TECHNICAL REPORT

ISO/IEC TR 29181-2

First edition
2014-12-15

Information technology — Future Network — Problem statement and requirements —

Part 2: Naming and addressing

Technologies de l'information — Réseaux du futur — Énoncé du problème et exigences —

Partie 2: Dénomination et adressage

Reference number
ISO/IEC TR 29181-2:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 6, *Telecommunication and information exchange between systems*.

ISO/IEC TR 29181 consists of the following parts, under the general title *Information technology — Future Network — Problem statement and requirements*:

— *Part 1: Overall aspects*

— *Part 2: Naming and addressing*

— *Part 3: Switching and routing*

— *Part 4: Mobility*

— *Part 5: Security*

— *Part 6: Media transport*

— *Part 7: Service composition*

Introduction

This part of ISO/IEC TR 29181 is the second part of this Technical Report on Future Network — Problem statement and requirements developed by ISO/IEC JTC1 SC6. As ISO/IEC TR 29181-1 provides an overall perspective of the missions and requirements of the FN project, this part of ISO/IEC TR 29181 focuses on the issue of naming and addressing. The objective of this part of ISO/IEC TR 29181 is to discuss how to develop a clean slate designed new naming and addressing schemes (NAS) to help FN project achieve its lofty ambitions.

Naming and addressing schemes are the cornerstones of telecommunication networks and information systems. NAS designs not only provide fundamental building blocks for network designs, but can also influence network characteristics, performance, and capabilities. Therefore, NAS needs to be among the top priorities of network design projects.

NAS plays an even more important role in FN. As a project aimed at designing a totally new network with a clean slate design approach, FN has to produce a clean slate designed naming and addressing scheme. The need for new naming and addressing systems were based from the gaps between the existing NAS systems and the rising future demands of new applications which produces many technical challenges the existing NAS systems cannot provide satisfactory solutions. This Technical Report summarizes some of the challenges and also offers some new directions for future research on NAS standardization.

However, as the new network has to produce a network structure which would allow information to flow more smoothly, fast, and securely among various networks with various kinds of naming and addressing structures, designing a new NAS which would not only function within the new system, but also interoperate with other naming and addressing systems (such as old systems like DNS or telecom networks and new systems such as RFID and sensor networks) is a very challenging task.

Considering evolutionary approaches which seek to engage gradual improvement with available technologies while protecting the integrity of overall structure of old networks, a new scheme will produce a totally new naming and addressing scheme. A clean slate design needs thorough analysis, full understanding of the demand, careful planning, and collective work. In order to achieve the maximum benefits and find the best solution, a strategic planning document is needed before specific schemes are standardized.

Information technology — Future Network — Problem statement and requirements —

Part 2: Naming and addressing

1 Scope

This part of ISO/IEC TR 29181 describes the general characteristics of Future Network naming and addressing schemes, including problem statements, requirements, design objectives, gap analysis, and development directions.

— Problem Statements: The characteristics and problems of existing NAS in existing network will be discussed.

— Technical Challenges: A list of major technical challenges to assure that the FN-NAS will be able to provide solid technical support from the base level to meet the objectives of FN.

— Requirements: The general characteristics of Future Network are discussed and their impact on NAS design.

— Gap analysis: Examines the gap between existing network NAS and future network performance expectations.

In Annex A, FN-NAS Standardization Plan, design objectives, gap analysis, development guidance, chronological scenarios for future network naming, and addressing guidance are described in detail.

Though this part of ISO/IEC TR 29181 mainly presents a list of up-to-date surveyed problems, requirements, and plausible techniques for Future Network, it does not mean that all of those would be applied to a single Future Network in common, since the naming and addressing scheme can be applied to the various networks, such as global networks, local networks, access networks, mobile networks, etc. If a specific Future Network is designed and implemented, some appropriate parts of ISO/IEC TR 29181 would be considered depending on its network usage and its characteristics.

2 Terms and Definitions

For the purposes of this document, the following terms and definitions apply.

2.1
Future Network naming and addressing schemes
system of mechanisms to provide identify and locate for information exchange in Future Network

Note 1 to entry: The system may design new naming schemes, new addressing schemes or an integrated scheme that combines identification and location.

2.2
naming
scheme which gives identity to every computer or object connected with the network or the party who is going to send or receive information from the network

2.3
addressing
scheme which provides information on the point, where sender or receiver is located in the networks

Note 1 to entry: It contains two mechanisms, one is to define the location (address format) and another is to specify how to find the addresses.

2.4
naming authority pointer
NAPTR
type of DNS resource record, used in particular (but not only) which is used for E.164 telephone number to URI resolution

[SOURCE: IETF RFC 3403(NAPTR)]

2.5
routing locator
RLOC
sddress of an ETR

Note 1 to entry: Typically, RLOCs are numbered from topologically- aggregatable blocks that are assigned to a site at each point to which it attaches to the global Internet.

[SOURCE: IETF RFC 6830 (LISP)]

2.6
end point identification
EID
address used in the source and destination fields of the most inner LISP header of a packet

Note 1 to entry: The host obtains a destination EID the same way it obtains a destination address today. The source EID is obtained via existing mechanisms used to set a host's "local" IP address.

[SOURCE: IETF RFC 6830 (LISP)]

2.7
ingress tunnel router
ITR
router that resides in a LISP site

Note 1 to entry: Packets sent by sources inside of the LISP site to destinations outside of the site are candidates for encapsulation by the ITR. The ITR treats the IP destination address as an EID and performs an EID-to-RLOC mapping lookup.

[SOURCE: IETF RFC 6830 (LISP)]

2.8
egress tunnel router
ETR
router that accepts an IP packet where the destination address in the "outer" IP header is one of its own RLOCs

Note 1 to entry: In general, an ETR receives LISP-encapsulated IP packets from the Internet on one side and sends de-capsulated IP packets to site end-systems on the other side. ETR functionality does not have to be limited to a router device. A server host can be the endpoint of a LISP tunnel as well.

[SOURCE: IETF RFC 6830 (LISP)]

2.9
EID-to-RLOC database
global distributed database that contains all known EID-prefix to RLOC mappings

Note 1 to entry: Each potential ETR typically contains a small piece of the database: the EID-to-RLOC mappings for the EID prefixes "behind" the router.

[SOURCE: IETF RFC 6830 (LISP)]

2.10
locator
LOC
network layer topological name for an interface or a set of interfaces

Note 1 to entry: LOCs are carried in the IP address fields as packets that traverse the network.

[SOURCE: ITU-T Y.2015 (2011)]

2.11
node ID
identifier used at the transport and higher layers to identify the node as well as the endpoint of a communication session

Note 1 to entry: A node ID is independent of the node location as well as the network to which the node is attached so that the node ID is not required to change even when the node changes its network connectivity by physically moving or simply activating another interface.

[SOURCE: ITU-T Y.2015 (2011)]

2.12
ID/LOC mapping storage function
stores the mapping of NGN identifiers, node IDs, and LOCs

[SOURCE: ITU-T Y.2015 (2011)]

2.13
address
identifier for a specific termination point and is used for routing to this termination point

[SOURCE: ITU-T Y.2091 (2011)]

2.14
identifier
series of digits, characters, and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g. physical or logical objects)

[SOURCE: ITU-T Y.2091 (2011)]

2.15
name
identifier of any entity (e.g. subscriber, network element) that may be resolved/translated into an address

[SOURCE: ITU-T Y.2091 (2011)]

3 Abbreviations

DNS Domain Name Service

EID Endpoint ID

ENUM	E.164 NUmber Mapping
ID	Identifier
LER	Locator Edge Router
LOC	Locator
NAPTR	Naming Authority Pointer
NAS	Naming and Addressing Scheme
NID	Node ID
RLOR	Routing Locator

4 Problem statements

4.1 Naming and Addressing in Network Operation

Naming and addressing are an engineering approach to computer networking, and are two closely related core schemes in any network designs. Both names and addresses uniquely identify a host (or an interface on the host) Naming is a scheme which gives identity to every computer or object connected with the network or the party who is going to send or receive information from the network. -.

Addressing is a scheme which provides information on the point where receiver node is located in the networks. It contains two mechanisms in a single address field; one is to define the location and another is to specify how to find the addresses

At present, due the explosive growth of devices (especially mobile devices) and sites, scalability and mobility become hot issues to the future network.

Communication networks (composed of telecom networks and computer networks) are designed to deliver information from one point to another remote point or from one person to another person. In order to conduct the delivery, the sender must know the other party's name and where the other party is located. Therefore, a network system must contain the naming and addressing schemes as the most fundamental protocols so that the telecommunication networks and information systems know whom and where to send the information effectively and efficiently.

4.2 NAS Types

4.2.1 Telecom Network Naming and Addressing Schemes — addressing mode

The first generation of network is the traditional telecom network which is typically known for telephone system sending analogue signals through circuit switches and copper lines (or modernized fiber optical lines). The phone network connects people at two ends of the communication line. Typically, E.164 numbering system has been being used. The phone numbers have two different characteristics. One is a pure object identifier (a name), the other is function as an address.

For fixed line communication in first generation telecom networks, the fixed line telephone number is a simply address mode. A phone number actually contains information about the location and path. Fixed line telephone number is a system that mostly relies on addressing schemes. Furthermore, the E.164 is regarded as an easy-to-remember well organized addressing scheme.

Note: For example, when people dial number 861088888888,the telecom switch instantly know the identification of the party been called, but also knows which country (86) which city (10) and which location (88888888) the party is located. The telephone address is fixed, but the person who was called is unsure or not a requirement for communication.

Figure 1 — Addressing Mode NAS (Telecom network)

4.2.2 Telecom Network Naming and Addressing Schemes — naming mode

Other than the fixed line telecom networks, there is another type of network which sends communication signals not through wire but through the air, mobile telecom network, in which E.164 numbering system is also being used. In these kinds of networks, the same E.164 addressing does not provide the location (or device name) and path at the same time. The address is just a device name only, while mobile telecom network provides the path to the point where the device name is located using location management.

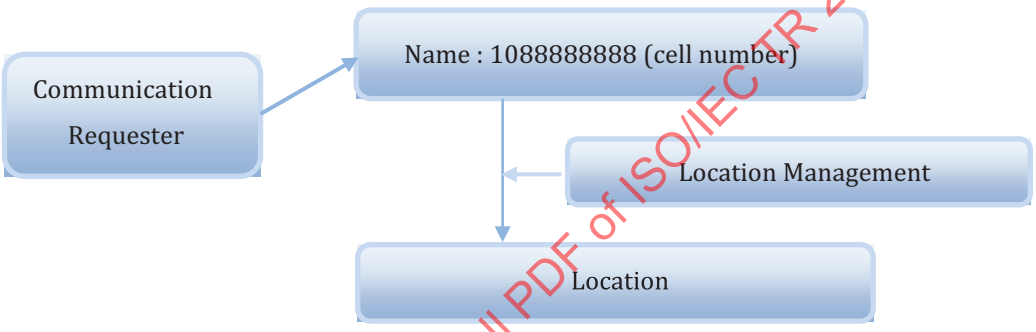

Figure 2 — Naming Mode NAS (Mobile Telecom network)

4.2.3 Computer Network Naming and Addressing Schemes — dual mode

Another generation of network is represented by Internet which mostly sending digital signals through routers and fibre optical backbones to connect computer hosts. In computer networks (Internet), there is also an address only communication mode. Internet address is composed of subnet prefix and host Identification, where host identification is to locate the host, while subnet prefix is advertised to the routers for routing path.

Since the internet address itself identifies a host or subnet, it faces some serious problems: (1) it does not scale well due to the finite address size limitation, (2) due to the renumbering, occurring whenever the network topologies change, more addresses are required, (3) the increased size of address field comes to be heavy especially in the short data payload packet, and (4) the size-increased address is worse human understandable.

Since even though the size of IPv4 address is 32 bits (relatively shorter than that of IPv6), it is not still human friendly, the name is used and translated via DNS server. It means two or more names can be assigned to the same host or site.

There is a dual mode NAS in telecommunication and information networks, in which both name and address are required for information exchange. IP based computer networks are typical dual mode NAS. IP network communication relies on domain name and IP addresses which are two different structures. Most of the computer communication involves a process inputting a domain name, finding matches involving a DNS server and converting into registered IP address.

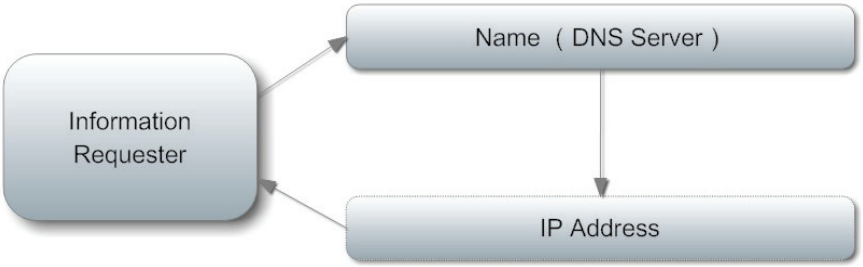

Figure 3 — Dual Mode NAS (IP network)

4.2.4 .Computer Network Naming and Addressing Schemes — naming mode

While the current internet address identifies a subnet and a host in a same address field, the other alternative is to separate host identification and subnet routing path. A same address format is separated into two new numbering spaces: an host identifier (or name) and routing locator. Each host has a globally unique ID(or EID) or name. Packet with EID is sent to the default locator router(Routing Locator, or ITR) which then map EID to destination RLOC using EID-to-RLOC database. The packet will be traversed from sending ITR to destination ETR using conventional routing mechanism. Finally the destination ETR will deliver the packet to the destination host.

While Tunnel Routers manage and maintain the routing path among them using the conventional routing mechanisms, the user only keeps the unique EID's for communication. From user's perspective, the internet access network behaves like telecom network, while the internet core itself performs in a conventional way.

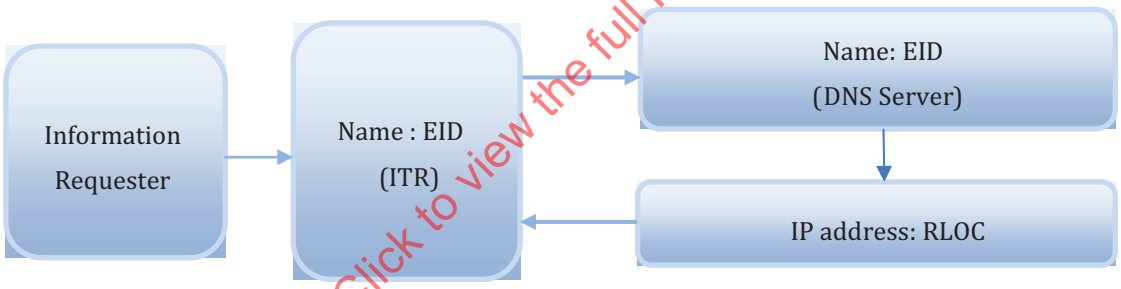

Figure 4 — Naming Mode NAS (IP network)

4.2.5 Hybrid Network Naming and Addressing Schemes — Addressing mode

Even though internet is widely deployed network and popular to users, (mobile) telecom network is another powerful and popular network as well. As long as two types of networks exist, it is natural to combine them. There are two ways to implement combined networks: Access network can be either telecom network or internet.

Since E.164 numbering is more user friendly and telecom network is more widely deployed up to date, a telephone number can be used to identify a host, while the telephone number is translated to the IP address,

Note that the use of any/multicasting changes the one-to-one association of an address with a physical endpoint

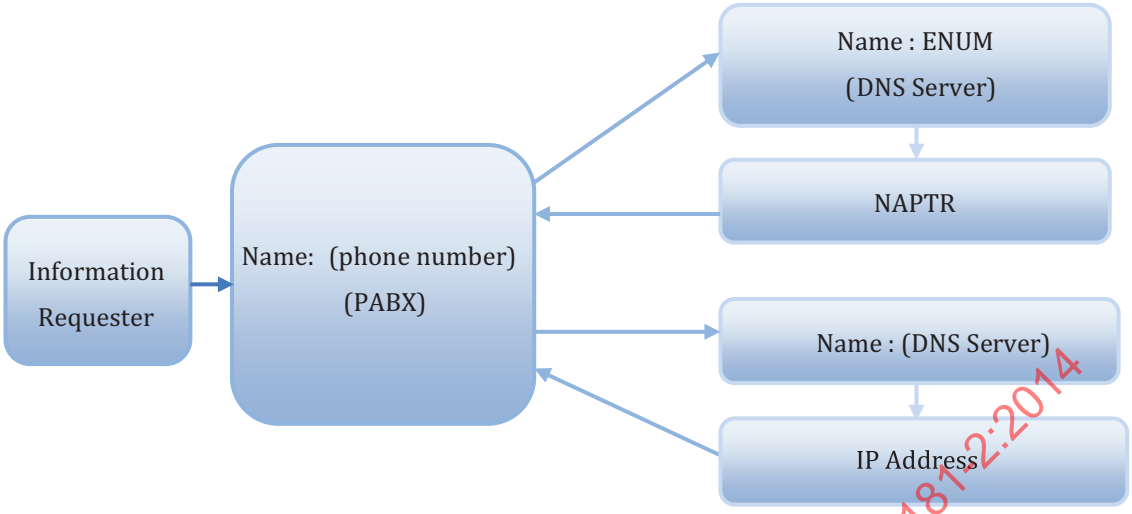

Figure 5 — Addressing Mode NAS (Telecom network + IP network)

4.3 Problems in Network Integration

The brief reviews of network naming and addressing schemes indicate some problems for any attempt to integrate existing networks.

— Telecom networks and computer networks have different addressing formats.

— Telecom networks and computer networks have different naming formats and different method in addressing searching, transporting and forwarding.

— Many forms of naming and addressing in old networks make the network integration very complicated, if not impossible. Even though technicians can find technologies to allow information shared among the networks, it would be a huge effort to overhaul the existing network infrastructures.

— In order to avoid duplicating construction, sharing network resources, providing more and better services, there is a tendency to integrate various kinds of networks into one system to allow information seamlessly transmitted among networks. This is one of the objectives for Future Network.

— Considering the fact that IP networks have the potential to be a platform for future network integration, its own problems should be fundamentally resolved. Otherwise, if they are spread into other networks, it would bring more broad and severe problems.

4.4 NAS and Network Performance

In network designs, naming and addressing are not only essential and indispensable, but should also occupy top priority in design schedules. Reasons are:

— Only after naming and addressing schemes are set, the whole architecture and other subsystems such as router designs and application services can have a base to start work on.

— NAS structures may affect network performances

— NAS format influences network security

— NAS format influences accuracy for information delivery, etc.

4.5 Technical Limitations of Existing Naming and Addressing System

4.5.1 Central Registration Authority

The existing schemes require the Central registration authority, which maintains the control of the key facilities of the Internet. This causes widely concerns of information security among the international community.

4.5.2 Address Space exhaustion

IPv4 addressing space would be in danger of exhaustion due to the increased numbers of wireless devices, always-on connections, or higher Internet adoption rates. The development and planned deployment of IPv6 was regarded to be a long-term solution to this problem. However, its deployment is being delayed.

4.5.3 Name and Address Costs

The centralized domain name registration schemes create economic burdens for heavy IP address users or nations.

4.5.4 Identifier-Locator Separation

IP address identifies an attachment point of an IP node for data delivery. Also It is used as a transport layer session identifier, or even by some applications as node identifier. When host changes its IP address, transport layer session breaks downs, and so does application on top of it.

4.5.5 Routing Table

Routing tables are becoming more and more bulky. It causes problems for management and maintenance and increases router work load due to the increased number of sites, or possibly due to the increased address size.

4.5.6 Vertical Addressing Structure

Centralized domain name system forms a vertical addressing structure with multiple redundancy or bottlenecks which generate or increase heavy network congestion.

4.5.7 DNS Translation

The separation of domain names and IP addresses requires a Domain name to IP Address translation process. Failure of DNS system may cause degradation of overall network performance.

4.5.8 Data Encryption

IPv4 can only utilize data encryption (IPv6-IPSec[1)]), but its addresses cannot be encrypted. It cannot provide address confidentiality.

4.5.9 Address Category

IPv4 addresses can only provide “type” addresses, but do not provide “leveled” addresses which are essential for high quality communication applications such as multi-media and real time information transmissions.

1) Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, and data confidentiality (encryption), and replay protection. The Microsoft implementation of IPsec is based on Internet Engineering Task Force (IETF) standards.

4.5.10 Policy

Existing naming and addressing schemes lacks consideration or respect for geographical or national boundary considerations. It creates problems for national government in network management and information security. With additional information like geographical location, it may solve the current problems like scalability, mobility, security, etc.

4.5.11 No Address in Native Language

IP domain names and addresses schemes do not provide language (such as Chinese, Korean, Japanese, Russian, French, German, etc.) direct routing function, and have to rely on domain name conversion schemes.

However, current domain name conversion systems do not provide multiple language supports other than English. It does not convert domain names based on other languages such as Chinese, Korean, Japanese, Russian, French, German, Arabian, etc.

4.5.12 No Decimal Naming System

Current domain name conversion system does not provide all decimal name systems such as telephone number, OID coding, mobile phone number, merchandise code, etc. Those numbers have to be inserted into English domain names for conversion. It makes the process complicated, reduces data security, and wastes network resources.

4.5.13 IPv6 Limitations

The major improvements of IPv6 are that it increases the length of IP addresses and expands address resources. However, IPv6 does not make significant changes to other aspects of the IPv4 domain naming and addressing structure. IPv6 still carries most of IPv4 problems in naming and addressing without additional properties considering management, security and economic efficiency.

4.6 FN-NAS Development Challenges

4.6.1 Scalability

The rigid structure of centralized domain registration and hierarchical routing systems in IPv4-IPv6 prevent scalable networks from emerging. Scalability issues have mobility, multi-homing, renumbering, provider independence routing, IPv6 impact, etc. on the today's Internet architecture.

4.6.2 Security

The centralized domain name conversion and exposed IP addresses cause wide security concerns.

4.6.3 Mobility:

Current domain names and address protocols does not fit well into the future network environment which will have more and more new communication devices or services such as mobile phones, RFID, sensors, etc.

4.6.4 Quality of Service

The future network should support quality of service (QoS) from user and/or application perspectives. The current IP-based network naming and addressing schemes needs to give more freedom to users and more rooms of expansion for applications.

Even though it seems that QoS may not be directly related to NAS, QoS is mentioned here since it is closely related the routing which is based on the addressing scheme.

4.6.5 Heterogeneity

Current domain names and address is incapable of providing name and address structural support for accommodating the integrated networks.

4.6.6 Robustness:

The centralized domain name conversion and hierarchical network routing structures in current IP-based networks is one of the causes for network congestion.

4.6.7 Customizability

Current naming and addressing schemes has too rigid policies and does not provide flexibility for customized network communications.

4.6.8 Economic incentives

Current IP, especially IP domain names and addresses fee systems are too expensive for users. Better designed naming and addressing structures also may produce economic incentives resulting from more security and network efficiency.

5 Requirements

5.1 Content Description

This section describes technical requirements for FN-NAS design, including the following aspects:

— System Requirements: Including design concepts, system architecture, etc.;

— Special NAS requirements: including address format, network space, network communication structure, routing, DNS, communication protocols, security, etc.

— Foreseeing mechanism: consider how the Future Network will change and benefit the human society in the future.

— Compatibility Requirement: considering the emergence of FN-NAS will largely influence Future Network's basic technological designs including network space, network resources, communication protocols, network architectural modes, security, QoS, routing protocols, upper layer protocols, interoperability, it is desirable to have considerations and design to allow compatibility and interoperability with existing networks.

— Others: Future network forward compatibility, future continuous development and testing and compliance requirements.

Reasons for specifying these technical requirements are:

— From the perspective of network performance, demonstrative Future Network's main characteristics and capabilities, and to show a more clear future outlook for the development of Future Network.

— To point out objectives and directions for global research on new generation networks.

— To produce clear criteria for technical assessment in the next stage (proposal evaluation)

— To provide reference criteria for other research projects in Future Network program.

5.2 System Technical Requirements

5.2.1 System Integrity Requirement

From the perspective of system requirements, a complete NAS system should include at least the following elements: naming, network space, network resources, addresses, network architecture, predictive mathematic model, application, experiment, testing, etc. FN-NAS plan must have these elements. (From historical experiences, some communication system may requirement single mode, such as naming only or address only. If a proposal specifies only one mode, reasons must be given.

5.2.2 Intersystem Coherence Requirement

Besides having many sub-systems inside FN-NAS, it is also a part of a larger Future Network system. FN-NAS should not only study and seek coherence among its sub-systems, but also should seek compatibility and mutual support with the larger system. FN-NAS should consider how to be consistent, supportive, benefit and interoperate with other systems in Future Network. FN-NAS should not produce conflict with other systems and should avoid lowering the Future Network performance to meet the lower requirements caused by deficient NAS design.

5.2.3 Structural Requirement

5.2.3.1 Addressing Structure

Future Network should have a complete new addressing structure with the following requirements:

— Good human-machine interface.

— Support conventional computing, future quantum computing, biological computing and other computing language and various human languages based computing, and their compatibility and interoperability.

— Protocol, addressing format and addressing solution schemes that would form a secure network structure supporting and satisfying the concept of authentication before communication.

— A communication method mixing virtual layer-three circuit switching and Layer-four packet switching.

— Direct routing network architecture that will reduce carbon emission and produce greener networks.

— Fast and large capacity network services.

— Been able to interoperate with existing networks, allowing lower cost and seamlessly upgrade of old networks, ability to maintain forward compatibility and potential for continuous development.

5.2.3.2 Reference Architecture

Existing networks mainly use two types of switching. In telecom networks (mainly telephone network) circuit switching is the primary form. In computer networks (mainly Internet), the dominant protocol is TCP/IP (simply referred as IP protocol) uses mainly packet switching. Future Network faces the task of offering both data communication and video/voice communication in one network. To solve this problem, Future Network should employ a transmission architecture model constructing a mixed layer structure, using the layer three for virtual circuit switching to transmit video broadcasting and voice communication while using the layer four structures for IP dada transmission.

5.2.3.3 A Network Structure mixing Virtual Circuit Switching and Packet Switching

Future network should be flexible so that it can be perceived as either packet switching network or virtual network, as needed. It may provide both services by implementing two separate switching mechanisms in the same intermediate node, or by implementing a new hybrid mechanism in a node.

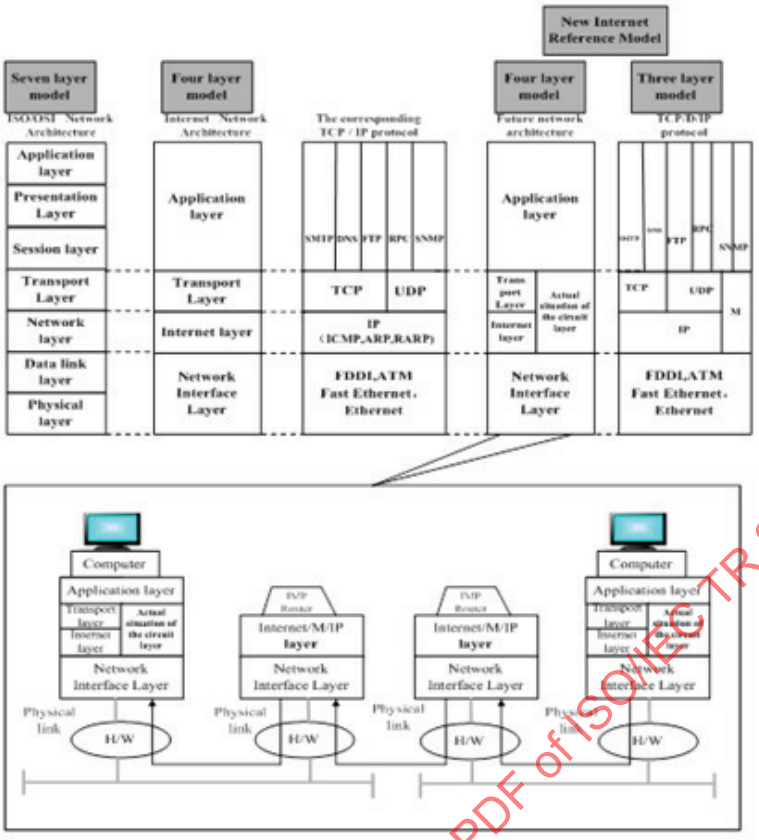

Figure 6 — Network Model for the future (Note: M = mixed protocol)

5.2.3.4 Separation of Control Layer and Data Layer

Current internet has been using the layer such as control layer and data layer. However, in this circumstance, delivery problem of control packet can occur in a situation of a flood of data packet by DDOS attack or mobility of node. As a result, control layer and data layer must be separated.

5.2.4 Specific Technical Requirements

5.2.4.1 Addressing Technical Requirements

5.2.4.1.1 Address Format

Future Network NAS should consider having a new address system which will create a totally new network space for the Future Network to exist, operate and expand.

A new address format is the foundation of a new address system. FN-NAS should have a new format of addresses that is different from all existing NAS, but it should have the potential to allow compatibility with existing address formats.

FN-NAS address format should go beyond of serving computer, but also make it more human friendly, to allow users easier operate the addressing scheme while maintaining the efficiency for computing.

Digital Coding: The ten digits Arabian numerals are globally used language. Pure decimal encoding is one of the most commonly used ways of expressing. Future Network should consider the need for pure decimal coding from real applications such as commercial good coding, sensor coding, cell phone number, geographic location, Space object location coding, molecule order coding for living bodies, etc.

Character coding: the FN-NAS address format could be in characters, such as Arabian numerals, Latin Characters or other symbols that is easy for computer recognition and human interaction. In other words, the address format should support various language environments.

5.2.4.1.2 Separation of ID and Location

IP addresses are to be replaced with two types of numbers: routing locators which is assigned to network attachment point, and endpoint numbers which is assigned independently from the network topology. However as the mobility service is widely required, the endpoint number is further divided into local network attachment point and node identification like a unique name. It means that each node will possess its own unique ID for identification, and its local network attachment point address which will be used to locate it. When it sends a data to a node which is located out of its local network, new globally unique routing locators which are assigned to the local network attachment point to the global backbone network will be used.

5.2.4.1.3 Addressing Model

— Addressing through subnet prefix in address:

  Future Network can use subnet prefix in address to fulfil addressing. A certain subnet prefix can be linked to only one link circuit or to multiple link circuit. A certain link circuit can possess multiple subnet prefix in the same time.

— Addressing through direct character addressing and direct routing

  Future Network can consider using the direct addressing through character addressing and routing, omitting the process of DNS translation. The benefits of this method is unifying the naming and addressing, enhance network performance efficiency. For compatibility considerations, the DNS translation interface should be reserved.

— Addressing through direction information

  Due to the scalability, mobility, and more diverse application services, current address is split to “ID” and “LOC”, where ID is to identify the device or any identifiable entity and LOC is assigned topologically for routing. However, still even in the core network or in the edge network, LOC and ID is to be searched through conventional ways. If additional information such like contents, QoS, policy, or direction is assigned to LOC or ID, routing can be performed based on the packet contents, physical location coordinate, and etc.

5.2.4.1.4 Address Space

Address space is one of the most important requirements for Future Network. Address is the foundation of the network space. Address not only determine the existence of a network, but also determines how big is the space of the network. The longer the address, the larger the network space will be.

The length of addresses should be long enough to create an address space which would increase the number of addresses and to satisfy the demand for longer addresses in some situations.

The first generation Internet (IPv4) address length is only 32 bits which created a problem of address shortage. IPv4 addresses ran out only twenty years after its opening to commercialization. The next (or 2nd) generation of Internet (IPv6) has 128 bits in address format. However, as the attachment to this document about geographic location based addressing scheme indicates, 128 bits may not be long enough to satisfy the needs of future applications.

Therefore, Future Network should establish a new address format with flexible length. This would also allow larger network space and long enough to satisfy most needs in the future.

5.2.4.1.5 Variable Address Length

In contrast with first generation and second generation internet protocols which both have fixed length address format, Future Network may consider variable length address format to satisfy the demand of various applications, to achieve transmission efficiency and to allow long term expansion.

5.2.4.1.6 Address Types

Future Network must go beyond the category addresses in existing networks and consider a layered address structure. The layered structure can provide layered address to satisfy the demand of high quality communication applications, such as the need for simultaneous transmission of multimedia real-time information transmission and data packet transmission. It will expand network application space and optimize addressing and routing technologies.

— Direct Routing Addresses: When characters coding are used as addresses, the routing addresses are determined by the location of the router and select the geographic regional address code as directing address method.

— Emergency Routing Addresses; FN-NAS should consider setting emergency routing addresses. In situations where networks are partially destroyed by unforeseen catastrophes, network administers can use the method of router broadcast, revise routing table, acquire other routers for emergency use.

— Verification Addresses: This type of verification addresses is the verification code to be used with address encryption/decryption.

— Direction Addresses: Direction address indicates a forwarding direction based on physical and geographical location of a node. It might be obtained by signal reception direction or GPS-like technologies.

5.2.4.1.7 Address Selection

All existing networks used fixed length and fixed bit location approach. IPv4 is 32 bits length, IPv6 is 128 bits length. Future Network may consider setting the base length of 256 bits to allow forward expansion. But Future Network would also allow variable lengths.

This variable length requirement along with the multiple address types, there will be requirement for setting address length option in the header to distinguish address types and lengths, to identify virtual circuit addresses (virtual circuit broadcasting address, virtual circuit unicast address for three layer model) and other addresses(for four layer model).

There may be following address selection methods:

— Fixed length and fixed bits location addressing scheme

— Fixed length and non-fixed bits location addressing scheme

— Addressing scheme based non-fixed length and non-fixed bits location

5.2.4.1.8 Fields in Addressing

An address may be made up with some of these fields:

— Addressing type: the type which represents what addressing is used

— Mobile/Fixed node flag: the flag that represents whether the interface connecting with node is mobile or fixed

— Backbone/local flag: the flag that represents whether address can be used in only local network or in backbone network.

— Bandwidth Information: the bandwidth information of interface that is connected with node

— Processor Information: processor information of node

— Virtual Circuit flag: the flag that represents whether Virtual Circuit is supported.

— Virtual Circuit region: information about a range of using Virtual Circuit.

— Virtual Circuit label: label that is used in Virtual Circuit

— Service type.

— ID: Identification of the end system of a communication session.

— Node Information: other distinguishing information of node

— LOC: Address assigned to routers or node for routing in the core network.

5.2.4.2 Future Network Domain Name Translation

Future Network proposes a distributed and cross boundary domain name translation system, which would allow national bodies to manage their own root servers, establishing distributed and over-the-boundary network links, straight localized translation. These approaches would reorganize global network information flow, reduce network congestion, optimize network performances, save energy and cut network costs.

5.2.4.3 Translation/Tunnelling between local and backbone networks

Either translation or tunnelling may be needed between Local network and backbone network..

First, these are the cases to use translation.

— One-to-one address translation: One address in local network is mapped to one address in backbone network the same way of current NAT.

— Many-to-one address translation: Many addresses in local network are mapped to one address in backbone network the same way of current NAT-PT.

— One-to-many address translation: One address in local network is mapped to many addresses in backbone network. The address of backbone network is determined according to service or function which node of local network uses.

— Many-to-many address translation: Many addresses in local network are mapped to many addresses in backbone network. This is the case that both many-to-one address translation and one-to-many address translation are used at once.

Second, these are the cases to use tunnelling. Tunnelling can be used in local network and backbone network.

— One-to-one tunnelling: One tunnelling address is used for one address.

— Many-to-one tunnelling: One tunnelling address is used for many addresses. This is the same way as tunnelling between routers of specific section in current internet.

— One-to-many tunnelling: Many tunnelling addresses are used for one address. Tunnelling address is determined according to service or function used for one address.

— Many-to-many tunnelling: Many tunnelling addresses are used for many addresses. This is the case that both many-to-one tunnelling and one-to-many tunnelling are used at once.

5.2.5 Complementary Technical Requirements

5.2.5.1 Security Technical Requirement

5.2.5.1.1 New Communications Rules To Supplement New NAS

In order to protect the addressing security, Future Network may consider adopting a new communication rule requiring verification of source address and destination address before sending message to the networks. The new rules should design and utilize better and newer authentication and verification systems to achieve system wide security.

— To construct a true identity authentication, verification and certification system.

— To change from passive and defensive network security into proactively managed cyber security.

— To prove communicator true identity, verify network (internet) address and routing path authenticity, and prevent unauthorized access, and realize trusted connection.

— To certify the authenticity of software and the consistency of software identity and software data, achieving trusted computing.

— Trusted connection which is the key for trusted systems. Trusted routing is the key for realizing trusted connection.

5.2.5.1.2 Address Allocation Encryption System Requirement

Future Network should consider address encryption in address allocation system, so to form a more secure network environment and prevent addresses and user information are used for hostile or malicious purposes.

This requirement can be realized in address allocation management system and DHCP system.

The address encryption is used during the communication process, local address display does not require showing of encrypted form.

5.2.5.1.3 Header Requirement

Address encryption system requires head to have sufficient expansion function. During the transmission process, only those nodes which are related to expanded head will process them, the middle routers only pay attention to the hopping limit field and routing head. The head can be flexibly reorganized according application and network demand, to achieve the option of mobility.

The system support IP level certification authentication, carried-on encryption negotiation, and some specially defined applications.

The system should have enough addresses to allow one host machine to be used in different location and different times, to perform irregular frequency hopping. These methods would prevent attackers from getting hold and locking on the user IP address value, which means better network security.

5.2.5.1.4 Emergency Routing

In Future Network protocol, there should have an emergency status code, so that emergency routing acquisition function can be established.

5.2.6 Extension Technical Requirement

Conventional internet is based on territorial surfaces. As the space activities are increased, since the internet addressing scheme is relatively free from landscape limitation, future space communication and space-earth communication will rely more and more on internet system. There will be a new application area in Space Internet.

The Space Internet would require a new set of naming and addressing schemes. FN-NAS also should consider how to make interconnection and interoperability between earth internet and future space internet.

5.2.7 Evaluation and Test Requirement

During the process of Future Network development and design, the testing and experimenting technologies and certification requirements should also be developed and standardized. Criteria should include, but not limited to, functions, media transport, equipment, performance, network management, power usage, environment, security and economic benefits.

5.2.8 Infrastructure Requirement

FN-NAS should consider the need and time requirement from the perspective of network infrastructure establishment such as:

— The construction of Future Network experimental platform

— Construction of Future Network Backbone

— Experiment of transition of existing networks to Future Network

— Construction Future Network system and connect with existing networks.

— Building management systems.

— Building application platforms.

— Testing and compliance

Annex A
(informative)

FN-NAS Standardization Plan

This technical report outlines the objectives, tasks and requirements for FN-NAS and produces many important claims. If these claims are agreed by national bodies, they will form a solid ground to start. When objectives and directions are clear, the next is to find a rout for going forward. Making an action plan for FN-NAs is also an important objective for this report. This plan should not only cover what to do, but also a general time line.

A.1 Gap Analysis

Future Network is to create a network that would be able to satisfy future long-term technical and socio-economic needs. To achieve these objectives, FN would take the clean slate design approach, which means to design a new network based on fresh new ideas, principles, rules, methods and structures.

The clean slate design approach would face several problems. The first problem is that for many years network designers have been accustomed to doing maintenance and amending work. The clean slate approach would create challenges to them both mentally and technically. Another problem is the complication of networks. One of the objectives of Future Network is to allow information run smoothly among various networks. The new design has to take into account of characteristics of various networks and provide a coherent plan for more efficient information exchange among the networks, both old and new.

Furthermore, FN would involve a lot more factors (e.g. information security of nation) other than technology. Factors would have huge impact upon the way how FN standardize. And these are how technical experts handle those non-technical influences.

The same shall apply to NAS. For example, there are many different schemes in naming and addressing in existing networks. FN-NAS has to know the advantages and deficiencies of existing NAS so that advantages can be preserved and defects are corrected or avoided in the new NAS.

Facing these hard challenges, it is wise for Future Network to take a cautious approach by developing technical report first before formal standards are developed. This approach would allow technical experts and network designers see the whole picture of the situation and have a clear and common view of the objectives.

Based on above analysis of the limitations of current IP-based network technologies, we can derive the following views:

— Current IP-based networks have some deficiencies.

— Those deficiencies result from structural designs.

— Problems in current IP-based networks were largely related to inefficiency in naming and addressing schemes.

— It is impossible to overcome those problems without structural overhaul.

— The evolutionary approaches such as IPv6 may be still inadequate to fix the problems.

— A clean-state design must include redesigning the naming and addressing schemes.

In order to achieve the design goals of Future Network, gaps between the goals and current systems should be resolved

A.2 FN-NAS Development Plan

FN-NAS development plan include five steps:

Step 1 Situation Analysis: to study the need for NAS and its relationship in Future Network. The focus is on whether NAS be included as a project in FN. This step has mostly completed during 2007-2008.

Step 2 Project Visioning: To set missions for FN-NAS, set project objectives, identify major problems, look for approaches, establish development guidelines, etc. Chinese expert contribution in 6N13948 has produced a solid ground for this work. This technical report will incorporate 6N13948 and go a step further by taking the work specified in step 3.

Step 3 Technical challenges: To achieve the lofty visions of Future Network, FN-NAS has to overcome many technical challenges. A successful NAS design has to show the ability to support technologies that would satisfy demands from all kinds of applications in the future. Knowing what the challenges are would help developers to produce a well-planned scheme.

This technical report describes design principles and technical requirements for FN-NAS. The purpose of producing this report is to provide general guidelines for network researches to assist their research and design new NAS that would be usable in FN. Another purpose is to set a list of technical performance standards based on which prospective technical proposals can be evaluated and selected.

Developing NAS is a very daunting task, requiring a lot of thinking, experimenting, huge resources and technical challenges. ISO/IEC does not have the resources to develop the technologies. ISO/IEC Future Network can invite members to contribute mature new NAS technologies and standardize them as International Standards. However, ISO/IEC should not sit and wait for new NAS to appear and take what is available. As the organization controlling the standardization process, ISO/IEC can set guidelines, directions, requirements and qualifications for NAS technical proposals.

Step 4 Proposal evaluation: After Step 3 is complete (common criteria for evaluation of NAS technical strength is set) SC6 should send out calls for proposals which would compete for acceptance as FN-NAS candidate and technology provider. Competing proposals then will be evaluated or organized. The proposal or a combination of proposals which meet the prerequisite conditions and can overcome the most challenges will be accepted as core FN-NAS project.

Step 5 Standard development: NAS standards will be developed based on the core FN-NAS technology.

A.3 FN-NAS Standardization Plan

A.3.1 Major Tasks in the Future

The major tasks in the future for FN-NAS include:

— Refine and complete this technical report

— Look for and select the best proposal for a general framework on FN-NAS

— Standardize the general framework of FU-NAS

— Make standards of specific schemes under the general framework of FN-NAS

— Make complementary standards or imbedding FN-NAS into Future Network system

— Provide NAS assistance to study of Future Network applications

— Start work on registration and distribution of numbers and addresses for Future Network

— Make a plan for address resources management policies

A.3.2 Time line

Table A.1 — Timeline of FN-NAS Development

A.3.3 Coordination with Other Organizations

Future Network NAS research would have an extensive impact on network research and would therefore attract attention from many organizations. How to coordinate with other organizations? The following are some guiding principles:

a) Maintain Independence: Future Network is developing a new set of naming and addressing schemes, without complying with restrictions in any old rules. Therefore, Future Network project should have self-determining rights regarding the format and content of FN-NAS. Any relationship with other organizations should not undermine this right.

b) FN-NAS will face two types of issues when interacting with other organizations. The first kind is how to deal with old NAS schemes, and the other is how to deal with new NAS projects that is developed in parallel with the ISO/IEC project. Different guiding principles should be developed for these two situations.

c) For old NAS systems and their developers/maintainers, Future Network can adopt the following policies: Clearly explain the difference between evolutionary and clean slate designed NAS projects; state clearly that FN does not oppose the continued existence and improvement of old NAS; the new NAS would not seek to disrupt or destroy old network; the old and new networks can have a peaceful coexistence, develop in parallel path, utilize each other's advantages and strengths; the New NAS development work does not discriminate or reject research and development on technologies providing compatibility and interoperability between old and new network systems; when new technologies emerges which can enhance both old and new networks, we will consider mutual beneficial actions such as either joint development, dual adoption or making recommendation.

d) The standardization on Future Network Naming and Addressing should be proceeded with any SDO's which are interested in this subject

Annex B
(informative)

Current Internet technology

B.1 HMIPv6

HMIPv6[1] allows nodes' communication with correspond nodes without changing its IP address while moving in IPv6 network. HMIPv6 mobile node has HoA and CoA. HoA of mobile node doesn't change while movement. CoA is an address only in visited foreign network. While mobile node moves the foreign network, basically mobile node and corresponding node communicate by the tunnelled packet through home agent. The tunnelled header contains the mobile node's CoA and home agent's address. If mobile node and correspond node use additional signalling, mobile node and correspond node can communicate directly.

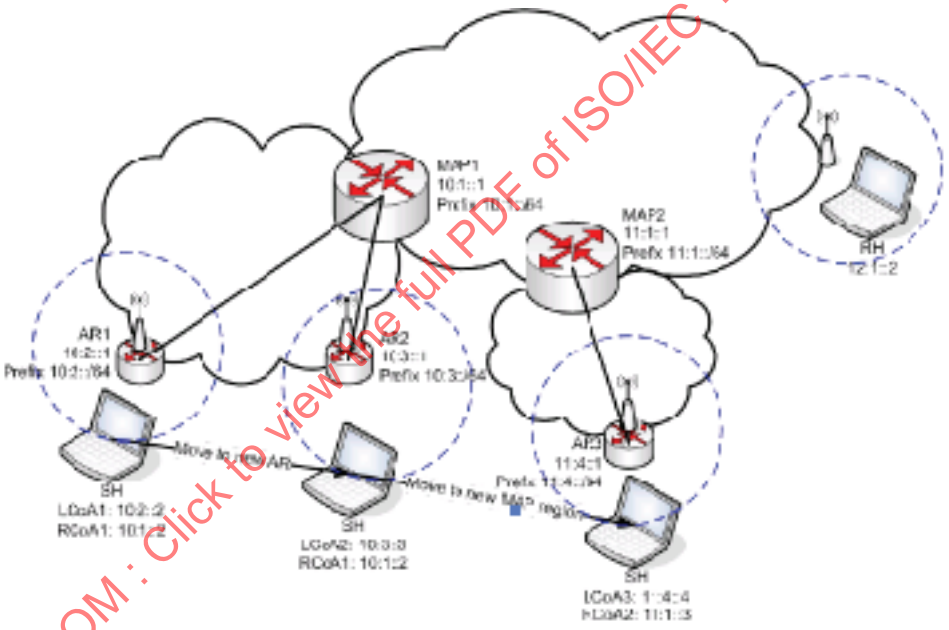

Figure B.1 — Handover in HMIPv6 network

B.2 LISP

LISP[4][7] proposed for solving routing scalability problem. LISP separate IP address with RLOCs (Routing Locator) and EIDs (Endpoint Identifiers). An EID is a 32-bit (for IPv4) or 128-bit (for IPv6) value used in the source and destination address fields of the first (most inner) LISP header of a packet. An EID is allocated to a host from an EID-prefix block associated with the site where the host is located. EIDs use for end-to-end packet exchange. A RLOC is an IPv4 or IPv6 address of an egress tunnel router (ETR). A RLOC is the output of an EID-to-RLOC mapping lookup. An EID maps to one or more RLOCs. RLOCs are numbered from topologically-aggregatable blocks that are assigned to a site at each point to which it attaches to the global Internet. A RLOC is the output of an EID-to-RLOC mapping lookup. RLOCs use between ITR and ETR. During end-to-end packet exchange between two Internet hosts, a host sends a packet using only "inner header". IP addresses in "inner header" are EIDs. And an ITR prepends a new LISP header ("outer header") to each packet and an egress tunnel router strips the new header. The IP addresses in this "outer header" are RLOCs.

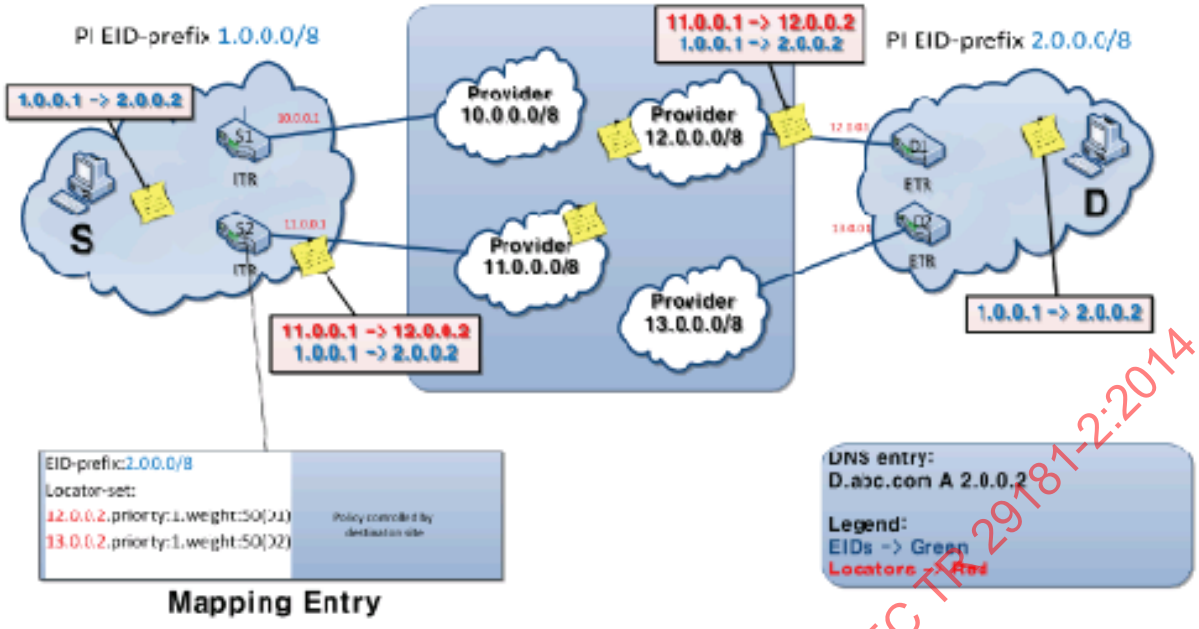

Figure B.2 — Information flow in LISP using EID and RLOC

An ITR is a router which accepts an IP packet with a single IP header (more precisely, an IP packet that does not contain a LISP header). The router treats this "inner" IP destination address as an EID and performs an EID-to-RLOC mapping lookup. The router then prepends an "outer" IP header with one of its globally-routable RLOCs in the source address field and the result of the mapping lookup in the destination address field.

An ETR is a router that accepts an IP packet where the destination address in the "outer" IP header is one of its own RLOCs. The router strips the "outer" header and forwards the packet based on the next IP header found.

B.3 Location based routing

Location based routing algorithms eliminate some of the limitations of topology based routing by using additional information. They use that location and node mobility information of the nodes for routing decision. Each node knows location through Global Positioning System (GPS)[25][26] or some location service.

Geographical routing protocols use location and node mobility information for the routing process. Location Aided Routing (LAR),[24] The Distance Routing Effect Algorithm for Mobility (DREAM)[27] and The Grid Location Service (GLS) use the information in different ways and provide different services.

LAR uses location information to reduce routing overhead of the ad-hoc network. Normally the LAR protocol uses the GPS to exploit node's location information. The mobile nodes knows there physical location through GPS. LAR assumes that every node knows every node's location information. LAR can be combining with a reactive routing protocol. Aims of LAR are effective route discovery and to restrict the flooding of route request packets. Each packet has location information of destination in the packet. On the contrary, DREAM can be combining with proactive routing protocol and every node maintains every node's location information. In DREAM, the location update frequency is decided by the distance between nodes and mobility characteristics of node. GLS is not a routing protocol, but it offers a location service. In GLS, each node in network has several location servers scattered throughout the network which provide location information.

Although the flooding is constrained in both LAR and DREAM by using location information, they are still not suitable for large-scale ad hoc networks. Their poor scalability roots in the directional flooding reactively initiated in LAR and proactive location information flooding in DREAM. On the contrary, GLS

can be used in large-scale mobile ad hoc networks with high node density. In GLS, a node chooses a small set of location severs throughout the network. LAR and DREAM exploit flooding for location update and query, but GLS doesn't exploit flooding for location update and query.

B.4 Connectivity between MANET and Internet

Aim of MANET routing protocols is maintain route within MANET.[10][12][28][29] MANET routing protocols do not utilize connection between node in MANET and node in Internet or infrastructure network. The purpose of MANET is to allow users to communicate reliably and cost effectively through various media, at any time, anyway, and anywhere. So, MANET demands consideration about the connectivity between MANET and Internet.

Global Connectivity for IPv4 Mobile Ad hoc Networks proposed a way to enable MANET to obtain Internet connectivity. It is integration between Mobile IPv4 and AODV,[11] such that a mobile node outside the FA transmission range can get a CoA and connect with the Internet through other hops in the MANET. It can roam to another MANET subnet without disconnection using Mobile IP.

And, Global Connectivity for IPv6 Mobile Ad Hoc Networks proposed a way to enable MANET nodes to communicate with the fixed Internet. The connection between the MANET nodes and the Internet is through nodes called Internet-gateways, which are connected to the Internet using a wired interface and connected to MANET using a wireless interface. It has proposed two methods to enable MANET nodes to find the Internet gateway and obtain the global prefix information, so that the MANET node can generate a global IPv6 address, which is used for sending/receiving packets from/to the Internet.

Annex C
(informative)

Current Internet Views

According to views, these are comparisons of such suggestions.

C.1 ID

In HMIPv6, ID is HoA (Home Address). HoA of node does not change when node is even moved to different network of IPv6 address. Therefore, HoA is global ID. HoA has home network prefix. The node which is moved to new network creates new CoA. This CoA is ID in local network. CoA has foreign network prefix. In end-to-end communication, each node uses HoA as ID. In MPLS,[23] ID in MPLS domain is IPv6 address or IPv4 address. In End-to-end communication, each node uses IP address as ID. In 6LoWPAN,[30] ID is interface identifier. Node of 6LoWPAN creates IPv6 address using network prefix information of router advertisement and interface identifier. In LISP, ID is EID (End-point ID). EID of node does not change when node is even moved to IPv4 address. In End-to-end communication, each node uses EID as ID. In Location based routing, ID does not change when node is moved to IP address. In end-to-end communication, each node uses IP address as ID. HMIPv6 and MPLS have ID in a certain network. In HMIPv6, 6LoWPAN, LISP and Location based routing; IP address is used as ID.

C.2 LOC (Locator)

CoA of node changes when node is moved to the different network of IPv6 address. CoA of moved node is used for routing between moved node and correspond node. In MPLS domain, LOC is MPLS label value among label switching routers. Label switching router decides next-hop from MPLS label value. MPLS label, which includes MPLS label value, is prepended in MPLS ingress node and removed in MPLS egress node. Therefore, MPLS label is used among MPLS switching routers. In LISP, LOC is Routing Locator (RLOC). RLOC changed to new RLOC when node is moved to IPv4 address or IPv6 address of ETR. Node doesn't notice its own RLOC. RLOC is used for the outer header between ITR and ETR. This outer header is prepended in ITR and removed in ETR. It is assumed that in location based routing, every node knows LOC information through GPS or location service. In HMIPv6, node notices LOC but In MPLS and LISP, node doesn't notice LOC. LOC is different information from IP address. In HMIPv6 and LISP, IP address is used as LOC. In HMIPv6, MPLS and LISP, tunnelling is used to use LOC.

C.3 Routing within local network

In HMIPv6, routing within local network is routing between MN and HA. Routing within local network is formed according to MN's HoA or MN's CoA. In other words, current IPv6 address routing within local network is formed. In MPLS, routing within local network is without MPLS domain. In Without MPLS domain, next-hop is decided according to IP. In 6LoWPAN, each node in network has routing same as MANET. In the node of network, routing within local network is capable using the routing table. In LISP, routing within local network is routing between node and ETR or ITR. Routing within local network is formed according to EID, which is IPv4 address or IPv6 address, in the inner header of packet. In the connection between MANET and Internet, routing within local network can be classified into proactive and reactive location based routing protocols. Proactive routing protocols maintain all nodes in MANET about one or more routing tables. They attempt to update the information of routing tables either periodically or by change in network topology information. Reactive routing protocols initiate a route discovery mechanism by the source node about destination node. Discovery start the source node has data packets to send to the destination node. Location based routing protocols use location and node mobility information for the routing process. HMIPv6, 6LoWPAN, LISP, In HMIPv6, 6LoWPAN,

LISP and MANET, IP address is used for routing. Location based routing protocols additionally use extra information of location.

C.4 Routing within backbone network

In HMIPv6 routing within backbone network is routing between CN and HA. In HMIPv6, routing within backbone network is the same as general IPv6 routing. In MPLS, routing within backbone network is MPLS domain. In MPLS domain, next-hop is decided according to MPLS label value. MPLS label that includes MPLS label value is prepended in MPLS ingress node and removed in MPLS egress node. In LISP, routing within backbone network is routing between ETR and ITR. Routing within backbone network is formed according to RLOC which is IPv4 address or IPv6 address in the outer head of packet. In the connection between MANET and Internet, routing within backbone network is the same as current IP routing. In HMIPv6, MPLS and LISP, routing within backbone network is used tunnelling for packet forwarding. HMIPv6, LISP and MANET use IP address to decide next-hop.

C.5 Mapping information

In HMIPv6, HA maintains MN's HoA and CoA mapping. At this time, HoA uses ID and CoA uses LOC. In MPLS, IP address becomes ID and MPLS label value becomes LOC. In MPLS ingress node, IP address and MPLS label value mapping are maintained to prepend MPLS label according to IP address. In 6LoWPAN, adaptation layer between IPv6 and IEEE 802.15.4 maintains mapping of both IPv6 address and interface identifier. Adaptation layer can restore IPv6 address compressed through the interface identifier of received packet and can compress IPv6 address of packet to be sent. In LISP, EID is used by ID and RLOC is used by LOC. At this moment, ITR prepend RLOC by seeing EID of packet to be sent to backbone and ETR respond to MAP request from backbone. Therefore, ITR maintains EID and RLOC mapping and ETR maintains local network prefix and RLOC mapping. In Location based routing, IP address is ID and location information is LOC. Each node maintain mapping of IP address and location information. In connection between MANET and Internet, gateway between MANET and Internet know list about nodes or network prefix of MANET. That's because the gateway decide whether received packet is node of MANET or not. The nodes of HMIPv6, 6LoWPAN and MANET maintain mapping information. On the other hand, In MPLS, LISP, node does not have to maintain mapping information.

C.6 Who use LOC?

HMIPv6 does tunnelling by using CoA between HA and MN when MN moves to the different network. At this time, CoA is used as address of tunnelling. This CoA represents LOC of MN. In MPLS, after MPLS label value is checked from label switching router, next-hop is decided. MPLS label value is used for between switching routers. In LISP, RLOC is used for outer header of packet between ITR and ETR. ITR prepends RLOC to outer header and sends the packet to backbone network. ETR removes RLOC and sends the packet to local network. Nodes don't know RLOC. In location based routing, all of nodes know location information of nodes in network. Also, all the nodes perform routing by using location information. In Connection between MANET and Internet, because gateway between MANET and Internet should know the location information about whether the destination of received packet is in MANET or in node, list about nodes or network prefix of MANET is used for routing.

C.7 Packets transmitting and receiving of node

In HMIPv6, a MN sends a packet to a CN includes the mobile node's HoA in the Home Address option. Source address of the packet is CoA of the MN and Destination address of the packet is address of the CN. A CN sends a packet to a MN. The IP header of the packet contains the HoA of mobile node in the destination address field, and the address of CN in the source address field. The home agent intercepts the packet and forward to the MN through tunnelling. The tunnelling header contains the CoA of mobile node in the destination address field, and the address of home agent in the source address field. In MPLS, a sending node sends a packet to receiving node. Source address of the packet is address of the sending node and destination address of the packet is address of the receiving node. MPLS ingress node receives the packet and prepends a MPLS label between layer 2 and layer 3. MPLS ingress node forwards the packet to MPLS

domain. MPLS egress node receives the labelled packet and removes the MPLS label. MPLS egress node forwards the packet to MPLS edge node. In 6LoWPAN, a sending node generates a packet that using IPv6. And adaptation layer compresses packet's IPv6 header to 6LoWPAN header. A receiving node receive the compressed packet that using 6LoWPAN. Then, adaptation layer decompress packet's 6LoWPAN header to IPv6 header. In LISP, a sending node generates a packet that using EID. Source address of the packet's inner header is EID of the sending node and destination address of the packet's inner header is EID of the receiving node. ITR receives the packet and prepends an outer header. Source address of the packet's outer head is address of ITR and destination address of the packet's outer header is address of ETR. Address of ETR is RLOC of receiving node. Next, ITR forwards the packet to LISP site. ETR receives the packet and removes the outer header. And, ITR forwards the packet to local network. . In HMIPv6, MPLS and LISP, tunnelling is used during transmission and receiving packet but in 6LoWPAN, IP header is compressed into 6LoWPAN header. In HMIPv6, MPLS and LISP, node does not know the address used for tunnelling. However, in 6LoWPAN, node can decompress the compressed header.

C.8 Functions of Nodes between local network and backbone network

In HMIPv6, there is home agent between local network and backbone network. The function of the home agent is tunnelling of packet which goes to MN through HoA of MN, CoA mapping management and itself. In MPLS, there are MPLS ingress node and MPLS egress node between local network and backbone network. . MPLS ingress node prepends MPLS label to packet from the outer MPLS domain and forwards to MPLS domain. MPLS egress node removes label from labelled packet and is forwarded to MPLS domain. In 6LoWPAN, there is a gateway between local network and backbone network. The gateway is to enable to communicate between 6LoWPAN and heterogeneous networks. In LISP, there are ITR and ETR between local network and backbone network. ITR prepends outer header to packet from the local network and is forwarded to LISP site. ITR queries RLOC from destination EID of received packet's inner header of received packet. ETR replies by MAP-reply about MAP-request of its own EID-prefix. ETR removes outer header received from LISP site and is forwarded to the local network. Gateway between MANET and Internet maintains list about nodes or network prefix of MANET and decides that it forwards to either MANET or Internet according to the list information. In HMIPv6, MPLS, LISP, the nodes maintains mapping table and performs encapsulation and decapsulation. In 6LoWPAN and MANET, the gateway enables to communicate between heterogeneous networks.

C.9 LOC management for node

In HMIPv6, node performs binding updates to inform home agent of its own movement whenever node moves. From the binding updates, node is able to receive the packet coming to itself through the home agent even though it moves. In IEEE 802.21, node offers network information of user terminal through media information service on the way to move. Then, node can decide handover through the information. In Location based routing, all nodes suppose location information of nodes in network. Therefore, LOC management isn't a matter to consider. In MANET and 6LoWPAN, IP of node includes LOC information. Therefore, when node moves, node updates information of neighbour nodes and broadcasts or replies its new information. HMIPv6 and IEEE 802.21 inform the changes whenever they move. LISP confirms LOC in regular intervals.

Annex D
(informative)

Packet Transferring using Geographical addressing scheme

This Annex is to show some examples how geographical address in end-system or routers can be used in LISP-like network topology and architecture, since LISP is already well known. It just shows the functional aspects of geographical addressing, not formal protocols and detailed procedures. Most definitions herein are extended version of definitions defined in LISP

D.1 Definitions

Geographical Addressing (GA): Geographical location-based addressing scheme, which adapts geographical location information to node. Node may denote routers, servers, or host.

Geographical address: Address which indicates a physical and geographical location of a node. It might be obtained using GPS or similar technologies. Geographical address can be represented by Absolute geographical address or Relative geographical address.

Absolute geographical address: Absolute geographical address is represented by latitude, longitude, altitude, and its range from the physically absolute position information.

Relative geographical address: Relative geographical address is represented by relative distance and range from reference point. Distance information is to represent relative location from the reference point. Range information is to represent as area with reference point as a centre.

Geographical Locator (GLOC): GLOC represents geographical location of a node in the network. It can be either Absolute GLOC or Relative GLOC, which are represented by absolute geographical address or relative geographical address, respectively.

Geographical ID (GID): GID represents geographical location of an end system. It can be represented by Absolute GID or Relative GID, which are represented by absolute geographical address or relative geographical address, respectively

End-node: An end-node is a device like an end-system defined in LISP. However end-node may have EID and GID, and perform GID-related functions like EID-GID mapping lookup, EID-GID management, etc.

Access-node: An access node is an access point which resides in the edge network with EID and GID. Access-node is locally identified, not globally identified. When EID blocks are assigned in a hierarchical manner in the edge network, access-node may be an anchor point for the sub-access network end-nodes. Access-node may have EID and GID, and perform GID-related functions like EID-GID mapping lookup, EID-GID management, etc. like end-node. And access-node will keep and manage the list of end-nodes in its own sub-access network. Note that if the access-node is mobile, the access-node will register its GID to its GITR or the another access-nodes which are connected each other.

GA-site: A set of routers in an edge network that are under a single technical administration. GA routers which reside in the GA edge network are the demarcation points to separate the edge network from the core network.

Geographical ETR (GETR): It is like an ETR which can accepts the packet with geographical address. When GETR receives GLOC-encapsulated IP packets from the internet, it decapsulates and once again re-encapsulates using EID-to-GID mapping lookup, if GID is available.

Geographical ITR (GITR): It is like an ITR that resides in GA-site. If the packet destination EID is to outside of the GA site, using EID-GLOC mapping lookup, GITR will encapsulate it with GLOC if available. If GLOC is not available, RLOC will be used. Routers in core network may equip with either GLOC or RLOC.

Geographical PETR (GPETR): It is a like PETR with geographical address capabilities.

Geographical PITR (GPITR): It is a like PITR with geographical address capabilities.

EID-to-GID database: The EID-to-GID database in a locally distributed database in a GA-site. It is updated and kept like a neighbour discovery manners in an edge network

EID-to-GLOC database: The EID-to-GLOC database is a global is global distributed database like EID-to-RLOC database in LISP.

GA-Site: A set of routers or routable hosts in an edge network with geographical addressing is applied.

D.2 Geographical address

Geographical address can be represented by Absolute geographical address or Relative geographical address, as shown in Figure D.1. Absolute geographical address is represented by latitude, longitude, altitude, and its range from the physically absolute position information. Relative geographical address is represented by relative distance and range from reference point. Distance information is to represent relative location from the reference point. Range information is to represent as area with reference point as a centre.

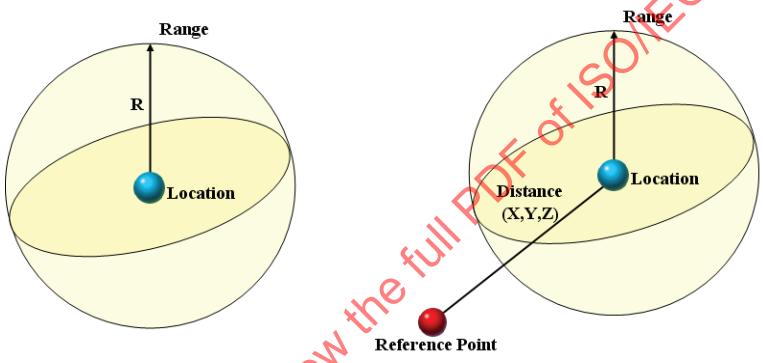

Figure D.1 — Locations represented by absolute address and relative address

The Geographical address which is given to a node with LOC or ID, is composed of code identifier, range information, distance information and location Information fields. That is, geographical address is able to describe specific location information and area centring the specific location information by using range information. Also, the address is able to describe relative location away as distance information from specific location.

Detail description of each field is as following.

— Code Identifier Field: Code Identifier field contains information which divides format and kinds of geographical address. That is, it divides whether LOC is represent by ASCII format, Binary format, or code format defined by user. Also, code identifier divides kinds of location information represented in location information field. The code represented by absolute location information becomes absolute location code while the code represented by LOC, alias, area/country code, so on, becomes relative location code. Composition of range and distance information can be different according to code identifier information. Therefore, first of all you should analyse code identifier field of LOC.

— Range Information Field: Range information represents an area centring the point represented in location information field. Range Information can be variously utilized as sensing range of node, area covering of node or error range, so on. It is composed of range, unit, and scale, so on. Unit indicates length such as Km, m, etc. only when range information is described. Range information field may not be used to according to option.

— Distance Information Field: Distance information field is used to represent relative location from the point include location information field. That is, final location is away as the distance information

from the reference point included location information field. Distance Information may be not used according to option. Generally distance information is not generally used since it is unnecessary information in absolute position code.

— Location Information Field: Location information field includes absolute location or reference point of relative location. And location information field should be hierarchical structure. Absolute location information is described by latitude, longitude, and altitude while reference point of relative location is described by using various formats such as the LOC, alias, or area/country code, so on.

The structure of LOC should consist hierarchical. Detail structure of LOC is as following.

Figure D.2 — Detailed LOC structure

D.3 Transferring packets in backbone network using GA

This section shows how packets from GETR are delivered to GITR using GLOC as shown in Figure D.3. It is only focus on the packet transferring in the core network.

Here it is assumed that both GITR and GETR keep and manage the list of end-nodes inside their own edge network. For more details in the edge network, refer to D.3.

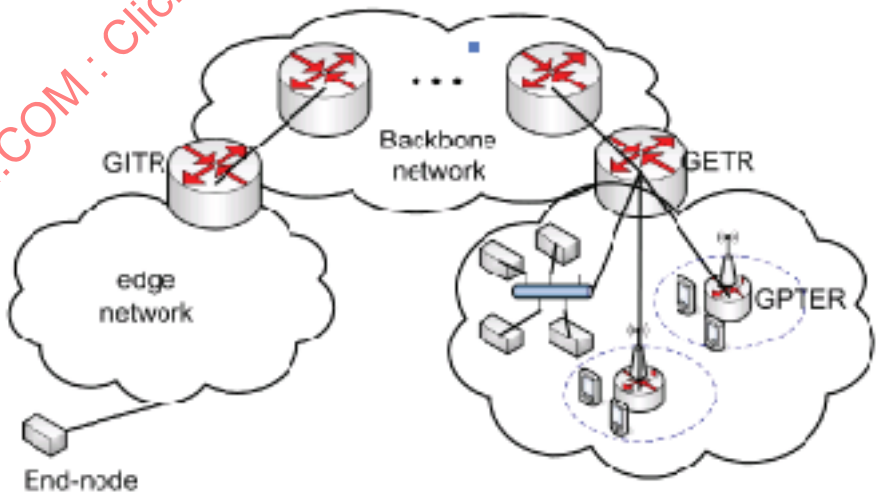

Figure D.3 — Core networks and edge networks with GETR, GITR, end-node

When GITR receives a packet from the inside of its own edge network, it performs the EID-to-GLOC mapping lookup for the destination EID, encapsulates with its own source GLOC and destination GLOC