Chapter 5
Routing Architecture of Next-Generation Internet (RANGI)

Xiaohu Xu
Huawei Technology, China

Meilian Lu
Beijing University of Posts and Telecom, China

ABSTRACT
This chapter describes a new Identifier/Locator split architecture, referred to as Routing Architecture for the Next Generation Internet (RANGI), which aims to deal with the routing scalability issues. Similar to the Host Identity Protocol (HIP) architecture, RANGI also introduces a host identifier (ID) layer between the IPv6 network layer and the transport layer and hence the transport-layer associations (e.g., TCP connections) are no longer bound to IP addresses, but to the host IDs. The major difference from the HIP architecture is that RANGI adopts hierarchical and cryptographic host IDs which have delegation-oriented structure. The corresponding ID to locator mapping system in RANGI is designed to preserve a “reasonable” business model and clear trust boundaries. In addition, RANGI uses special IPv4-embedded IPv6 addresses as locators and hence site-controllable traffic-engineering and simplified renumbering can be easily achieved while the deployment cost of such new architecture is reduced greatly.

INTRODUCTION
It has been widely recognized that the underlying reason for the so-called routing scalability issue (Meyer, Zhang, & Fall, 2007) is the overlapping semantics of IP address which is used as both locator and identifier in current Internet architecture. This overload of the IP address role makes it impossible to renumber the addresses in a topologically aggregate way in case of host or network site mobility or re-homing. An approach for solving the routing scalability issue is to separate the identifier role from the locator role of the IP address.

Host Identity Protocol (HIP) (Moskowitz & Nikander, 2006) is a well-known Identifier/Locator separation architecture which is developed by IETF (Internet Engineering Task Force) and IRTF...
(Internet Research Task Force). The major goal of HIP is to support host mobility, host multi-homing and enhance communication security. However, since HIP uses flat labels (i.e., hash values of the public keys) as host identifiers, there is no any hierarchy in the host identifier namespace and therefore it is impossible to introduce any hierarchy into the corresponding mapping system. As a result, it is impossible for multiple operators over the world to manage and operate such mapping resolution infrastructure in a cooperative way just as what they did in their 2G or 3G mobile communication systems.

This chapter describes a new ID/Locator split architecture, referred to as Routing Architecture for the Next Generation Internet (RANGI). Similar to the Host Identity Protocol (HIP) architecture, RANGI also introduces a host identifier (ID) layer between the IPv6 network layer and the transport layer and hence the transport-layer associations (e.g., TCP connections) are no longer bound to IP addresses, but to the host IDs. The major difference from the HIP architecture is that RANGI adopts hierarchical and cryptographic host IDs which have delegation-oriented structure. Therefore, the corresponding ID to locator mapping system in RANGI has a reasonable business model and clear trust boundaries. In addition, RANGI uses special IPv4-embeded IPv6 addresses as locators and hence site-controllable traffic-engineering and simplified renumbering can be easily achieved while the deployment cost of such new architecture is reduced greatly.

**SOLUTION DESCRIPTION**

The RANGI architecture is described in details in the following sub-sections.

**Host Identifiers**

In RANGI, host IDs are hierarchical and 128-bit long. As depicted in Figure 1, a host ID consists of two parts:

1. The leftmost n-64 bits part is the Administrative Domain Identifier (AD ID) which has embedded organizational affiliation and global uniqueness, and
2. The remaining part is the Local Host ID which is generated by computing a cryptographic one-way hash function from a public key of the ID owner and auxiliary parameters, e.g., the ID owner’s AD ID.

The binding between the public key and the host ID can be verified by re-computing the hash value and by comparing the hash with the host ID. As these identifiers are expected to be used along with IPv6 addresses at both applications and APIs (Application Programmable Interfaces), especially in the RANGI transition mechanisms defined in (Xu, 2009), it is desired to explicitly distinguish host IDs from IPv6 addresses (i.e., locators) and vice versa. Hence, a separate prefix for identifiers should be allocated by the IANA. As

---

**Figure 1. Host identifier structure**