セッション多重化技術の刷新により安心・安全な通信を実現する IPv6 Unified Multiplex 通信アーキテクチャの研究開発（08063984）

An IP Communication Style Innovation - Unified Multiplex Communication Architecture -

研究代表者
北村 浩　日本電気株式会社
Hiroshi KITAMURA　NEC Corporation

研究分担者
阿多 信吾†　村田 正幸††
Shingo ATA†　Masayuki MURATA††
†大阪市立大学 大学院工学研究科　††大阪大学 大学院情報科学研究科
†Osaka City University　††Osaka University

研究期間　平成 19 年度～平成 21 年度

概要
これまでエンドポイントの識別に広く用いられていた「IP アドレス+ポート番号」という通信アーキテクチャを根本的に見直し、IPv6 アドレスの広いアドレス空間を活用してポート番号の概念を廃した「Unified Multiplex 通信アーキテクチャ」の提唱とその実現モデル、および、それに基づいた実験システムの研究開発を行った。本課題によって得られる成果によって、従来のポート番号を用いることに起因する諸々の問題を抜本的に解決できるだけでなく、IPv6 のもつ広大なアドレススペース、アドレス自動設定機構などの機能的特徴を生かすことによって、より安心・安全な通信モデルに基づくネットワークサービスを提供することができるようになった。

Abstract
In this research, we have reviewed the fundamental role of communication architecture of IP networks to deprecate the concept of 'IP address + port number' which was used as a conventional method of identifying the end-point. We have newly designed and developed a new communication architecture called 'Unified Multiplex' that innovates in the current IP communication style. The node owns and consumes IP addresses that are used as communication sessions' identifiers. Sessions are multiplexed at network layer (not at transport layer). In the architecture, transport layer "Port" information have become less significant, and session multiplexing and identifying method becomes much simpler and securer than the current method.

１．まえがき
本研究によって得られる成果によって、従来のポート番号を用いることに起因する諸々の問題を抜本的に解決できるだけでなく、IPv6 のもつ広大なアドレススペース、アドレス自動設定機構などの機能的特徴を生かすことによって、より安心・安全な通信モデルに基づくネットワークサービスを提供することができる。以上の目的を達成するために主に 2. に述べる 5 つの課題について取り組んだ。

２．研究内容及び成果
2.1 Unified Multiplex 通信アーキテクチャの設計
Unified Multiplex 通信アーキテクチャ（Unified Multiplex）では、下記の 2 種類のアドレスを定義する。

1. Ephemeral Address (EA)[1]: 従来から存在するトランスポート層 ephemeral port と呼ばれる機能を、本研究で開発した新たな機能としてネットワーク層において実現したものである。EA は一般的なクライアントからサーバに対する接続におけるクライアント側の発信元アドレスとして使用することにより、クライアントの高い匿名性を提供できる。

2. Specific Service Address (SSA): 特定のサービスを提供するためだけに用意したアドレスで、ここで述べるサービスとは一般に想定するサービスより細かな粒度のもので、クライアントが変わったり、接続開始時期など変わったりしただけでも異なるサービスであり、それに対応するアドレスも流動性が高く頻繁に変化するものである(図 1)。サーバ側で特定のサービスを提供するために用いるアドレスである。SSA は従来にない、外部に対する匿名性を維持しつつグローバルな到達性を実現する新しいタイプのアドレスである。

本研究開発では、これらのアドレスに基づきサーバ、クライアントがどのように動作すべきであるかの詳細について検討し、Unified Multiplex の基本設計を行った。

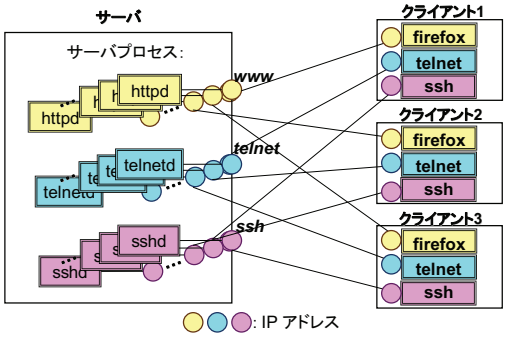

図 1 Unified Multiplex におけるアドレスの利用形態

Unified Multiplex では多数のアドレスを動的に生成し利用することになる。動的生成アドレスの利用では、従来の静的アドレス利用では顕在化していなかった、生成直後はアドレスが使用可能でなかったりアドレスの事前予約ができなかったりするなどの問題に直面する。既存実装に影響を及ぼすことなく、上記の問題を解決する方法として図 2 に示す新しいアドレス状態である Uncertain 状態[2]を導入することで解決する方法を創出し実装した。

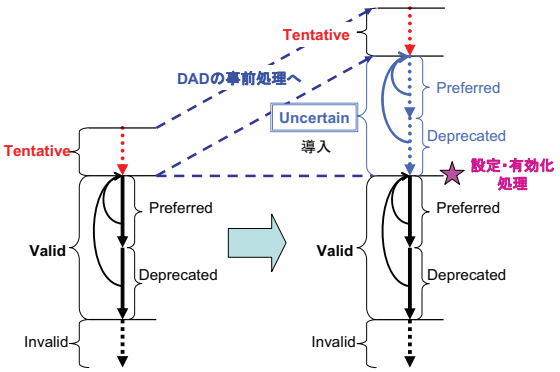

図 2 新しいアドレス状態 Uncertain State

2.2 エンドノードに対する修正点の把握

2.1 で決定された詳細設計にもとづき、ソフトウェアの試作(カーネルの機能強化)を行った。

- FreeBSD 6.2R/8.0R　全機能の実装、
- Linux kernel 2.6.24　EA を中心とした機能の一部

2.3 移行モデルの確立

Unified Multiplex と既存のアーキテクチャが混在した環境においても問題なく動作するための、互換性の検討を行い、動作検証によって、Unified Multiplex と既存のアーキテクチャが共存可能であることを確認した。

2.4 安全なアドレス解決メカニズムの確立

管理可能かつ匿名性を有する EA のアドレス生成を実現する機構の設計、実装を行った。

Unified Multiplex では、EA の生成ルールを適切に設定することで、外部から特定されにくい通信を実現することが可能である。しかしながら一方で、高い匿名性を有するアドレス生成は、同時にネットワーク管理者に対してより管理を困難にさせることとなる。このように、匿名性と追跡可能性はトレードオフの関係にあり、匿名性を高めるということは、同時に管理者に対しても隠匿性を高めることを意味し、ノードの追跡管理が困難になることになる。

本課題では、この相反する 2 つの要件を Unified Multiplex を使用して解決する方法を検討する。提案システムの概要を図 3 に示す。具体的には、ハッシュ関数の性質に着目し、同一ハッシュ値をもつ複数の IPv6 アドレスをグループ化する。そのグループ化されたアドレスを EA として順番に使用することで、第 3 者からはランダムに見える EA が、管理者側ではハッシュ関数を通すことで同一のハッシュ値をもつことを認識できる。このように、動的アドレス生成およびアドレスプール機構を用い、関連性を持つランダム生成アドレスを複数使用することで、インターネット上のノードからの匿名性と管理者による識別をともに実現する。

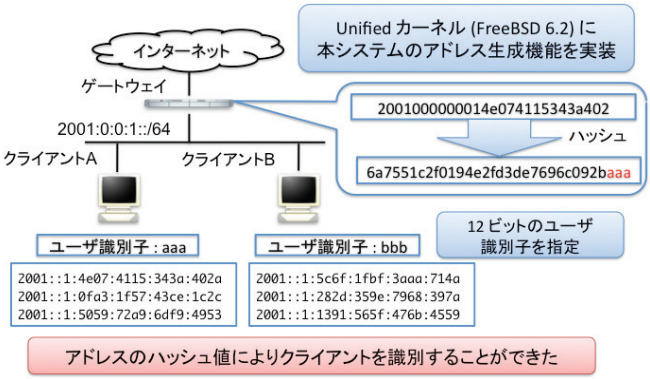

図 3 ハッシュを利用した匿名アドレス生成システム

2.5 実用化に向けた取り組みと動作検証

本課題では、大規模ネットワークにおける Unified Multiplex の動作検証、ならびにその結果をフィードバックしたプロトコルの改良として IPv6 におけるデータリンク層アドレスとネットワーク層アドレスの解決を行う Neighbor Discovery において、その情報保持を行う Neighbor Cache の更新および削除方法について新たに提案した[3]。

IPv6 では、通信相手のデータリンクアドレスとネットワークアドレスの関連を Neighbor Cache で行っている。Neighbor Cache の情報は初回通信時に生成され、以降の通信はキャッシュされた情報を用いる。しかし、現在の Neighbor Discovery では Neighbor Cache の生成については規定されているものの、キャッシュの管理、とくに削除および更新については実装依存とされている。Unified Multiplex は、セッションごとに独自アドレスを割り当て・解放することによって、アドレス寿命をセッション時間と対応させている。これにより、総当たりによるアタックやスキャンからノードを保護するなどの高い安全性を提供することができる。しかし、一方でアドレスの有効時間はセッションの確立時間と同じであることから、ノードごとに IP アドレスを割り当てる方法と比較して、短時間に大量の異なるアドレスが動的に生成、使用され、セッション終了後に未使用となるという状況が発生する。

本提案では、既存の機器に修正を加えることなく削除可能な手法と、Neighbor Discovery メッセージの拡張により確実な削除を実現する 2 つの手法を提案した。

3．むすび

Unified Multiplex 基本仕様の設計はほぼ完了しており、またその実装については、FreeBSD カーネルにおいて全機能を実装完了している。さらに Linux カーネルに対してはクライアントの機能である EA を中心に実装完了している。並行してアプリケーションの作成および既存アプリケーションの動作検証についても、主要アプリケーションの動作検証について確認し、Unified Multiplex 環境下でも正しく動作することを示した。

【国際標準提案リスト】

[1] IETF ,73rd meeting 6man WG, draft-kitamura-ipv6-ephemeral-address. “IPv6 Ephemeral Addresses,” Oct. 2008.
[2] IETF 73rd meeting 6man WG, draft-kitamura-ipv6-uncertain-address-state. “Harmless IPv6 Address State Extension (Uncertain State),” Oct. 2008.
[3] IETF 76th meeting 6man WG draft-kitamura-ipv6-neighbor-cache-update. “IPv6 Neighbor Cache Update,” Oct. 2009.

【誌上発表リスト】

[1] Keiichi SAKAKIMA, Shingo ATA, and Hiroshi KITAMURA, "Anonymous But Traceable IP Address-based Communication System," International Conference on Networks & Communications (NetCoM-2009), pp. 259.264, December 2009.

【本研究開発課題を掲載したホームページ】

http://unified-mutiplex.anarg.jp/
http://www.anarg.jp/achievements.html