# On the Study of Internet Ossification, Impacts, and Solutions

Lin Han, Richard Li
*Futurewei Technologies, Inc.*
Santa Clara, California, U.S.A
email: lin.han@futurewei.com; richard.li@futurewei.com

***Abstract*— The current Internet is based on IPv4 and IPv6. It has been in service for many years and is very successful. However, it is facing challenges in protocol ossification, security, and service quality. Recently, the geographical tension, trading confrontation, digital asset and digital sovereignty, the regulation for data protection and localization have raised decentralization requirements for the Internet. This paper analyses the factors for the Internet ossification and its impacts, it proposes a new architecture that is distributed based on region or country. It can maintain the support of the current IPv4/IPv6 and existing applications, and provide more flexibility for the protocol, thus mitigating the ossification of the Internet. With the new architecture, the Internet will be decentralized based on regional governance and provide more space for more diversities within different regions. Meanwhile, the global connectivity, accessibility and integrity of the Internet are kept.**

***Keywords- Future Internet; Ossification; Decentralization; Distributed; Fragmentation.***

## I. INTRODUCTION

This paper is an extended version of [1], which investigates the Internet ossification, proposes a new architecture and protocol to solve the problem.

The Internet has penetrated everywhere in our life and has provided tremendous momentum to the development and progress in communication, technology, culture, and economy. The current Internet is based on IPv4 [2] and IPv6 [3] protocols, and consists of many other protocols for different areas, such as address assignment, domain name service, routing and switching, security, transport. All these protocols are governed by the Internet Engineering Task Force (IETF). In the document thereafter, the name IP represents both IPv4 and IPv6.

However, the Internet's deficiency and ossification are also noticed. This includes slow evolution, protocol ossification, resource allocation unfairness, security and privacy concerns. Digital asset [4] and digital sovereignty [5] are also debated in different countries and regions. All these problems are not easy to be solved under the current Internet architecture since those factors were never considered in the time of the Internet was born.

The paper briefs our research on a new architecture for the Internet and associated protocol structures. It can provide extra flexibility for the Internet while maintaining the current IP based technologies and services. Internet ossification can be mitigated by a new architecture including distributed Internet resource management and domain name service, free choice of address type, and heterogeneous communications.

The rest of the paper is structured as follows. In Section II, we present an overview of the Internet architecture and protocols. Section III discusses the Internet ossification and analyzes the root causes. The technical factors are analyzed in Section IV. Our new network protocol is proposed in Section V. Section VI presents the detailed design. Section VII illustrates the new Internet architecture with the new protocol. The compatibility issues are discussed in Section VIII. Sections IX and X summarize the advantages and disadvantages of the new proposal, respectively. Section XI concludes the paper and gives further research directions.

## II. OVERVIEW OF THE INTERNET

The Internet is the global system of interconnected computer networks that uses the Internet protocol suite to communicate between networks and devices [6]. Recently, with the growth of 5G [7], Internet of Things (IOT) [8], Non-Terrestrial-Network (NTN) integration [9], the Internet has become the communication infrastructure that almost every person, every device and everything can be connected to. The Internet scope is very broad and has a couple of key fundamental blocks:

- The definition of IP address, the mechanism to allocate and assign the IP addresses. There are two types of IP addresses, one in IPv4 and another is IPv6. Currently, IPv4 is in the process of becoming obsolete from the perspective of IETF, and IPv6 is the only supported address. The IP address (except the local address and non-routed address) is globally significant and unique in the world. It is allocated by the Internet Assigned Numbers Authority (IANA) [10] to each region and country. There are five Regional Internet Registries (RIRs). Each RIR has a couple of Local Internet Registries (LIRs) or National Internet Registries (NIRs). They are responsible for the allocation of the IP addresses block on their authorized areas. Figure 1 and Figure 2 show the hierarchical architecture of IANA [11].
- The definition of Asynchronous System Number (ASN) [12], and the mechanism to assign ASN. ASN is used for BGP [13] to represent autonomous systems across the Internet. Similar to IP address, the public ASN is also globally significant, it is managed by IANA. ASN is key to BGP that is critical protocol for the inter-connection and inter-working of different networks distributed globally. BGP will exchange the global IP address of different networks, thus making every global IP address reachable from anywhere around the world.
- The definition of Domain Name, the mechanism to manage Domain Name Servers and provide the Domain Name System (DNS) [14] Service. Similar to IP address, Domain Name is also globally significant. The DNS root zone management [15] and DNS root servers [16] are managed by IANA as well. Domain Name and Domain

Name Servers are distributed globally. There are thirteen DNS root server located in U.S.A. Different leaf servers belonging to different region and country are deployed globally. In addition to this, some countries may have mirror root servers in their own region to back up the root server and speed up the DNS services.

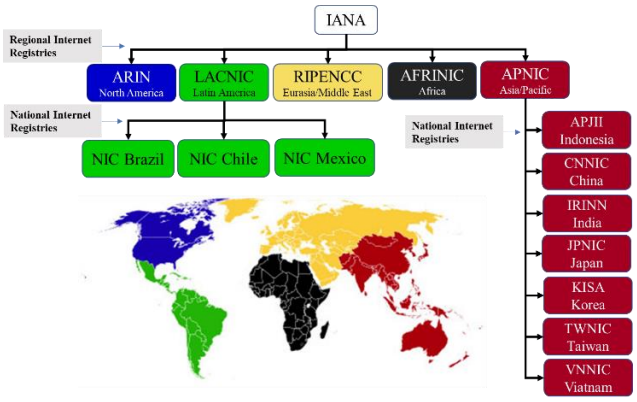


Figure 1. The hierachy of IANA architecture

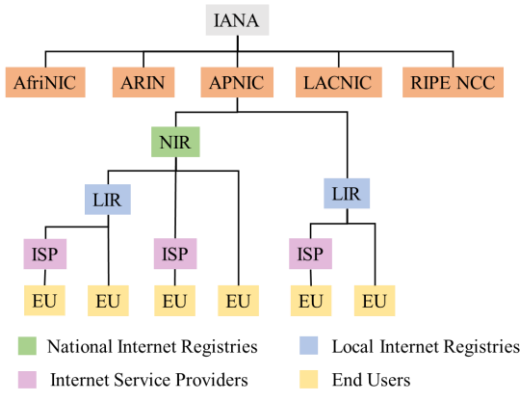


Figure 2. Understanding address management hierarchy [10]

- The protocols to control the Internet. The fundamental protocols are IPv4, IPv6 and many other protocols on top of IPv4 and IPv6. Excluding protocols on L2 that are controlled by the Institute of Electrical and Electronics Engineers (IEEE) and the International Telecommunication Union (ITU), the protocols for Internet include layers from L3 to L7 that are controlled by IETF. There are thousands of protocols related standards that are called RFC (Request for Comments) documents, e.g., more than 500 RFC for IPv6 has been published. Below just lists a very small portion of RFCs and very typical protocols:
  1. Host configuration related protocols (ND[17], DHCPv6[18], etc.)
  2. L3 or routing protocols (BGP, IS-IS [19], OSPF [20], etc.),
  3. Traffic Engineering (MPLS [21], RSVP-TE [22], SRv6 [23], etc.)
  4. L4 or transport protocols (TCP [24], UDP [25], etc.),
  5. Upper layer protocols (QUIC [26], TLS [27], HTTP [28], etc.),

## III. INTERNET OSSIFICATION

### A. Root Cause

The Internet was essentially designed with simplicity and scalability. [29] has detailed analysis of how this is achieved and lists the important timeline for Internet evolution. After the Internet becomes available to the public in the 1990s, it experienced more than 40-years' development of technology. Gradually, the evolution of the Internet becomes slower and slower. There are less and less new technologies and services coming up for the Internet, especially for the parts of infrastructure and fundamentals. The structure of the internet becomes more rigid and difficult to change over time, and this sometime is called Internet ossification. For example, IPv6 was designed to replace IPv4, but this has not been accomplished since the first IPv6 standard RFC 2460 [30] was introduced in 1998. Even right now, there are still arguments that IPv4 should not be obsoleted [31], and the adoption of IPv6 in Service Provider is still slow.

There are couple of research that proposed new or enhanced architecture for Internet, such as RINA [32], SCION [33], New IP [34], IPv10 [35], and Extensible Internet (EI) [36][37]. Detailed analysis and comparison of proposals of RINA, SCION and New IP can be found in [38]. IPv10 is to allow the communication between IPv6 and IPv4. EI introduces Layer 3.5 between L3 and L4 to provide services that were not available in the current Internet architecture.

Two categories of factors associated with management and technical solutions can contribute to the Internet ossification:

- Consensus challenges:
  The Internet is a huge global network. Many technical definitions, solutions, and changes are globally significant. Any decisions or changes about its development, operation and deployment involve a wide range of stakeholders, including governments, organizations, operators, and individual users. Reaching consensus on changes can be very difficult and slow, especially when there are competing interests or different priorities. As a comparison in the standardization in wireless area, 3GPP has finished the 5G (the fifth generations of wireless technology) in almost the same period that IETF has not completed the IPv4 to IPv6 transition.
- Technical solutions:
  Due to the vast number of users, devices and applications, the Internet has accumulated many technical feedbacks and problem reports. Completely fixing those problems or enhancing the existing solutions are always slow. Some quick fixes that are implemented in a short term, but may need to be addressed or replaced later on. The slow global consensus on any problem fixing, new enhancements or features, can make it more difficult to change any piece of the internet's infrastructure. The Internet is a complex system that involves many different networks, technologies, and standards. How to drive the Internet moving forward but maintain the previous investment is

not only a business objective but also a technical challenge. Ensuring compatibility between these different elements can be difficult, and changes to one part of the system may have unintended consequences elsewhere. Due to this reason, people are always conservative and hesitate to adopt new technologies.

### B. Consequence of Internet Ossification

The Internet ossification has impacted the internet's ability to continue evolving and progressing. It contributes more or less to the slow solution for following issues and requirements:

- Privacy and Security: These two contradictory requirements have never been solved with satisfaction from different parties. To solve the privacy issues, IETF has had the Working Group for "Host Identity Protocol" [39], HIP [40] provides a cryptographic namespace to applications, and the associated protocol layer, thus provide the best privacy protection. But since many nations do not want such information invisible to the law enforcement for the sake of security, this protocol was never widely deployed. TLS [27], HTTPS [28], IPSec [41] are all security protocols at different layers and are widely used in Internet, but the Internet security issues never disappear even many security events are not associated with the technologies used. Distributed Denial-of-service (DDoS) attack [42] is one of the most notorious security issues for many years. It caused lots of business losses and may lead to international conflict if the DDoS source and victim are in different nations. The current technologies to stop DDoS attacks need to have protection mechanism at different places from connected service provider network to the cloud the application is running [43], the solution is quite extensive and needs coordination between different organizations. To eliminate such attacks, without some Internet infrastructure changes, it is quite difficult.
- Digital Asset and Digital Sovereignty: Bitcoin has been very succeeded in its security, value growth and become a hot trading target, but it has never been recognized as legal currency for the legal business. Non-Fungible Token (NFT) is another type of digital identifier for any digital asset, its recognition is also doubtful due to no endorsement from any government or authorization. The Internet is a network with unified address, protocol, and centralized resource management. The failed acceptance of Bitcoin and NFT have driven us to think whether we should consider the requirements from the sovereignty at the original design of the Internet. Since none of the basic Internet resources (IP address, ASN and Domain name) is controlled and managed by a government or authorized administration for a country, it will naturally cause concerns. Digital Sovereignty is a controversial topic in the European Union and other countries recently. Even though its scope, target and method are still to be decided, it has raised a question how the Internet can be designed to consider such factors.
- Fragility of Internet Architecture
  Even though the Internet architecture is claimed to be distributed and resistant to failure of partial network, it has never been tested for large scale failure due to unexpected incidents like nature disasters or war. The current Internet only relies on the BGP to establish new routes whenever some global network is not reachable. However, since the Internet scalability is super large now, any failure of some links crossing small regions may lead to unexpected and large scale of consequences. The research in [44] has indicated that the Internet in non-relevant countries will be severely degraded if some links between China and Taiwan are cut. [44] has also given the detailed analysis for the reason why such small scale of link failure can lead to large scale of impacts to the Internet, it also proposes to study "Wartime BGP routes" as a short-term solution to handle such scenario.

## IV. Design Factors for Internet Ossification

Even though there are many factors, technical or non-technical, contributing to the Internet ossification, we think some short-term design of Internet has made Internet less flexible at the beginning, thus is one of the most important factors we need to consider when thinking about the future architecture. The following are some technical perspectives that contribute to the Internet ossification.

- The Internet resource (IP address, ASN and Domain Name) assignment and management are essentially a centralized hierarchical architecture. The problem of this centralized architecture is that (1) IANA and Regional Internet Registries are both non-profit organizations that do not have any jurisdiction. (2) The Internet resources are hardly allocated fairly, for example, IPv4 address block is not enough in some countries but more than required in other countries. (3) Address preference is not the same in different regions, countries, operators, users, and applications. For example, IPv4 is still preferred by many service providers and enterprise network. That is one reason that IPv6 deployment is so slow. (4) Centralized architecture makes the Internet fragile when the geopolitical tensions are high. In the recent events of war and trading confrontation, some voices to stop the Internet service to specific area is around and has put the threat to the integration of Internet.
- Since IP address is globally significant, it requires that all end-user devices and network devices use IP as unique format for the data packet header, all L3 devices should follow the same principle to process IP packet and provide the services to upper layer. This design is called "narrow waist". Obviously, it has benefits in simplicity and scalability, but it becomes one factor contributing to the Internet ossification, since any changes in IP header will have global impact and hard to get consensus in IETF.
- From the IP packet forwarding perspective, the IP based Internet is flat. All internet packets are forwarded based on IP address lookup; thus, all globally reachable IP addresses must be stored in every network device (even in MPLS network, the Provider Edge (PE) Routers also must store all reachable IP prefix). This can result in two problems: (1) huge amount of IP addresses or prefixes storage leads to huge lookup table size. (2) BGP, the only protocol to exchange the global IP reachability between

different networks in different regions or countries, must process huge number of global IP prefixes. Any small internet state changes may lead to BGP re-route huge amount of traffic as described in [44].

## V. CONSIDERATION OF NETWORK LAYER

### A. Tecnology Progress Considerations

From the analysis in Section IV, we can see that one of the major factors for Internet ossification is the IP design is too rigid. Such rigid design was partially because the hardware or semiconductor performance was limited in the 80s and 90s in the last century. To achieve the line rate of packet processing, it is hard to give too many flexibilities in the address and functions in the packet header, e.g., the address type and size, the extensions, and options. After many years' development, the semiconductor industry has progressed a lot. Recently, high-performance chips with programmability have been commercialized. It is time to think about what we can do from a technical perspective that can mitigate the Internet ossification.

### B. Requirements of Internet Decentralization

#### 1) Compared with other system

As a global data communication network, the Internet is supposed to be only responsible for the inter-connection between different networks in the world. The networks could be for enterprises, ISP (Internet Service Providers), a country or a region. Let us compare the similar situation in phone network and mail system. For those two global communication systems, there is no restriction on how to define a local phone number, and local address format. The international community only needs to get consensus on the country code for international calls, or the country names for global mail delivery. Each country will manage and design its own structure of phone numbers, mail addressing system and delivery infrastructure. We think the Internet should take the same approach.

#### 2) Regulation requirements

Recently, more and more countries or regions have new legal requirements for international ISP to provide the service in the country. For example, the internet service provider's infrastructure, including cloud, computers, storages, etc., that is associated with the locally provided services, must be deployed within the territories of the country. All provided services (applications, contents, accounting, etc.) should comply with local regulations for security, privacy, etc. These regulations naturally require ISP to have a decentralized Internet infrastructure and a decentralized Internet service. From this perspective, the major international ISPs already deployed their infrastructure and services in a distributed manner crossing different countries or regions.

#### 3) Trendes for the content localization

To achieve better service (higher bandwidth, shorter latency, less probability of congestion) for content delivery, the content servers or data centers are moving closer to data consumers. This trend has been accelerated after 5G introduced the Mobile Edge Computing (MEC) technologies. Moving closer to data consumer needs to have the localization in Content Delivery Network (CDN), associated APP (Applications), Name resolving, Content searching, etc. All these trends lead to the Internet traffic to be grouped on the base of population and sovereignty.

### C. Design Principals for Ideal Internet

Considering all above analysis for Internet history, the current requirement and trends happened for Internet, if we have a chance to redesign an ideal Internet, we may have following principals:

- The Internet should have more flexibility, less restrictions and centralization. Keeping the technology diversity for the Internet will not only reduce the ossification but also satisfy different requirements easier.
- The Internet should be distributed globally based on region or country. All regions are equal and there is no central control. No region can impact other's decision in address selection, peering and service.
- Small countries can decide to form a region if the countries do not want to be independent in internet resource and DNS management due to economy and other constraints.
- Each region has the freedom and authorization to manage the Internet resources used locally, such as address selection, address allocation, ASN allocation, domain name registration, DNS root server, etc.
- The internet should support heterogeneous address types and communications.

## VI. DESIGN DETAILS

The key aspects of the new architecture are as follows:

- The Internet for each country or region is connected by a separate protocol. We have two options for this protocol. One is to design a new protocol (described in the sub-section A), and another is using the current IP technology (described in the sub-section B). The comparison of two options is discussed in sub-section C. The paper focuses on the discussion of using the new protocol.
- Each country or region will have independent internet resources including IP addresses, ASN number, DNS, etc. All these resources are managed by the country or region. Since the details of these architecture changes for two options (described in sub-section A and B) are the same, the paper will only focus on the discussion of the architecture changes, compatibility issue and benefits (in Sections VII to IX ) for the 1st option or using new protocol.

### A. Using a New Protocol

The new network protocol packet header for the Internet as shown in Figure 3. The packet format is preliminary and only for illustration. Final design will decide the detailed coding. This new packet is on top of Layer 2, thus, a new EtherType assignment from IANA is required.

Below is the explanation for each field in the Figure 3:

- Declaration: This field defines the basic info about the packet, it may contain following essential info:
  1. HL: Hop limit, this value is decremented by one at each forwarding node and the packet is discarded if it becomes 0 (except on the last node).

2. Prot: The protocol number for payload, it could be a protocol number defined currently by IANA, e.g., IPv4 or IPv6, TCP or UDP, or a new protocol number defined in the future.
3. Len: Total length of the packet including the Pay Load. The unit can be defined in standardization.
4. Other definitions: other definitions for the packet header, it will be defined later.

- Regional codes: This field may contain the "Src (Source) Region Code" and "Dst (Destination) Region Code" for source and destination. The size, code structure and detailed coding should be standardized by an international organization. It could contain region or country code that was defined by ITU E.164 [45], and have its own hierarchy, e.g., region, sub-region, and more granular definitions. See Figure 4 as an example. Only the 8-bit "Region Code" needs to be standardized by an international organization, "Sub-region code" will be managed locally in the region.
- Service: This field contains information about the service and is to be defined. Its length is variable.
- Payload: This part contains the payload which type is specified by the protocol number defined in Declaration. The Payload could be IP type or any other types for L2 to L4.

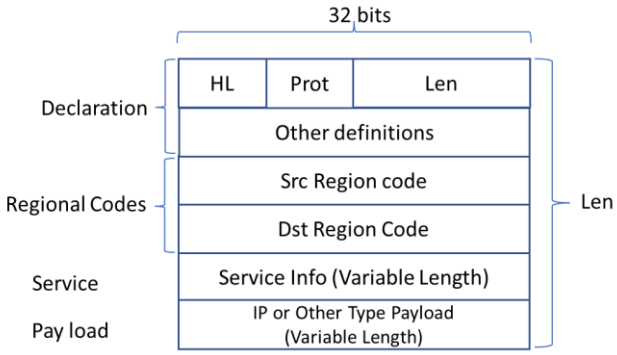


Figure 3. New Internet protocol packet header


Figure 4. The Region Code Example

### B. Using Current IP

This option will use the existing IPv4 or IPv6 technologies to interconnect the networks in different countries and regions. By this option, the architecture for the internet is the same as by using a new protocol (sub-Section A). Following works must be done:

- IANA should permanently reserve some un-used IPv4 or IPv6 addresses, then each country or region will have a permanent IP address assigned by an international organization. This address is similar to the area code for telephone system and can only be used to connect different countries. Whether each country will be assigned multiple IP address will be decided by the international community.
- The IPv4 or IPv6 tunnels between countries and regions are established. These tunnels are only used for the traffic crossing border.
- Each country or region will develop its own address assignment, management, and DNS server system. After all these systems are set up, the country can switch those management from the current to local.
- An international organization is responsible for the DNS root connection and traffic distribution between countries and regions.

### C. Comparisons of Two Options

- Using the new protocol can give us chance to go through all possible design aspects, make it possible to fix the problems of the current Internet and to satisfy future requirements, thus, it should have longer term benefits.
- Using the existing IPv4 or IPv6 is simpler than using a new protocol, but it will not have the benefits of the new protocol, e.g., it may not support the services that can be introduced by the new protocol. Additionally, it will overload the original IPv4 or IPv6 address definition (prefix plus length) for the use of Point-to-Point interconnection between countries, some existing address aggregation, forwarding, and protocols have to be re-examined to make it not conflicting to the existing IP network.

## VII. Architecture for Internet Based on New Protocol

### A. Internet Resource Management

The internet resources will include region code, IP address space or other type of address space, ASN, and protocol number. The management of those resource are based on following rules:

International organization managed items:

- The Region code structure and Region code assignment are responsible by international organization, ITU or IANA.
- For the protocols that the interconnection between different region or country are supported, e.g., the new protocol defined by this paper (new EtherType), IPv4, IPv6, Ethernet, MPLS, etc., the protocol numbers are still managed by international organization IANA.

Regional authority managed items:

- Each region or country will be responsible for the sub-region code assignment and management.
- Each region or country will be responsible for the IPv4/IPv6 address and ASN number allocation and management for its own jurisdiction area. Different regions or countries may have different policies and schemes to manage the resource.
- Each region or country can use the whole IPv4/IPv6 address and ASN space. All addresses only have local significance in the region or country, thus different regions or countries may have the same address.

- Each region or country can define new protocol numbers that are only used locally within the region or country.

### B. Scope of New Protocol

The new protocol applies to the internet connection between different regions and countries as shown in Figure 5. It does not restrict communication within the region or country. The current IPv4 and IPv6 can still work. A region or country can define and run a new version of IP without any interruption or interference to the whole Internet. For example, IPv10 to support communication between IPv4 and IPv6 was proposed in IETF but was not accepted. With the new protocol, one region only needs to get consensus on IPv10 in its own sovereignty and then use it within the region.

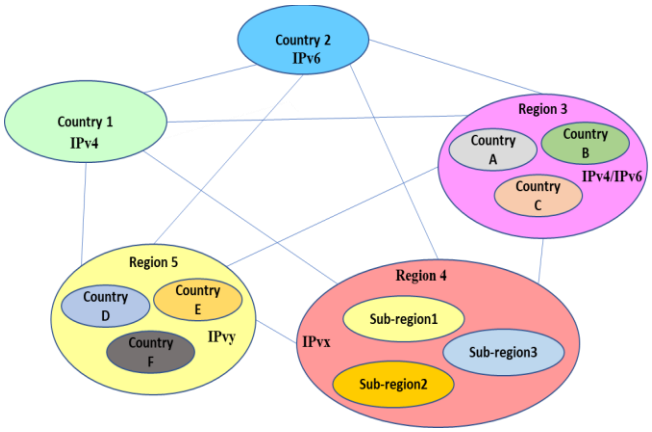


Figure 5. Internet based on new network protocol

It is important to note that a region can also use the new region-based protocol for communication within its own territory (see the communications between sub-regions in Region 4 in Figure 5).

### C. Domain Name Service

The Domain Name Service architecture is similar to the current DNS hierarchy architecture, Figure 6 illustrates the new DNS architecture and Figure 7 demonstrates a DNS request and response crossing different regions or countries. The major difference with the current architecture is that the current centralized DNS root zone and root servers are removed, thus is a distributed architecture. Following are details:

- Each region or country will have its own DNS root server and different root servers from different regions or countries are fully equal and there is no central control, thus the current DNS root zone and root servers not needed.
- All DNS root servers are connected virtually to form a DNS network. The addresses of all root servers can be based on the new protocol, thus are unified for different regions. The network may run a dedicated protocol to exchange DNS information for all root servers. This network will be overlay on top of either existing IP or the new network protocol proposed in this paper.

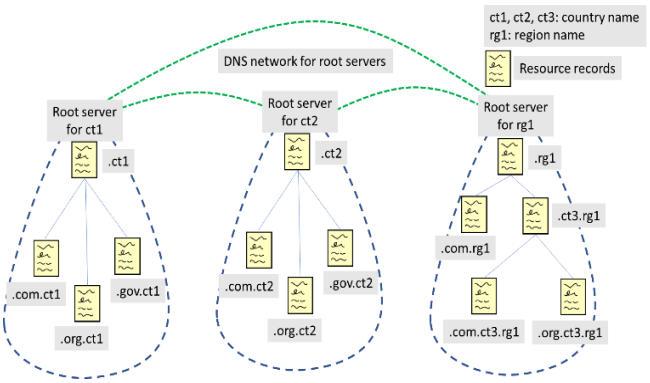


Figure 6. Domain Name System architecture

- The connection between all DNS root servers are fully meshed virtually. Any connection between two servers are voluntary and only managed by two servers' regions or countries. When a new root server for a region or country joins the network, it should have agreement and then connection with existing root servers.
- The ".region" or ".country" domain is the only Top Level Domain (TLD) for the region or country. All other domain names are lower-level domains.
- The ".region" or ".country" suffix is needed when the DNS requester and real domain name are in the different region or country. The suffix can only be omitted when the DNS requester and the real domain name are in the same region or country.
- A domain name with a ".region" or ".country" suffix is always associated with an address physically located within the region or country.

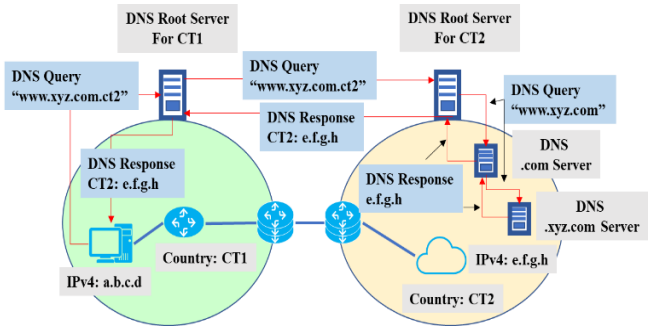


Figure 7. DNS service crossing different regions or countries

The DNS service will have some corresponding implementation changes with the new architecture. Also, there are some regulation or legal issues involved, e.g., a company name in a "domain name" in a different region must be approved by the local authority.

Here is an example: An international company xyz has the header quarter in the country named as "ct1", then the domain name "www.xyz.com.ct1" always points to an address assigned by the DNS authorization in the country ct1. In another country ct2, if there is a branch or service from the company xyz, the DNS request of "www.xyz.com" from ct2 will return an address info found in the name server ".com" in

the country ct2. If there is no registration for the company in ct2, DNS request of "www.xyz.com" from ct2 will return null.

Due to the bonding of a name and IP address in every region physically, the new DNS mechanism will make the internet service localization more transparent and easier to be compliant to the local regulation or laws.

### *D. Communication Between Region or Country*

To provide interconnection between different regions or countries using new network protocol, proper control plane and data plane must be defined.

#### 1) *Control Plane*

- The border devices connecting different regions need to support the new control protocol.
- The new control protocol will exchange information about the interconnected border devices, the associated links, the region code, and the reachable end-user's address details, etc.
- The new control protocol could be link-state routing protocol like IGP, or path-vector protocol like BGP.
- New control protocol also must be running within a region or a country to populate the information learnt from border devices about the outside interconnected networks of other regions or countries, e.g., the links that can reach other regions or countries, the associated remote reginal code, the remote reachable address associated with the regional code, etc.

#### 2) *Data Plane*

- For the egress region, where the traffic is originated from, the data packet forwarding is based on the lookup of "Region/Country code" at all network devices. See the country CT1 in Figure 8.
- For the ingress region, where the traffic is destinated to, the data packet forwarding is based on the lookup of "the address of payload" at all network devices. See the country CT2 in Figure 8. In the example, the "address of payload" is IPv6 address.
- For the transit region, there are two approaches, one is Transparent Mode, another is Tunnel Mode.
  1. For Transparent Mode, the data packet forwarding is based on the lookup of "Region/Country code" at all network devices in a transit region. See the country CT3 in Figure 8.
  2. For Tunnel Mode, the data packet forwarding is based on the lookup of "Region/Country code" at edge network devices in a transit region. Proper packet encapsulation (at ingress router) or decapsulation (at egress router) are needed. See the country CT4 in Figure 8. In the example, the IPv4 tunnel is used and IPv4 address lookup for the tunnel is done on every network device within the region.
- For all scenarios, a very small table is needed to store all "Region/Country code" for the communication crossing regions. The table lookup will use "exact match". These two behaviors are different as the IP prefix lookup, which needs huge amount of table to store global IP prefix, and the lookup is Longest Prefix Match using TCAM (Ternary Content-Addressable Memory).

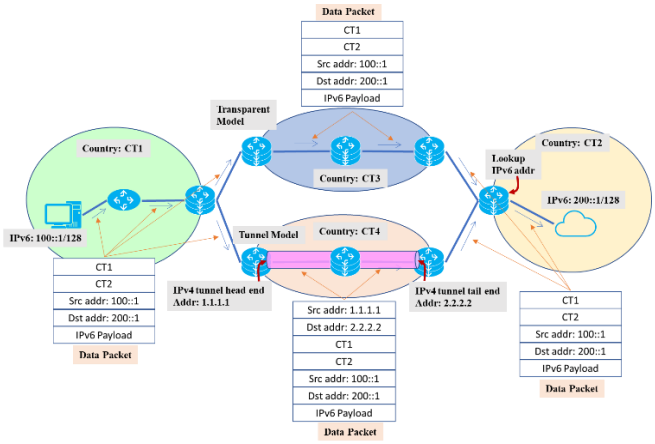


Figure 8. Homogeneous communication: Transparent Mode and Tunnel Mode (only the essential parts of packet header are shown)

#### 3) *Heterogeneous Communication Between Region or Country*

The above discussions are about the homogeneous communication between regions or countries, or the address type are the same for all end users.

The new network protocol and architecture can support heterogeneous communication worldwide. Heterogeneous communications are communications with different types of address. This is very useful to many applications in security, privacy, IoT, etc., below are some supported address combinations for heterogeneous communication:

- Different length of IP for source and destination, e.g., IPv10 or other type of IP that the address length is not 32-bit and 128-bit.
- Different type of address for source and destination, e.g., between Ethernet and IP.
- No source address, the source address is hidden in the application data.
- Variable length public key as address.

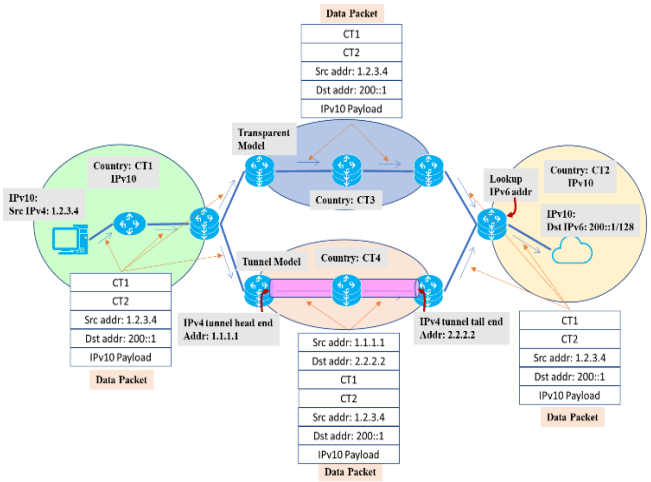


Figure 9. Heterogeneous communication: Transparent Mode and Tunnel Mode (only the essential parts of packet header are shown)

Figure 9 illustrates the data plane for a case where IPv10 is supported in country CT1 and CT2, and how an IPv4 host in CT1 sends data to IPv6 host in CT2. For IPv10 case, both IPv4 and IPv6 address are supported, thus the lookup of IPv6 in CT2 is obviously supported. We can see that to support IPv10, only communication participants (CT1 and CT2) need to have an agreement to support it. This is much easier to have a global consensus to support IPv10.

## VIII. Compatibility Issues

The major changes of the Internet based on the proposed new network protocol are the Internet resource management, the DNS architecture, and the use of new network protocol.

For the communication or IP service within the same region or country, the current IP based internet service can still be used, and there is no compatibility issue. The new Internet resource management and new DNS architecture have very little impact on the end-user application and network operation, i.e., some provisioning (to the DNS server and domain name management) may need to be changed.

For the communication or IP service crossing different regions or countries, the new network protocol needs to be used, and it is not compatible with the existing IP, but we can maximize the current Internet investment through the detailed design of new network protocol header.

It is easy to notice that the new network protocol packet header is very similar to the IPv4. This is intended to make the future design easier to be implemented in IPv4 capable hardware. We have two options in the final design of the packet header encoding: (1) re-use the IPv4 packet header for the new network protocol, or (2) only re-use the 32-bit IPv4 address space for the region code and redesign other fields in packet header. Since the current IPv4 header has design flaws in some areas, such as: (a) The protocol is not extensible due to the limited IPv4 option size, (b) The header checksum is not required, (c) Fragmentation is not a good design. So, we prefer the option (2): define the 32-bit source and destination region codes; redesign other fields in the packet header.

With the above design considerations and coupled with redesigned protocol running between regions, by the minimal re-programming, the existing hardware can be easily re-used for the future Internet.

## IX. Advantages of New Network Protocol

### A. Benefits

The proposed new network protocol is only for the interconnection between regions and countries. The Internet based on new protocol will have following benefits:

- Much less restriction at the protocol for interconnection:
  The new network protocol only defines the regional interconnection mechanism that is based on regional codes, but not limit the communication address and communication mechanism within a region or a country, thus reduces the restriction caused by globally uniformed IPv6 header for global network. Heterogeneous communication support will be easier to achieve between interested parties.
- Minimized changes on the current Internet architecture:
  The current IPv4 and IPv6 protocols and data forwarding can still work in a region or country. DNS changes very little. The architecture of IP based Internet is kept, and the investment is not wasted.
  The control protocol and data forwarding for interconnection between regions and countries can be realized based on extension of existing IP routing protocols and IP packet forwarding. It needs minimal investment.
  Existing and future IP based applications within a region can still run without any feeling that the underlayer networking is changed for the interconnection between regions. The application to reach outside of a region just needs minor modification for the address format to include the regional codes.
  The routing table size will be dramatically reduced due to the fact that routers in a region will only keep the prefix defined in the region. All addresses to outside of a region can be summarized as regional codes.
- Independent technology evolution:
  With the new network protocol, Internet technology can evolve in different regions or countries independently. It is expected to be much easier and faster than the current situation that the global consensus is needed, thus will mitigate the Internet ossification a lot.
- Distributed Internet resource management and DNS:
  The new Internet resource management and DNS are distributed and based on sovereignty and jurisdiction, thus has no legal obstacles to making the regional Internet technologies adaptive to local laws or regulations. It will make any security, privacy changes or enforcement much easier and faster.
  The new Internet resource management and DNS root servers are distributed and fully controlled by a region or country. The Internet service of any country will not be impacted by other countries. It makes the Internet more robust and resilient to any disasters and geopolitical interruption.
  The new distributed Internet resource management also makes each region or country able to use the whole IP address space and ASN space. This will not only eliminate the unfairness issues in IP address allocation, but also expand the IP address resource for all countries.
  The new architecture and network protocol gives each region or country full control and freedom of what type of address and communication are used for the internet service within the region. This will eliminate the IPv4 to IPv6 migration mandates if IPv4 is preferred in a region or country. Also, other new types of address can be invented and adopted locally.
- Internet integrity is maintained:
  Internet fragmentation [46] is always a concern for new technology proposals. From a technical perspective, the new proposal does not impede the ability of systems to fully interoperate and exchange data packets. The Internet functions are consistent as before at all end points. Internet interoperability, universal accessibility, the reusability of capabilities, and permissionless innovation are all not impacted. While the data protection and localization from

many regional regulations can be naturally satisfied by the architecture, more freedom in addressing can provide more possibilities for new technologies in security and privacy.

### B. Advantages

Comparing with the existing proposals, RINA, SCION, New IP, IPv10 and EI, the new proposal has following advantages:

- Unlike RINA and SCION, the new proposal is not a clean slate solution, it can keep the current IP based internet service in a region or a country unchanged, it only impacts the interconnection between regions and countries. Considering most of internet traffic is local and international traffic crossing borders of countries are relatively small, the impact to current internet service is limited. Additionally, for the impacted interconnections between regions, proper migration strategy can be developed to upgrade inter-links individually to new protocol and minimize the service interruption.
- The new protocol is orthogonal to other variations of IP, like New IP, IPv10 and EI. It can make those technologies easier to be adopted locally without global consensus and impacts.

## X. Disadvantages of New Network Protocol

The proposal will have disadvantages compared to the current Internet architecture; these include:

- The Internet is no longer a unified and flat network with the same type of addresses. While we can obtain the benefits of the new internet protocol such as diversified address, architecture and technologies, we also lose the simplicity of the current Internet.
- The traffic crossing the boundary of regions and countries are discouraged. This is not economical sometimes, i.e., the same application may have to deploy more servers in different regions to provide the local services. This is the same side effect as the requirement to provide the localized services based the regulations in some major countries and regions.
- The root DNS servers distributed in different region or country will require the information exchanging and database synchronization. This is not needed for the current DNS system.

## XI. Conclusions And Future Work

The paper has proposed a new network protocol and architecture that can provide more flexibility and mitigate Internet ossification. The new architecture is distributed without any central control, thus making the Internet more robust and resilient to geopolitical interruption. It can also expand the usable Internet resources for each region and country. Meanwhile, the new proposal can keep the current IP based Internet in regions, thus it can minimize the impacts to Internet and maximize the old investments.

Further works are needed for detailed solutions in every area where the new technologies or protocol redesign are required, such as protocol for distributed DNS, the control protocols and forwarding engine for interconnection between regions, upgrading and migration approaches, etc.

It must be noted that the purpose of the paper is to analyze the internet ossification and possible solutions for future internet. It is expected that any solution including the proposal in the paper will face a lot of questioning, challenges, and objections. For example, the basic IPv4 and IPv6 packet formats have never been changed since the 1st version were proposed in IETF. But it is believed that doing something will be better than doing nothing. As the most important invention of human beings, the Internet can only be pushed forward after whole interested parties join the work and contribute the ideas.

## References

[1] L. Han and R. Li, “On the Study of Internet Ossification and Solution,” Internet 2023, IARIA, https://www.thinkmind.org/articles/internet_2023_1_30_40006.pdf.

[2] “Internet Protocol,” RFC 791, Internet Engineering Task Force, Sept. 1981.

[3] A. Bridgwater, “What is a digital asset?,” Computerweekly.com. 2014. [Online]. Available: http://www.computerweekly.com/blogs/cwdn/2013/09/what-is-a-digital-asset.html. [Accessed on Aug. 7, 2023]

[4] J. Pohle and T. Thiel, "Digital sovereignty," Internet Policy Review, vol. 9, no. 4, 2020.

[5] S. Deering and R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification,” RFC 8200, Internet Engineering Task Force, July, 2017.

[6] “Internet,” Merriam-Webster.com Dictionary, Merriam-Webster, [Online]. Available: https://www.merriam-webster.com/dictionary/Internet. [Accessed on Mar. 7, 2023].

[7] 3GPP, “5G System Overview,” [Online]. Available: https://www.3gpp.org/technologies/5g-system-overview. [Accessed on Mar. 7, 2023].

[8] “Internet of Things,” Encyclopedia Britannica, Encyclopedia Britannica, Inc., [Online]. Available: https://www.britannica.com/science/Internet-of-Things. [Accessed on Mar. 7, 2023].

[9] 3GPP, “Solutions for NR to support Non-Terrestrial Networks (NTN),” TS 38.821. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/38_series/38.821/38821-g10.zip.

[10] “Internet Assigned Numbers Authority (IANA),” [Online]. Available: https://www.iana.org/. [Accessed on Mar. 7, 2023].

[11] APNIC, “Understanding address management hierarchy,” [Online]. Available: https://www.apnic.net/manage-ip/manage-resources/address-management-objectives-2/address-management-objectives/ [Accessed on Mar. 7, 2023].

[12] “Autonomous System (AS) Numbers,” Internet Assigned Numbers Authority. [Online]. Available: https://www.iana.org/assignments/as-numbers/as-numbers.xhtml. [Accessed on Mar. 7, 2023].

[13] Y. Rekhter, T. Li, and S. Hares, “A Border Gateway Protocol 4 (BGP-4),” RFC 4271, Internet Engineering Task Force, Jan. 2006.

[14] “Domain Name Services,” Internet Assigned Numbers Authority. [Online]. Available: https://www.iana.org/domains. [Accessed on Mar. 7, 2023].

[15] “Root_Zone Management,” Internet Assigned Numbers Authority. [Online]. Available: https://www.iana.org/domains/root. [Accessed on Mar. 7, 2023].

[16] "Root Servers," Internet Assigned Numbers Authority. [Online]. Available: https://www.iana.org/domains/root/servers [Accessed on Mar. 7, 2023].

[17] T. Narten, E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," RFC 4861, Internet Engineering Task Force, Sept. 2007.

[18] T. Mrugalski et al., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," RFC 8415, Internet Engineering Task Force, Nov. 2018.

[19] C. Hopps, "Routing IPv6 with IS-IS," RFC 5308, Internet Engineering Task Force, Oct. 2008.

[20] R. Coltun, D. Ferguson, J. Moy, and A. Lindem, "OSPF for IPv6," RFC 5340, Internet Engineering Task Force, July 2008.

[21] E. Rosen, A. Viswanathan and R. Callon, "Multiprotocol Label Switching Architecture," RFC 3031, Internet Engineering Task Force, Jan. 2001.

[22] Daniel O. Awduche et al., "RSVP-TE: Extensions to RSVP for LSP Tunnels," RFC 3209, Internet Engineering Task Force, Dec. 2001

[23] L. Ginsberg, B. Decraene, S. Litkowski, and R. Shakir, "Segment Routing Architecture,". RFC 8402, Internet Engineering Task Force, July 2018.

[24] J. Postel, "Transmission Control Protocol," RFC 793, Internet Engineering Task Force, Sept. 1981.

[25] J. Postel, "User Datagram Protocol," RFC 768, Internet Engineering Task Force, Aug. 1980.

[26] J. Iyengar and M. Thomson, "QUIC: A UDP-Based Multiplexed and Secure Transport," RFC 9000, Internet Engineering Task Force, May 2021.

[27] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, Internet Engineering Task Force, August 2018.

[28] E. Rescorla and A. Schiffman, "The Secure HyperText Transfer Protocol", RFC 2660, Internet Engineering Task Force, August 1999.

[29] J. Mccauley, S. Shenker, and G. Varghese, "Extracting the Essential Simplicity of the Internet," Communications of the ACM, vol. 66, no. 2, pp. 64-74, February 2023.

[30] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460, Internet Engineering Task Force, Dec. 1998.

[31] S.D. Schoen, J. Gilmore, and D. Täht, "IETF Will Continue Maintaining IPv4, " draft-schoen-intarea-ietf-maintaining-ipv4, Internet Engineering Task Force, Sept. 2022.

[32] J. Day, Patterns in Network Architecture: A Return to Fundamentals, Prentice Hall, 2008.

[33] X. Zhang et al., "SCION: Scalability, Control, and Isolation on Next-Generation Networks," *2011 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 2011, pp. 212-227, doi: 10.1109/SP.2011.45.

[34] S. Jiang, S. Yan, L. Geng, C. Cao, and H. Xu, "New IP, Shaping Future Network: Propose to initiate the discussion of strategy transformation for ITU-T", TSAG C-83, Sept. 2019.

[35] K. Omar, "Internet Protocol version 10 (IPv10) Specification," draft-omar-ipv10, Internet Engineering Task Force, Sept. 2017.

[36] H. Balakrishnan et al., "Revitalizing the public internet by making it extensible," ACM SIGCOMM Computer Communication Review, vol. 51, no. 2, pp. 18–24, April 2021.

[37] International Computer Science Institute, University of California, Berkeley, "An Extensible Internet for Science Applications and Beyond," [Online]. Available: https://www.icsi.berkeley.edu/icsi/projects/extensible-internet/science-applications.

[38] T. Eckert, L. Han, C. Westphal, and R. Li, "An Overview of Technical Developments and Advancements for the Future of Networking," ITU Journal on Future and Evolving Technologies, vol. 3, no. 3, December 2022.

[39] "Host Identity Protocol Working Group," IETF, [Online] Available: https://datatracker.ietf.org/wg/hip/about/.

[40] R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture," RFC 4423, IETF, [Online] Available: https://www.rfc-editor.org/rfc/rfc4423.txt.

[41] S. Frankel and S. Krishnan, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap," RFC 6071, IETF, [Online] Available: https://www.rfc-editor.org/rfc/rfc6071.txt.

[42] "Understanding Denial-of-Service Attacks," Cyber Security and Infrastucture Security Agency, U.S.A, [Online]. Available: https://www.cisa.gov/news-events/news/understanding-denial-service-attacks.

[43] "Understanding and Responding to Distributed Denial-of-Service Attacks," Cybersecurity and Infrastructure Security Agency, U.S.A, [Online]. Available: https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf.

[44] Nick Merrill, "Taiwan & the internet during world war," [Online]. Available: https://www.else.how/p/taiwan-and-the-internet-during-world.

[45] "E.164 : The international public telecommunication numbering plan," International Telecommunication Union. [Online]. Available: https://www.itu.int/rec/T-REC-E.164/. [Accessed on Mar. 7, 2023].

[46] W. J. Drake, V. G. Cerf, and W. Kleinwächter, "Internet Fragmentation: An Overview," [Online]. Available: https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf. [Accessed on Mar. 7, 2023].