

Discussion Paper: An analysis of the "New IP" proposal to the ITU-T

Hascall Sharp (author), Olaf Kolkman (Internet Society editor)

This is a discussion paper. This paper represents the Internet Society's emerging opinion, but does not represent a final Internet Society position. Instead, we intend it as a means to gather information and insight from our community on the topic. Comments are welcome. Contact the authors directly on newIP-discussion-paper@isoc.org or post to the discussion-papers@elists.isoc.org mailing list, which is public and archived.

Executive Summary

The Internet continues to evolve at a rapid pace. New services, applications, and protocols are being developed and deployed in many areas, including recently: a new transport protocol (QUIC), enhancements in how the Domain Name System (DNS) is accessed, and mechanisms to support deterministic applications over Ethernet and IP networks. These changes are only possible because the community involved includes everyone from content providers, to Internet Service Providers, to browser developers, to equipment manufacturers, to researchers, to users, and more.

Given this backdrop it is concerning that a proposal has been made to ITU-T¹ to "start a further long-term research now and in the next "study period" to develop a "top-down design for the future network."

A tutorial/presentation has also been given at several ITU-T meetings supporting this proposal and providing more detail. The proposal refers to this future network as the "New IP protocol system" and claims the following challenges faced by the current network (the Internet) as the primary reasons for a new architecture:

- The need to **support heterogeneous networks** (called ManyNets²) and the need to support "more types of devices into the future network." "[T]he current network system risks becoming 'islands'"
- The need to **support Deterministic Forwarding** globally.
- The need to **enhance security and trust** and support "Intrinsic Security"
- The ability to **support ultra-high throughput** and allow user-defined customized request for network services and get fine-grained information on the status of the network.

The Focus Group on Technologies for Network 2030 (FG NET-2030) is tasked with investigating "the future network architecture, requirements, use cases, and capabilities of the networks for 2030 and beyond."³ The IETF, IEEE, 3GPP, ETSI and other SDOs are also busy developing new protocols, and enhancing current protocols, to provide new capabilities.

¹ Telecommunication Sector Advisory Group (TSAG) contribution T17-TSAG-C83 [C83], presented at the September 2019 TSAG meeting.

² Manynets" is a translation of "万网"

³ <https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/ToR.pdf>

ManyNets, Islands of connectivity and interoperability

Communicating over multiple, heterogeneous technologies (including satellite systems), and avoiding islands of communication due to the diversity of networking technology, have been core design goals in the evolution of the Internet over the last 40 years.

Deterministic Networking

The IETF's deterministic networking [DETNET] and reliable and available wireless [RAW] working groups, and the IEEE 802.1 Time Sensitive Networking [TSN] task group, are developing standards related to deterministic networking, liaising with ITU-T SG15 and 3GPP.

Security

The IETF addresses security in specific protocols (e.g., BGP Security (BGPSEC), DNS Security (DNSSEC), Resource Public Key Infrastructure (RPKI), etc.) as well as by requiring a security consideration section in each RFC, taking into account research and new developments. The IEEE addresses Media Access Control (MAC)-level security in its protocols (e.g., IEEE 802.1AE, IEEE 802.11i).

Transport

The IETF Transport Area develops transport protocols (e.g., Stream Control Transmission Protocol (SCTP), Real-time Protocol (RTP) and Real-time Communications for the Web (WebRTC), and QUIC) and active queue management protocols (e.g., the Low Latency, Low Loss, Scalable Throughput service architecture (L4S) and Some Congestion Experienced (SCE) ECN Codepoint). These increase throughput, lower latency, and further support the needs of real-time and multimedia traffic, while considering interactions with, and effects on, TCP traffic on the Internet.

Consideration of this proposal for a new global protocol system should take into account the following:

- **Creating overlapping work is duplicative, costly, and in the end does not enhance interoperability.** The alleged challenges mentioned in the proposals are currently being addressed in organizations such as IETF, IEEE, 3GPP, ITU-T SG15, etc. Proposals for new protocol systems and architectures should definitively show why the existing work is not sufficient. Although the term "New IP" is frequently used and the proposals would replace or interact with much of the Internet infrastructure, the proposals have not been brought into the IETF process.
- **The billions of dollars of investment in the current protocol system and the effects on interoperability to prevent the development of non-interoperable networks.** Any new global protocol system will be costly to implement and may result in unforeseen effects on existing networks.
- **The need for business and operational agreements (including accounting) between the thousands of independent network operators.** Implementing a new protocol system is not simply about the protocols, there are myriad other systems that will need to be addressed outside the technical implementation of the protocols themselves.

- **The likelihood that QoS aspects of the proposal would complicate regulatory and legislative matters in several areas.** These areas could include licensing, competition policy, data protection, pricing, or universal service obligations.

When an organization (e.g., 3rd Generation Partnership Project (3GPP)) has identified a need to develop an overall architecture to provide services a successful model has been to identify the services and requirements first. Then work with the relevant standards organizations to enhance existing protocols or develop new ones as needed.

Developing a new protocol system is likely to end up with multiple non-interoperable networks, defeating one of the main purposes of the proposal. A better way forward would be to:

- Allow the FG NET-2030 to complete its work and allow the Study Groups to analyze its results in relation to existing industry efforts.
- Review the use cases developed as part of the Focus Group's outcomes
- Encourage all parties to contribute to further investigate those use cases, as far as they are not already under investigation, in the relevant SDOs. .

Introduction

At the September 2019 TSAG meeting, Huawei, China Mobile, China Unicom, and China Ministry of Industry and Information Technology (MIIT) proposed to initiate a strategic transformation of ITU-T. In the next study period the group aims to design a "new information and communications network with new protocol system" to meet the needs of a future network [C83]. This effort is in reference to the ongoing work in the Focus Group on Technologies for Network 2030. At the same meeting, Huawei gave a tutorial [TD598] illustrating their views in more detail and suggested that ITU-T Study Groups set up new Questions "to discuss the future-oriented technologies."

The contribution and tutorial posit that the "telecommunication system and the TCP/IP protocol system have become DEEPLY COUPLED into a whole." The ITU-T should therefore develop an even more deeply coupled system using a new protocol system, ultimately replacing the system based on TCP/IP.

C83 claims there are **three key challenges** facing the current network:

"Firstly, due to historical reasons, the current network is designed for only two kinds of devices: telephones and computers. [. . .][The] development of IoT and the industrial internet will introduce more types of devices into the future network."

"Secondly, the current network system risks becoming 'islands', which should be avoided."

"Thirdly, security and trust still need to be enhanced."

The tutorial provided by Huawei [TD598] during the meeting suggested **three main areas for improvement** as justification for the new network architecture:

- Interconnecting ManyNets (connect heterogeneous Networks)
- Deterministic Forwarding
- Intrinsic Security

The tutorial also mentions **two other areas for study**:

- User-defined customized request for Networks
- Ultra-high throughput

Key Elements of the proposed "New IP" protocol system

ManyNets and "islands" of communications

A main pillar of the proposed new protocol system is the concept of ManyNets. ManyNets refers to the myriad heterogeneous access networks with which the proposed new system needs to interconnect (e.g., "connecting space-terrestrial network, Internet of Things (IoT) network, industrial network [sic] etc."[C83]).

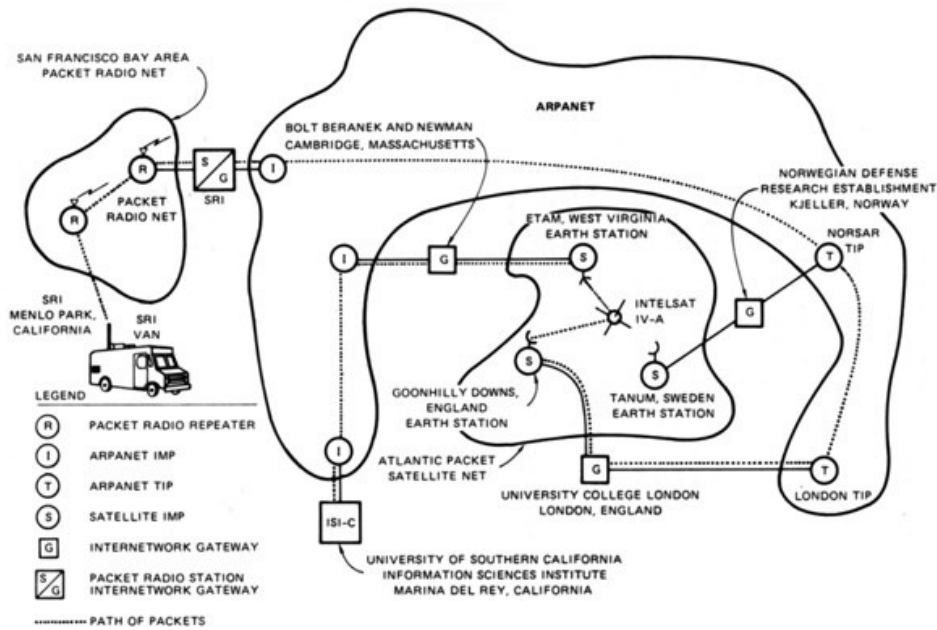
One argument is that the "diversity of network requires new ways of thinking." Another is that new technologies are developing their own protocols to communicate internally and that the "whole network could potentially become thousands of independent islands." Under the discussion of ManyNets, the "New IP" framework proposes a flexible length address space to subsume all the possible future types of addresses (IPv4, IPv6, semantic ID, service ID, content ID, people ID, device ID, etc.).

To better understand the current structure of the Internet we must first go back to how the Internet was initially created. From its inception, the Internet was designed to interconnect different network types. In Internet Experiment Note 48 [IEN48], a 1978 paper in a series of technical publications that document the work that led to the Internet, Vint Cerf wrote:

The basic objective of this project is to establish a model and a set of rules which will allow data networks of widely varying internal operation to be interconnected, permitting users to access remote resources and to permit intercomputer communication across the connected networks.

Figure 1 shows a demonstration of TCP/IP in 1977 that interconnected at least three types of networks (packet radio, satellite, ARPANET). This illustrates that interconnecting with and over wireless, wireline, and satellite networks has been included in the development of TCP/IP since the beginning.

Figure 1- TCP/IP demonstration, linking the ARPANET, PRNET, and SATNET in 1977⁴



The Internet architecture has proven to be adaptable as networking technology has evolved over the last 40 years, from 300 baud dial-up modems to multi-gigabit fiber. The decoupling of IP from the underlying network technology provides flexibility to support specific requirements on a particular network while allowing the different networks to be interconnected. Table 1 provides a subset of networking technologies over which IP runs.

The current Internet consists of upwards of 60 thousand independent "islands." These are called autonomous systems, with each making its own technology choices to serve its customers/users and interconnecting using interdomain routing protocols and bilateral agreements. Experience has shown that most of the problems (including creation of "islands") related to interconnecting networks are due to non-technical business, accounting and policy reasons. **Defining a new protocol system will not resolve these problems.**

⁴ Public Domain - from <https://en.wikipedia.org/wiki/ARPANET>. Original source - Computer History Museum

Table 1- Example technologies over which IP runs

| Personal Area Network | LAN | SAN | WAN | MAN | Mobile Wireless |
|--|---|---|---|--|---|
| <ul style="list-style-type: none"> • 6LoWPAN, IEEE 802.15.4 • Bluetooth • ITU-T G.9959. | <ul style="list-style-type: none"> • Ethernet (802.3), Token Bus (802.4), Token Ring (802.5) • ArcNet • 802.11 • FDDI | <ul style="list-style-type: none"> • FibreChannel • Infiniband • HIPPI | <ul style="list-style-type: none"> • Frame Relay • ATM • SONET/SDH • Leased line • dial-up modem • ISDN • X.25 • Satellite • DOCSIS (Cable) • Television Signals (VBI, MPEG2) | <ul style="list-style-type: none"> • SMDS • 802.16 (WiMAX) | <ul style="list-style-type: none"> GPRS, LTE, 5G |

Deterministic Networking

C83 and its associated tutorials claim that some applications and services have **tight timing** (e.g., latency, jitter), reliability and loss requirements that are not necessarily met over the Internet today. Examples given of such applications are telemedicine (e.g., remote surgery), industrial, and vehicular applications. While telemedicine, industrial, and vehicular applications have run over the Internet for years, there have been challenges to deploying QOS to meet every demand. Recognizing this, deterministic networking is being studied and standards are being developed in several key organizations:

- **IEEE 802.1** Time Sensitive Networking (TSN) Task Group [TSN] is developing extensions to support time sensitive networking using IEEE 802.1 networks.
- **IETF Deterministic Networking** (detnet) and Reliable and Available Wireless (raw) working groups are developing RFCs to support deterministic networking on routed networks and to interwork with IEEE 802.1 TSN. The IETF's Transport Area also continues its work in this area, for example its investigation of Low Latency, Low Loss, Scalable Throughput (L4S) Internet Service and active queue management.
- **3GPP** is defining standards to support its 5G ultra-reliable low latency communications (URLLC) capability over the Radio Access Network (RAN) as well as interworking with 802.1 TSN networking.
- **ITU-T SG15** is working with IEEE 802.1 TSN and 3GPP (5G) related to its transport-related Recommendations.

The above listed efforts tend to focus on applications that exist within a single administrative domain. Any proposal that claims to guarantee delivery of information over a network within certain parameters must address the physical limitations associated with data traversing distance (e.g., the speed of light).

The proposals in C83 and its associated tutorials don't make mention of any of the existing efforts or why a duplicative work stream is needed. In addition, it exhibits no recognition of the non-technical

inter-domain issues (e.g., business relationships, regulatory concerns) that will not be solved by a new protocol system.

Intrinsic Security

The third challenge identified in C83 states that "security and trust still needs to be enhanced" and that "a better security and trust model need to be designed and deployed" in addition to promoting "secure and reliable data sharing schemes." Several areas are called out in the tutorial:

Authenticity (e.g., IP address spoofing)

Accountability vs. Privacy

Confidentiality & Integrity

Availability (Distributed Denial of Service (DDOS) attacks)

While these areas of security would certainly be important for any new ground-up network technology design, solutions to many of these problems already exist in current networking technologies and the last decade has seen a wealth of investment in strengthening them.

It is also important to understand the difference between defining a capability in a standard and deploying it in operational networks. For example, methods for authenticating users connecting to the Internet and detecting and preventing IP address spoofing have been defined in RFCs and available on equipment for years, but aren't necessarily deployed in all networks.

While it is easy to claim that all these capabilities are intrinsically part of any new network architecture, it is much harder to ensure that they are actually deployed in operational networks. For example, while IPsec was included in the initial IPv6 specification [RFC1883], it has not been widely utilized especially in consumer markets. While a government can mandate deployment of a new network technology, such a mandate does not enhance global interoperability.

The proposal also doesn't distinguish between those capabilities that mandate a new architecture vs. those capabilities that could theoretically be run over the current routing infrastructure. For example, the proposal makes statements regarding the **Public Key Infrastructure (PKI) Certificate Authority (CA)** system relying on a single point trust anchor or vulnerabilities in key exchange. These are important points of discussion for any architecture, in fact they are being discussed in the relevant communities in the context of the current Internet infrastructure and don't require a completely new architecture.

Finally, networking protocols face inherent trade-offs between openness and security. While lack of ubiquitous deployment of strict mandatory authentication can contribute to spoofing and denial-of-service attacks, it also contributes to the ease of users to connect and reap the benefits of the Internet's global connectivity. Also, network operators understand that mandatory authentication adds expense and complexity to network operations.

Ultra-high throughput, new transport architectures

C83 and its associated tutorials emphasize the need for ultra-high throughput to support future projected applications such as holographic communication. While the bandwidth required for support of such applications will be the subject of research and development over the next decade (e.g., ITU-T SG15 on optical transport, the IEEE P802.3bs Task Force on Terabit Ethernet), the proposal focuses on the need for a new transport architecture, including user-defined customized requests for network service and network-awareness of transport and application.

The tutorial presented in support of the proposal for work on a new transport contains specifics of the network protocol and network operation clearly oriented toward Huawei's Big Packet Protocol [BPP] as opposed to laying out requirements indicating a need for a new transport. Huawei has submitted a contribution to SG11 to initiate studies on a new transport protocol [C322].

While TCP is the most widely used transport protocol on the Internet, the IETF has continued to develop other transport protocols as needed, for example real-time transport protocol work goes back to the early 1970's and the IETF has defined the real-time transport protocol (RTP) [RFC3550] for use by multimedia applications. There is active work in IETF to improve and enhance RTP for new applications including the recent development of WebRTC in collaboration with W3C.

There has been tremendous focus in recent years on performance improvements, most prominently with the development of the UDP-based QUIC protocol that is expected to become one of the most widely deployed transport protocols on the Internet. The IETF continues its work on transport protocols in its Transport Area (tsv) to investigate new requirements and where it can take into account lessons learned from operation of the Internet.

The participants in the IETF's Transport Area have years of experience in developing and operating transport protocols over the Internet. They take into account interaction with currently deployed protocols when investigating new protocols to ensure that new proposals have a viable deployment path and minimize harmful effects on the current Internet. Companies are encouraged to take advantage of this experience when making new proposals to avoid duplicative work streams.

C83 and its associated tutorial also throw in a number of technologies that have been investigated over the last few decades such as network coding, service-oriented routing, network computing, and source routing. Many of these topics are already under investigation in the Internet Research Task Force (IRTF), including:

- Coding for efficient NetWork Communications Research Group (nwcrg) (<https://datatracker.ietf.org/rg/nwcrg/>)
- Computing in the Network Research Group (coinrg) (<https://datatracker.ietf.org/rg/coinrg/>)
- Information-Centric Networking (icnrg) (<https://datatracker.ietf.org/rg/icnrg/>)
- Path Aware Networking RG (panrg) (<https://datatracker.ietf.org/rg/panrg/>)

Key Considerations

Interoperability and creation of "islands"

One of the concerns listed in C83 for the current network system is the risk of creating islands of non-interoperability, requiring complex "translators" between the islands. While the proposal talks about utilizing a flexible address space that can contain IPv4 or IPv6 addresses, there is no mention of interoperability with IP routing or the Internet. Creation and deployment of a new protocol and network architecture in ITU-T as described in the tutorial is likely to create the same interoperability problems the proposal claims to want to avoid.

In addition, networks will continue to migrate to IPv6 over the next decade, with the need to support pockets of IPv4 during that migration. Introducing a new protocol system that is not backward compatible or interoperable with IP (v4 or v6) would require the need for yet another decades-long migration, requiring tens of billions of IP-enabled nodes to interwork and interconnect with the new system.

Merely providing a variable-length address does not solve the problem. Creating a new protocol system to "solve" a perceived interoperability problem adds *another* interoperability problem and because of increased complexity likely adds security and resiliency issues as well.

Complexity/cost

C83 and its associated tutorial include elements (e.g., User-defined customized request for Networks, source routing, deterministic routing) that would create a more tightly coupled system from applications on endpoints through to network elements. Similar capabilities have been standardized before.

For example, in the 1990's, the IETF developed the Integrated Services (IntServ) architecture [RFC1633] as well as the Resource ReSerVation Protocol (RSVP) [RFC2205] to support real-time services. Industry also developed APIs (e.g., <https://pubs.opengroup.org/onlinepubs/9619099/chap2.htm>) to allow applications to request these new capabilities.

Although these capabilities were implemented, trialed, and deployed in a limited manner on specific networks (e.g., enterprise), they were never rolled out in the Internet as a generally available service. The complexity and cost of deploying and operating such a service, especially across domains operated by different business entities, were significant reasons for lack of deployment on a global scale[PANRNT]. Any service that requires allocation of per-router per-flow resources is likely to run into similar obstacles[HUSTON].

Such prospective deployments tie into business agreements, the need to account and bill for usage of enhanced service, and the allocation of resources for the enhanced service that could be used for basic service. Those non-technical costs generally outweighed the benefits of enhanced services and are not addressed by C83 or its associated tutorials. Based on experience in operational networks, less fine-grained capabilities were developed (e.g., Differentiated Services (diffserv)) for traffic engineering.

Use of Building blocks in network architectures

The design and deployment of services are generally tailored to the target customer base, for example, business-oriented services vs. consumer-oriented service. Industries with strict and business-critical requirements tend to utilize services tailored to their needs rather than use a general-purpose network

designed for consumer use. Similarly, network providers generally don't build general-purpose consumer-oriented networks with the capabilities required for meeting the needs of such industries.

Instead of designing a top-down new architecture integrating all possible functions, the Internet has grown by providing a more general loosely-coupled architecture. Capabilities can be integrated that are required for specific services for particular customer needs.

The IETF and others (e.g., IEEE, ITU-T SG15) have evolved their protocols to provide building blocks of mostly independent utility to address identified needs. This flexibility allows network operators to utilize those building blocks needed to provide the desired services. This allows the Internet to evolve to meet new challenges. RFC 5218 [RFC5218] provides general principles and case studies for success factors in developing new protocols.

While it is tempting to develop an integrated "top-down" design of a global network architecture defining a completely new protocol system meeting all possible requirements, the end result of such efforts has usually been for network operators to pick out pieces of the architectures of most utility (e.g., ATM PVCs) and leaving the rest.

Decades of experience with the development of Internet protocols demonstrated the importance of the critical feedback loop between implementation, deployment, and protocol design. As draft protocols get implemented and tested, bugs and optimizations are discovered. Data is gathered that is then fed back into the design before it gets finalized.

The IETF embedded this feedback loop into the standardization process. At times dozens of independent implementations are being developed and deployed at scale prior to the standardization of a new protocol.

Organizations such as the Broadband Forum (BBF) and MEF have likewise stood up major software development efforts that feed into their development processes. Attempting to design major new protocols ignores what has become the industry best practice method of protocol development: implementing, deploying, and designing in parallel to ensure new protocols can be successful.

A successful model for developing an overall architecture from some organizations (e.g. 3GPP) has been to identify the services and requirements and then work with the appropriate standards organizations to enhance existing protocols, or develop new ones if shown to be needed.

Research

While it is important to take a long-term view and develop potential uses cases for future networking, it is also important to recognize that research topics are not generally appropriate for standards development. Technology should reach a sufficiently mature level of understanding *before* international standardization. For example, as stated in SG16's response to the liaison regarding "New IP", related to the proposed work on hologram communications[TD697]:

Given that the hologram is still in very early stage of research, SG16 does not have a technology base on the hologram. It is premature for SG16 to start the hologram-specific content delivery work.

The studies underway in the FG NET-2030, once completed and analyzed by the Study Groups, might provide direction for research and development of technologies and identify areas to monitor for future standardization in the appropriate venue. While some of its work might be used to provide direction for research, they won't necessarily provide a basis for standardization of protocols. As mentioned

previously, the IRTF has research groups already engaged in some of the areas identified by FG NET-2030.

Conclusion

From its inception, the Internet was designed to interconnect heterogeneous networks. The alleged challenges mentioned in C83 have been addressed, or are currently being addressed, in organizations such as IETF, IEEE, 3GPP, ITU-T SG15. Creating overlapping work is duplicative and costly. In the end, it does not enhance interoperability.

Proposals for new protocol systems and architectures should definitively show *why* the existing work is not sufficient. Creating a new protocol system will require yet another expensive migration effort on top of the current migration to 5G, NGN and IPv6. Member States should consider sunk cost, investment protection, and compatibility with the embedded base.

The studies underway in the FG NET-2030 could also provide direction for research and development of technologies for monitoring to determine the need for standardization. It would be premature to start work on new protocol systems before the FG NET-2030 completes its work and the Study Groups have had a chance to analyze it. That analysis should consider current efforts and architectures.

Consideration of a new protocol system must take into account the embedded base of equipment and operational systems supporting the multi-billion dollar global online economy. Developing a new protocol system is likely to create multiple non-interoperable networks, defeating one of the main purposes of developing the new protocol architecture. A better way forward would be to allow the FG NET-2030 to complete its work, review the use cases developed as part of the Focus Group's outcomes and encourage all parties to further those, as far as they are not already under investigation, in the relevant SDOs.

References

- [BPP] R. Li, K. Makhijani, H. Yousefi, C. Westphal, L. Dong, T. Wauters, and F. D. Turck. A framework for qualitative communications using big packet protocol. ACM SIGCOMM Workshop on Networking for Emerging Applications and Technologies (NEAT'19), 2019. <https://arxiv.org/abs/1906.10766>.
- [C322] T17-SG11-C-0322. Source: Huawei Technologies. Propose new research for next study period: the New Transport Layer (Layer-4) Protocols. Geneva, 16-25 October 2019.
- [DETNET] <https://datatracker.ietf.org/wg/detnet/about/>
- [HUSTON] Huston, G., "The QoS Emperor's Wardrobe". The ISP Column, 2012-06. <<https://labs.ripe.net/Members/gih/the-qos-emperors-wardrobe>>
- [IEN48] Cerf, V., "The Catenet Model for Internetworking," IEN 48, July 1978. <<http://www.isi.edu/in-notes/ien/ien48.txt>>
- [PANRNT] Dawkins, Spencer, "Path Aware Networking: Obstacles to Deployment (A Bestiary of Roads Not Taken)", draft-irtf-panrg-what-not-to-do-07 (Work in Progress), January 2020, <<https://datatracker.ietf.org/doc/html/draft-irtf-panrg-what-not-to-do-07>>.

[RAW] <https://datatracker.ietf.org/wg/raw/about/>

[RFC1633] Braden, R., Clark, D., and S. Shenker, "Integrated Services in the Internet Architecture: an Overview", RFC 1633, DOI 10.17487/RFC1633, June 1994, <<https://www.rfc-editor.org/info/rfc1633>>.

[RFC1883] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 1883, DOI 10.17487/RFC1883, December 1995, <<https://www.rfc-editor.org/info/rfc1883>>.

[RFC2205] Braden, R., Ed., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, DOI 10.17487/RFC2205, September 1997, <<https://www.rfc-editor.org/info/rfc2205>>.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, DOI 10.17487/RFC3550, July 2003, <<https://www.rfc-editor.org/info/rfc3550>>.

[RFC5218] Thaler, D. and B. Aboba, "What Makes for a Successful Protocol?", RFC 5218, DOI 10.17487/RFC5218, July 2008, <<https://www.rfc-editor.org/info/rfc5218>>.

[TD598] TSAG-TD598, Source: Director, TSB, "Tutorial on C83 - New IP: Shaping the Future Network". Geneva, 23-27 September 2019.

[TD697] TSAG-TD697, Source: Study Group 16, "LS/r on new IP, shaping future network (TSAG-LS23) [from ITU-T SG16]", Geneva, 10-14 February 2020.

[TSN] IEEE Time-Sensitive Networking Task Group: <https://1.ieee802.org/tsn/>

Standards Groups Mentioned

Broadband Forum (BBF): <https://www.broadband-forum.org/>

3rd Generation Partnership Project (3GPP): <https://www.3gpp.org>

ETSI: <https://www.etsi.org>

Institute of Electrical and Electronics Engineers - Standards Association (IEEE-SA):
<https://standards.ieee.org>

International Telecommunication Union - Telecommunication Standardization Sector (ITU-T):
<https://www.itu.int/en/ITU-T/>

ITU-T Study Group 15 (SG15): <https://www.itu.int/en/ITU-T/studygroups/2017-2020/15/Pages/default.aspx>

ITU-T Study Group 16 (SG16): <https://www.itu.int/en/ITU-T/studygroups/2017-2020/16/Pages/default.aspx>

Internet Engineering Task Force (IETF): <https://www.ietf.org>

Internet Research Task Force (IRTF): <https://www.irtf.org>

MEF: <https://www.mef.net>

Other Background Resources

Jiang Weiyu, Liu Bingyang, Wang Chuang. Network architecture with intrinsic security. Telecommunications Science[J], 2019, 35 (9): 20-28 (last found at <http://www.infocomm-journal.com/dxkx/EN/10.11959/j.issn.1000-0801.2019215>) (original Chinese)

Qiang Qiang, Liu Bingyang, Yu Delei, Wang Chuang. Large-scale deterministic network forwarding technology. Telecommunications Science[J], 2019, 35 (9): 12-19 (last found at <http://www.infocomm-journal.com/dxkx/EN/10.11959/j.issn.1000-0801.2019213>) (original Chinese)

Li Guangpeng, Jiang Sheng, Wang Chuang. Network layer protocol architecture for many-nets internetworking. Telecommunications Science[J], 2019, 35 (10): 13-20 (last found at <http://www.infocomm-journal.com/dxkx/EN/10.11959/j.issn.1000-0801.2019224>) (original Chinese)

Zheng Xiuli, Jiang Sheng, Wang Chuang. NewIP[sic]: new connectivity and capabilities of upgrading future data network. Telecommunications Science[J], 2019, 35 (9): 2-11 (last found at <http://www.infocomm-journal.com/dxkx/EN/10.11959/j.issn.1000-0801.2019208>) (original Chinese)

Wan Junjie, Li Taixin. New transport layer technology. Telecommunications Science[J], 2019, 35 (10): 43-50 (last found at <http://www.infocomm-journal.com/dxkx/EN/10.11959/j.issn.1000-0801.2019225>) (original Chinese)