Abstract. The necessity to split the endpoint identity and locator has been understood since sometime both from routing and security perspective. Today endpoints are identified by IP address that is location dependent and attributed by ISPs, whereas the identity neither depends on location nor on ISP. So splitting the routing and identification space is expected to make network operation such as mobility, multihoming and traffic engineering transparent for the end user. While in the operator side the use of a single space for routing and identification brings scaling issues. The operators will benefit from the split by decreased routing table size.

Within IETF/IRTF solutions are being developed to separate the IP layer into Endpoint Identifier (EID) space and routing locator (RLOC) space in the form of Locator/ID Separation Protocol (LISP). In LISP the Identifier (ID) has the format of a IPv4 or IPv6 address. This architecture provides ID to locator resolution so that the packets can be routed through the Internet.

This paper proposes a solution that considers an Endpoint Identifier (EID) as the combination of a domain name and a cryptographic Identifier (cryptoID). Such EIDs are hosted in a mixed DNS/Distributed Hash Table (DHT) architecture. Resolution involves a DNS and a DHT resolution. We show how the use of DNSSEC enhances the routing algorithm of the DHT resolution, and present advantages a such an architecture in term of deployment and future use of the Internet.

1 Introduction

Internet today uses IP addresses for both identifying a node and routing packets. With the requirements such as mobility, and multihoming, and advent of wireless Internet a node can have multiple IP addresses on different network interfaces, such as Wi-Fi or WiMAX, and it is likely that its IP address changes, or at least the Care of Address (CoA), while moving from one network to one network. Such change in IP address will lead to discontinuation of an on-going session. Thus it is necessary to consider endpoint to endpoint connection independent of the IP address. This leads to consideration of splitting the IP layer into two spaces: the Endpoint IDentifier space (EID), and the Routing LOCator space (RLOC).
Protocols like SHIM6 \[1\] or Host Identity Protocol (HIP) \[2\] are already considering the use of EIDs for mobility and multihoming purposes. SHIM6 is initiating a connection with a routing locator, in a traditional way. When the initiating locator is not anymore routable, then it is considered as an EID and is bound to other routable locators. HIP is considering a new naming space of EIDs with security properties. Host Identity Tag (HIT) are hash of a public key and so called cryptographic identifiers (CryptoID). CryptoID are very useful since they can be self generated and provide proof-of-ownership even on adhoc scenario. Nevertheless, to proceed to a HIP connection an EID-to-locator resolution is required, and no naming system really fits this resolution.

EID-to-locator resolution with EIDs as cryptoID is really what is missing in the current Internet architecture.

As opposed to DNS naming space that relies on a hieratical structure, cryptoIDs rely on a flat structure. A common way to deal with flat data is to use Distributed Hashed Table (DHT) data bases.

We chose in this paper to consider the chord \[3\] DHT structure because all data are distributed and ordered on a circle. We do not claim that chord is the only DHT database to be used. The chord data base enables to make the binding between HIT and data associated to this HIT.

Using a global DHT chord database for HITs implies consensus of all Internet authorities/actors to delegate the Naming function to a single entity. This is hardly believable, at least in the short term. Furthermore it would also imply the coexistence of two different and independent Naming architectures : DNS and DHT.

The hierarchical Naming structure of the DNS can be used to split the administrative part of the EID-to-locator resolution. On the other hand, using DNS means a single entry for Naming resolution.

Our paper is not presenting a proposition on how to use the DNS system over DHT. It describes a new identifier format and a naming solution that can use the traditional DNS architecture as an entry point. For that purpose we present an architecture that combines DNS and DHT. The naming resolution requires two different protocols DNS. In our example the DHT related protocol is chord. We point out how DNS can provides enough information to enable and enhance the chord resolution by using DNSSEC \([4, 5, 6]\). Although DNSSEC was originally designed for security purposes, in this paper DNSSEC properties are used to indicate to resolvers the chord node the naming request has to be sent to. We also show how this property is improving the chord routing algorithm. Our work did not intend to look on how to enhance DHT routing algorithm for naming service \([7, 8]\) nor to compare \([9]\) or migrate DNS to DHT databases.

On the other hand as pointed out by DNS over DHT works, the use of DHT fits by nature the new requirements of cryptoIDs. DHT offers to naming system scalability \([10]\), robustness to DDoS \([11]\) and also reduce the administrative burden for delete update operations \([11]\).

This paper provide system requirements in section \[2\] then positioned the paper with related works in section \[3\] The EID format is discussed in section \[4\]