An Unified Multiplex Communication Architecture for Simple Security Enhancements in IPv6 Communications

Hiroshi KITAMURA
NEC Corporation Tokyo, Japan
kitamura@da.jp.nec.com

Shingo ATA
Osaka City University Osaka, Japan
ata@info.eng.osaka-cu.ac.jp

Kazuyuki NISHIDA
Osaka University Osaka, Japan
k-nisida@ist.osaka-u.ac.jp

Masayuki MURATA
Osaka University Osaka, Japan
murata@ist.osaka-u.ac.jp

August 2, 2010   EuroView2010

Introduction

Current IP communication style is not optimized and has various problems. Sufficient security considerations (including privacy protection) are not provided.

e.g.
It is known that:
“well-known port” method is inappropriate from security standpoint.
However, we still use it….
It is conventionally believed that:
“one node owns one IP address” and
“communication sessions are multiplexed at the transport layer basically.”

We are moving to the IPv6 era:
it has become normal for one node to own multiple IP addresses.
It must be good time:
to reconsider the current communication style and
to establish a new communication architecture for security enhancements

Approaches to New Architecture

There are two types of approaches.

• Clean Slate type:
  − Redesign from scratch / Drastic change happens
  − Can NOT coexist with current
  − May require modifying existing applications
• Coexist with current and Migrate type:
  − Can coexist with current
  − Can use existing applications without modifying them

We choose Coexist with Current and Migrate type

Requirements to New Architecture

• Anyone can use it with ease.
  − be simple enough (not complex)
• Provide sufficient security consideration
  But
• NOT modify current communication Applications
  − Applications should be used as it is now.
• NOT change end-users’ using convenience

Analysis: Current IP sessions’ Multiplexing and Service Providing Methods

The following four types of information

1. Destination Port  2. Source Port  (Transport Layer)
3. Destination Address  4. Source Address  (Network Layer)

and protocol information (TCP or UDP) are used as a set for multiplexing and distinguishing IP sessions.

We call this “Legacy Multiplex” method

This method was invented in the IPv4 era:
when one node owned only one IP address.
The notion of a Port in the Transport layer was introduced to multiplex the communications sessions

Problems with Legacy Multiplex method

1. Sessions are distinguished by using multi-layered information
  • It is NOT inevitable to utilize multi-layered information to distinguish.
    (single-layered information may enough)
  • It is inefficient operations from function implementation viewpoint.
  • It is required for intermediate nodes to parse Transport layer info.
2. Service providing method using a “well-known port”
  • Port number information does NOT stand for essential service
  • No sufficient privacy considerations are provided
    • which services are provided by a server is found by any clients
3. Anycast / Multicast (non Unicast) Communication
  • Essence of the service is show via IP address information.
  • Port number information is less significant (almost ignored)
Proposal: **Unified Multiplex**
Communication Architecture as a Solution

**Legacy**
- Sessions' multiplex / distinguish operations is simplified: can be done only on the single Network Layer
- Necessary information for the operations is simplified: Destination and Source IP address information only

<table>
<thead>
<tr>
<th>1: Destination Address</th>
<th>2: Source Address</th>
<th>(Network Layer)</th>
</tr>
</thead>
</table>

**Unified**

If sessions are different, **used addresses** in the sessions are different.
Used Address becomes specific for each session.

- **Client Side:**
  - EA (Ephemeral Address)
- **Server Side:**
  - SSA (Specific Service Address)

Addresses are dynamically **Generated and Released** when their sessions are Started and Ended. Address valid time period is limited

**EA (Ephemeral Address)** at Client Side from layer structure viewpoint

**SSA (Specific Service Address)** at Server Side from layer structure viewpoint

Relationship between **Process** and **Address**

- **Legacy Environment**
  - Process is running
  - Socket / Session Valid Period (not limited)
  - Address Valid Period (not limited)

- **Unified Multiplex Environment**
  - Process is running
  - Socket / Session Valid Period
  - Address Valid Period (limited)
  - Address Pool function is introduced
Improvements in Address Usages, Service Providing Methods etc.

1 Node - 1 Fixed Address ⇒ 1 Node - Multi-Floating Address

<table>
<thead>
<tr>
<th>Number of Used Addresses</th>
<th>Information Dealing</th>
<th>Service (on Servers)</th>
<th>Information Fluidity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Only One Address (Basically)</td>
<td>General and Share Use Same Address</td>
<td>Wait for Anytime (24hour / 365days)</td>
<td>Fixed (Not Changed)</td>
</tr>
<tr>
<td>(Proposed) Unified</td>
<td>Specific and Dedicated Use Different Address</td>
<td>Wait for Only When Access Expected to Come</td>
<td>Floating (Changed and Updated)</td>
</tr>
</tbody>
</table>

Quantitative Analysis: “Meet Again” Probability for the same Address

Condition:
- Ephemeral Address Creation/Selection Rule is: “At Random” from 64bit Interface ID space.

Probability Formula (Birthday Paradox):
- “n” times probability:
  \[ P_n = 1 - \frac{(2^{64}-1) \cdot (2^{64}-2) \cdot \ldots \cdot (2^{64}-n)}{2^{64} \cdot \ldots \cdot 2^{64} \cdot \ldots \cdot 2^{64}} \]

Estimation: Number of consumed addresses per (year, day, hour, min, sec)

<table>
<thead>
<tr>
<th>/ year</th>
<th>/ day</th>
<th>/ hour</th>
<th>/ min</th>
<th>/ sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>31,536,000</td>
<td>86,400</td>
<td>3,600</td>
<td>60</td>
<td>1.0</td>
</tr>
<tr>
<td>1,000,000,000</td>
<td>273,814</td>
<td>11,411</td>
<td>100</td>
<td>3.3</td>
</tr>
</tbody>
</table>

“100M addr./year” is much enough (sufficient estimation)

Characteristics of Specific Addresses (EA and SSA) introduced in the Unified Multiplex

- Client side: **EA (Ephemeral Address)**
  - Any users can use Ephemeral Address easily
  - It is not necessary for users to be conscious the existence of Ephemeral Address function (like Ephemeral Port).
  - Very low threshold to deploy and use this
- Server side: **SSA (Specific Service Address)**
  - Completely newly invented functions and very unique
  - No analogical functions can be found in the Legacy method
  - Further researches are required to fully utilize this

Hereafter, SSA issues are discussed

IP Address Using Style:
- **Legacy Multiplex Environment**
- **Transient Environment until SSA**
Implementation and Verification Status

Unified Multiplex Communication Architecture functions have been implemented on the followings.

- FreeBSD 6.2R  FreeBSD 8.0R
- Linux kernel 2.6.24 (implemented functions are limited)

- Without modifications of communication Applications:
  - Only with the Kernel replacement:

It has verified that basic functions work correctly as they are designed.

Conclusion

We have proposed:

- an new communication architecture “Unified Multiplex”
- and new address types (EA and SSA).
  - This can coexist with current communication style.
  - Anyone can use this with ease.

It have been proved:

- this is an advanced communication architecture
  that can provide sufficient security consideration.
  - No fatal problems have not observed until now.
  - Veiled problems may be remained

We will continue refining the design and implementation and evaluating the architecture by utilizing its functions on various communication applications.