218

suited for ad-hoc deployments of highly specialized private networks. Trying to make them into a standardized, one-size-fit-all architecture, as has been done with IP, seems overly ambitious and unlikely to succeed.

Due to the lack of specification, it is worth noting that it is difficult to see New IP as a candidate for a protocol standard. Rather, it appears to be a list of perceived issues about the current Internet architecture and a list of desired features. At a very high level, these desired features can be summarized as variable length addresses, ManyNets and better-than-best-effort networking.

Although the New IP header can carry IPv4 or IPv6 addresses, New IP would not appear to be fully compatible with IP; as such, it would have to be deployed in parallel to existing IP-based networks, forcing the use of gateways to connect to the current Internet. The introduction of these gateways will mean increased operating and capital costs and added complexity to network operations. Such a deployment model places a very high bar for adoption, especially when considering the still lackluster adoption of IPv6 twenty five years after its definition.

Better-than-best-effort networking appears to suggest a return to circuit-switched technology, harking back to ATM days. (It is worth noting that it is generally accepted that ATM failed in the marketplace[78].) It is unclear whether the benefits from such a technology would outweigh the deployment costs.

The notion of ManyNets, understood as a federated set of networks, brings along not only the end of a single Internet model, but also the prospect of a strong regulatory binding between an IP address and a user that could make pervasive monitoring much easier and increase the oversight of published content.

Also it is worth remembering that the success of the TCP/IP protocol suite is tied to the notion of a simple, global network connecting smart edges. As the content delivery network (CDN) caches have shown, the exact definition of what is the core and what are the edges has evolved over time, but the overall model remains the same. The TCP/IP model has led to the flourishing of new applications, accelerating innovation up to an unprecedented rate. A return to the old telephony model of circuit switching, with smart networks controlling every communication and simple, dumb edges implied by that model, has the potential to break this dynamic. The overall opportunity cost tied to the loss of the permissionless innovation model characteristic of the Internet could be very high. History has shown that successful technology evolution is either incremental (let’s build a better mousetrap) or disruptive (the invention of the refrigerator rendered ice factories obsolete). It is unclear whether New IP falls in any of these two categories.

[78] “The demise of ATM”, https://technologyinside.com/2007/01/31/part-1-the-demise-of-atm…/