A Brief Introduction about New IP Research Initiative

The Next-generation Network and Protocol System for Digital Networked Industry and Society

This article outlines the reasoning behind the New IP initiative, addressing the motivation (**why**) of the work, the definition and work areas of investigation (**what**) as well as the current progress (**how**). This is to clarify misunderstandings of what New IP entails as well as outline for our future partners on why and how to engage with us on this endeavor.

Why New IP?

For this, the ITU-T Network 2030 Focus Group [1] established in July 2018, has been working on building consensus in the industry on the next evolution of Internet technologies, fit for purpose in 2030 and beyond. The **societal and industrial digitalization** will affect many vertical industries through enabling, for instance, industrial manufacturing through novel means for virtual and augmented reality or transforming education through full-view holographic multimedia. Communication means will include but not be limited to satellite networks, networked aircrafts and Internet of Vehicles, while also utilizing vast amounts of sensor network deployments with lightweight devices. The communication requirements of such digitalization is seen to accelerate the already changing focus from human-oriented communication to machine-oriented communication. Often large-data transmission is no longer the first target and the assumption that "large bandwidth is equal to high quality" is no longer universally applicable. Instead, **determinism** that provides network-layer certainty of information transmission becomes more important. One trillion [2] devices are being expected to be connected to the Internet in 2035 with **heterogeneous**, often **resource-constrained**, devices being connected via **dynamic network topologies**. As a result, networks need to cope with **high dynamics** and complex **heterogeneous topologies** while also supporting **multi-channel concurrency** (due to increasing access technology opportunities) and **multi-channel collaboration** (due to complex services with inter-twined dependencies for transmitted information). In all this, the need for **security** and **privacy** of information but also the infrastructure is ever increasing, together with the need to achieve **sustainable efficiency** of the utilized technologies.

Identifying the requirements has only been the first step, followed by outlining technology study areas for addressing them – we collectively call the set of these emerging study areas New IP and will outline them briefly in the following.

What is New IP?

New IP can be characterized as a **technology study initiative**, driven by a **vision** on scenarios for utilizing Internet technologies in many facets of the future **digital industry and society**. As such research initiative, it is centered on **study areas** that address aspects of the Internet data plane as well as its associated architecture, technologies and protocols. These study areas address the **identified requirements** from associated efforts such as ITU-T Focus Group Network 2030 [3][4]. New IP technology study initiative is not relevant to the governance model discussion. 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). More specifically, New IP covers the following aspects:

1. **Semantic addressing** catering to an increasing number of services that utilize the data plane of the Internet, recognizing existing trends towards improved content delivery through replication in special deployed CDN systems as well as from previous initiatives such as information-centric networking [6] and in-network computing [7]. The goal is to bring the routing to key services “closer” to the basic data plane operations. This can be achieved through, e.g., embedding service information into the addressing scheme used for packet delivery [8], allowing for fast redirection to the “optimal” endpoint without requiring DNS-level operations as it is the case today.
2. **Flexible length** addressing catering to an increasing number of specialized network deployments (particular in industrial settings). This study area is driven by the long-standing recognition of IP header overhead, moving instead to a variable length address approach [8] that can be efficiently supported alongside the global reachability that the IP header generally facilitates, therefore still ensuring the global reachability that IP itself enables.
3. **ManyNets support** catering to emerging transport network technologies such as satellites, dynamic networks (in V2X scenarios) and THz access networks in future 6G networks. These networks afford a dynamicity of connections that require suitable support from the data plane to form an adequate and high performing fabric over which to reliably (and possibly deterministically) exchange information.
4. **Deterministic services** that guarantee low upper bound of end-to-end latency, jitter and loss rate for specified flows, catering to the increased rigorous QoS of new applications (e.g., smart manufacturing, telemedicine, and autonomous driving). Unlike TSN [9] which solves determinism in small-scale layer-2 networks, New IP targets large-scale layer-3 networks, where deterministic services and best-effort services may coexist.
5. **Intrinsic Security and Privacy**, to address inherent vulnerabilities of IP networks, including source address spoofing, privacy leak, trust model weakness, and distributed denial of service (DDoS) attacks, which were not considered as one of the original “seven design principles” [10]. Based on STRIDE security model [11], a network architecture with intrinsic security and privacy is studied, so as to maximally protect user privacy, consolidate

distributed trust basis, and build secure and trustable networks, which would meet the privacy protection requirements represented by GDPR and the security and trustworthiness requirements of industry-wide interconnection.

6. **High throughput** over a number of concurrent access technologies, ensuring not only the needed quality of the envisioned new services (with video technologies being core to driving the requirements for bandwidth) but also catering to the emergence of many networks at the access level, including satellite, 5G (and evolutions) and many others. Multi-path solutions [8], network coding, multi-layer cooperation mechanisms as well as the signaling of application requirements are key to ensuring this aspect to be properly addressed.
7. **Endpoint-definable Forwarding Operations** is being seen as central to utilizing in-network capabilities of the forwarding plane to improve on service experience. Contrasting the flow-based approach of contemporary solutions, such as SDN [12] and P4 [13], are approaches that embed such operations into the packet delivery, i.e., the IP packet, for consideration in the intermediary forwarding element. The tradeoff between overhead, complexity and service quality is a key focus of investigation in this area.

What is NOT New IP?

New IP is a suite of study areas for developing suitable evolved Internet technologies. New IP does **NEITHER** define governance models for the use of those technologies, **NOR** lead to “more centralised, top-down control of the internet” [14]. In that, we follow established paths for developing Internet technologies in standard bodies, disconnected from the specific governance that operators and governments in the world decide upon. This is illustrated in our work on prevention of DDoS attacks, which indeed proposes the so-called “Shut-off protocol” [15]. This concept is similar to proposals made by, for instance, Carnegie Mellon University scholars in the United States, as well as found in similar technologies that have been discussed in IETF DDoS Open Threat Signaling (DOTS) [16], among others. Such ‘shut-off’ is used by the attacked network to signal to the attacker’s source network the request for preventing further attack traffic [17]. This technology is therefore well established in existing solutions.

How to get to New IP?

Hundreds of high-level researchers from academia and industry in dozens of regions, including China, Europe, Japan, South Korea, North America, South America, and Africa, proposed future-oriented business **visions** and **requirements** with a focus on driving the wider **societal digitalization** through Internet technologies. We believe that the New IP initiative follows this tradition to the point through engaging with key international research communities to **explore the space of possibilities** to evolve IP technologies, while engaging with standardization organization to **derive the requirements** driving the evolution and ultimately **agreeing on common solutions**. In this, work in bodies such as the ITU Network 2030 focus group addresses the requirements, while our existing as well as future engagement with SDOs, such as IETF, ITU, ETSI, and others on a number of New IP solutions shows the integration into the consensus process the Internet community has established over time.

Contrary to the current politicized debate, New IP invites an **open and free discourse** through inviting researchers from all countries and industries around the world to **participate in the research** that would see IP evolve along the requirements found in relation to New IP and therefore drive the **sustainable development** of the global communication industry.

1. https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx (https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx)
2. https://www.delltechnologies.com/en-us/perspectives/future-of-living.htm (https://www.delltechnologies.com/en-us/perspectives/future-of-living.htm)
3. ITU-T FG NET2030, " A Blueprint of Technology, Applications and Market Drivers Towards the Year 2030 and Beyond", ITU-T Focus Group Network 2030,online: https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/White_Paper.pdf (https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/White_Paper.pdf)
4. ITU-T FG NET2030, " New Services and Capabilities for Network 2030: Description, Technical Gap and Performance Target Analysis", online: https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Deliverable_NET2030.pdf (https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Deliverable_NET2030.pdf)
5. Ian Brown, David Clark, and Dirk Trossen. 2010. Should specific values be embedded in the internet architecture? In Proceedings of the Re-Architecting the Internet Workshop (ReARCH ’10). Association for Computing Machinery, New York, NY, USA, Article 10, 1–6. DOI: https://doi.org/10.1145/1921233.1921246 (https://doi.org/10.1145/1921233.1921246)
6. https://www.cl.cam.ac.uk/~lw525/publications/icn-basics.pdf (https://www.cl.cam.ac.uk/~lw525/publications/icn-basics.pdf)
7. https://www.sigarch.org/in-network-computing-draft/ (https://www.sigarch.org/in-network-computing-draft/)
8. Zhe Chen, Chuang Wang, Guangpeng Li, Zhe Lou, and Sheng Jiang, “NEW IP Framework and Protocol for Future Applications”, in Proceedings of 2020 IEEE/IFIP Network Operations and Management Symposium (NOMS)
9. https://1.ieee802.org/tsn/ (https://1.ieee802.org/tsn/)
10. David Clark, "The design philosophy of the DARPA internet protocols." SIGCOMM Comput. Commun. Rev. 18, 4 (August 1988), 106–114. DOI: https://doi.org/10.1145/52325.52336 (https://doi.org/10.1145/52325.52336)
11. Microsoft, "The STRIDE Threat Model", online: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx (https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx)
12. https://www.opennetworking.org/sdn-definition/ (https://www.opennetworking.org/sdn-definition/)
13. https://p4.org/ (https://p4.org/)
14. Anna Gross and Madhumita Murgia, "China and Huawei propose reinvention of the internet.", March 28 2020, online: https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2 (https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2)
15. David Naylor, Matthew K. Mukerjee, and Peter Steenkiste. "Balancing accountability and privacy in the network." ACM SIGCOMM Computer Communication Review 44, no. 4 (2014): 75-86.
16. DDoS Open Threat Signaling (DOTS), https://datatracker.ietf.org/wg/dots/charter/ (https://datatracker.ietf.org/wg/dots/charter/)
17. David Andersen, Hari Balakrishnan, Nick Feamster, Teemu Koponen, Daekyeong Moon, and Scott Shenker. "Accountable internet protocol (aip)." In

Proceedings of the ACM SIGCOMM 2008 conference on Data communication, pp. 339-350. 2008.