Architectural Design of Unified Multiplex Communications for One-Time Use of IP Addresses

Shingo Ata (Osaka City University)
Hiroshi Kitamura (NEC Corporation / Univ. of Electro-Communications)
Masayuki Murata (Osaka University)

1

Outline

- Research Background
  - What is One-time use IP addresses?
- Unified Multiplex Communication Architecture
  - Overview
  - Two address types (EA and SSA)
  - Technical requirements
- Things to Do to Realize Unified Multiplex ?
  - New Technologies for Unified Multiplex Communication
  - Analysis of Interoperability
- Implementation

2

Motivation

- Machine-to-Machine (Peer-to-Peer, personalized) communication will become more important for future Internet.

Problem

- Not easy to deploy servers due to security risks.

Why?

- IP address is fixed for a long time so that attacker can have much chance to try cracking.

How to solve?

- Introduce **one-time IP address** for single communication.
- Design Unified Multiplex Communication Architecture

3

What are IP addresses used for?

- Currently (from beginning), IP addresses are considered to identify ***Nodes***.
- Connections are identified by using **IP addresses + port numbers** (+ protocols).
- IP addresses are used (almost) *permanently* during the node is active.

4

Problems regarding Security

- Everyone agrees that…
  - Deployment of server w/ global IP address requires to consider many security risks.
  - High-level measures against security are needed.
    - Configuration of firewall, packet filters, loggings, incident reports…
    - Setting up VPN paths, authorization…
    - Careful and frequent maintenance is needed.
  - Is it really possible to all end users? **NO!**
- Are there really nothing that end users want to deploy servers? **NO!**
  - Control nodes remotely from outside.
  - Retrieve resources from outside.

Is there a way for all end users to deploy servers with easy??

5

Hiding the Existence of Servers from Others

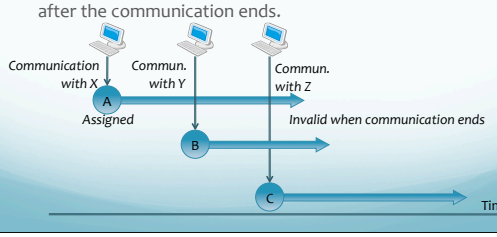
- In case of cell phone: That's easy!
  - Tell his/her phone number only to trusted people.
- WHY NOT to apply this principle to IP addresses??
  - Easy to make brute force attack in IPv4 address space.
  - Attack is much faster than phone calling.
  - Hard to regulate attack calls by administrators.
- However, IPv6 has a HUGE addressing space, i.e.,
  - Hard to brute force attack when IP address is unknown.
  - Shorten the lifetime of IP address as much as possible.
  - Changing IP address session-by-session.

NOT easy in IPv4, but possible in IPv6!!

6

One-time IP Addresses

- IP addresses are used to identify
  - NOT for nodes, BUT for sessions!
- Assigned just before the communication starts, disposed after the communication ends.



7

Security Advantages when using One-time Addresses

- IP address is ONLY valid for an associated session.
- Prevention against reverse tracking/attacking.
  - Though the IP address is known by someone, it is no longer used for any communication.
- Prevention against inference of node behavior.
  - Difficult to merge sessions having the same IP address
- Advanced authorization/authentication by using IP address only.
  - Embedding some magic numbers in IP address

Simple way to enhance security without any firewalls!!

8

Unified Multiplex Communication Architecture

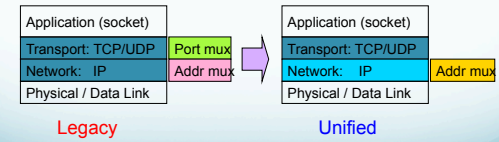
1 Node-1 Fixed Address ⇒ 1 Node - Multi-Floating Address

	(Current) Legacy ⇨	(Proposed) **Unified**
Number of Used Addresses	Use Only **One** Address (Basically)	Use **Multiple** Addresses
Information Dealing	General and **Share** Use **Same** Address	Specific and **Dedicated** Use **Different** Address
Service (on Servers)	Wait for **Anytime** (24hour / 365days)	Wait for **Only When** Access Expected to Come
Information Fluidity	**Fixed** (Not Changed)	**Floating** (**Changed** and **Updated**)

9

Unified Multiplex Communication Architecture

- 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



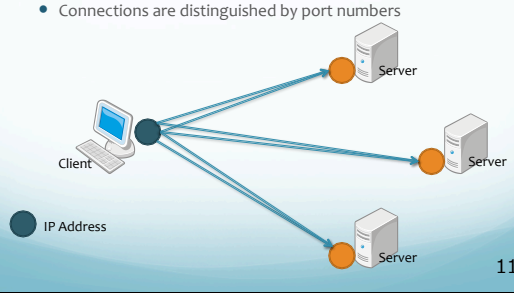
Legacy Unified

1: Destination Address 2: Source Address (Network Layer)

10

IP Addresses in Legacy Communication

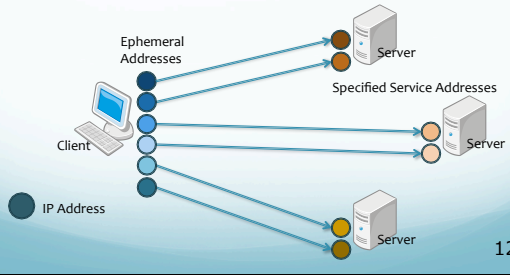
- Nodes have (typically) a single IP address
  - Connections are distinguished by port numbers



11

IP Addresses in Unified Multiplex Communication

- Nodes have multiple (many!) IP addresses
  - Different IP addresses are used for different connections



12

Two address types on Unified Multiplex

- **EA (Ephemeral Address)** for Clients
  - Like ephemeral ports in current TCP stack.
  - Unless specifying the port number explicitly, the client automatically use an available port number .
  - Before establishing connection, the client assigns a new IP address, which is not used for any other connections.
- **SSA (Specific Service Address)** for Servers
  - Only valid for a single session.
  - Before the communication, an SSA is generated for a client to communicate with the server and notified to the client.

13

Requirements for Unified Multiplex Communication

- Easy to deploy
  - Enable unified communication by updating OS software in end nodes only (no router replacements needed).
  - Support application without any updates (source modification, re-compiling).
- Co-existence with Legacy Communication nodes
  - Support gradual migration to Unified Multiplex Communication.

14

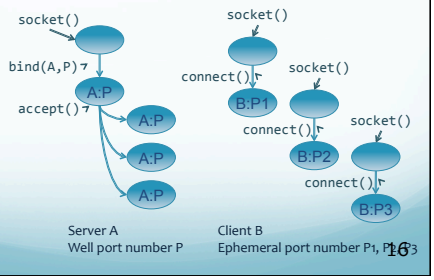
Comparisons of TCP communication between Unified and Legacy

- Setting up sockets
  - Timings of binding IP address to socket are completely different.
  - IP addresses for sockets are not determined at bind() call.
- Connection identification in kernel
  - Legacy: IP addresses, port numbers, protocol.
  - Unified: IP addresses ONLY.
- Address lifetime
  - Legacy: Used permanently.
  - Unified: Invalid after the connection ends.

15

Procedure for Establishing TCP Connection (Legacy)

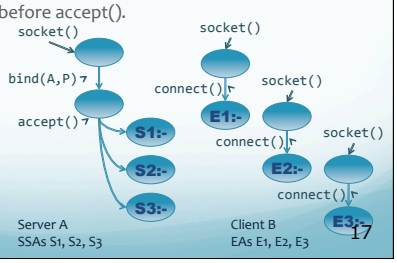
- Pre-determined address+port number are used for binding sockets.



16

Procedure for Establishing TCP Connection (Unified)

- Port number is abolished.
- Addresses for sockets are not determined at bind(), but assigned just before accept().



17

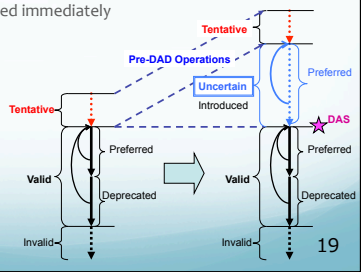
Functionalities needed for Unified Multiplex Communication

- Delayed address setting (DAS) at connection establishment
  - Set an IP address for the socket after bind() is called.
  - Introduce new (**Uncertain**) state of IP address.
  - Auto address setting for supporting applications without modification.
  - Address generation methods.
  - Introduce new TCP state for sockets without assigned IP address.
- Ignoring port numbers
  - Port number is no longer used for connection identification in PCB (Protocol Control Blocks) of kernel.
- Releasing addresses at the end of session

18

Uncertain State

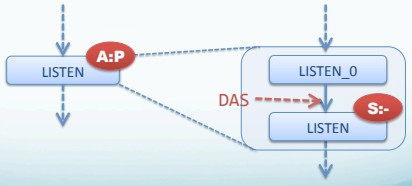
- New state to represent:
  - DAD (Duplicated Address Detection) is completed but the address is not used immediately



19

TCP State Transition

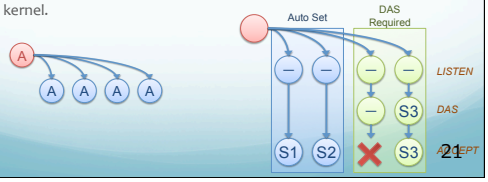
- New state (LISTEN_0) to represent:
  - Socket is listening, but no DAS'ed address is bound for accepting connection.



20

Auto Address Settings

- There is no procedure to assign EA/SSA in current applications.
  - Automatic assignment mechanism is needed for applications without any modifications.
- Two choices for address setting:
  - Automatic (Auto Set) : Suitable for most applications.
  - Manual (DAS Required) : Special address generation at outside of kernel.



21

Interoperability

- Four levels of treating port numbers for communication with Legacy nodes.

Port Ignore Mode Level 0
- Completely ignore port numbers in PCB.
- Port number fields in packet header are not used.

Port Ignore Mode Level 1
- Completely ignore port numbers in PCB.
- Set port number of source node for return packet.

Port Ignore Mode Level 2
- Use port numbers in PCB of client.
- Set port number of source node for return packet.

Port Aware Mode
- Same as Legacy node
- Set fixed (LEGACY_COMPAT) port number for compatibility

Pure Unified

Pure Legacy

22

Port Ignoring Level and Available Communication Styles

Mode Level	Use of port number for distinguishing sessions		Destination port number in packets	Available Communication Style Server(Addr, Port) – Client (Addr, Port)
	Server	Client		
Port ignore L0	No	No	Any	U(SSA, *) — U(EA, *)
Port ignore L1	No	No	Source port number of received packet	U(SSA, *) — U(EA, *) U(SSA, *) — L(LA, EP)
Port ignore L2	No	Yes	Source port number of received packet	U(SSA, *) — U(EA, *) U(*, *) — L(LA, EP)
Port aware	Yes	Yes	Source port number of received packet	U(*, WP) — L(LA, EP) U(*, RP) — L(LA, EP) U(*, WP) — L(LA, RP) U(*, RP) — L(LA, RP)

Node Address: U: Unified, L: Legacy; SSA: Service Specific Address, EA: Ephemeral Address, LA: Legacy Address
Port: EP: Ephemeral Port, RP: Reduced Port (LEGACY_COMPAT), WP: Well-known Port

23

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.

24

Conclusion

- One-time use of IP address is promising for reducing security risks of nodes easily and its benefit is applicable to all end users (non experts).
- Unified Multiplex Communication Architecture
  - Realizes one-time IP address communication style with ease.
  - Has interoperability with Legacy nodes.
- Design and implementation have done in FreeBSD and Linux (partially).
- Further refinement and validation of applications are needed for wide deployment.

25