

次世代インターネットプロトコル(IPv6)検証・評価システム

Verification and Evaluation Systems of the Next Generation Internet Protocol IPv6

岡部 宣夫^{*1} 星野 浩志^{*2}
 OKABE Nobuo HOSHINO Hiroshi
 田中 貴志^{*2} 星 哲夫^{*1}
 TANAKA Takashi HOSHI Tetsuo

次世代インターネットプロトコルIPv6(IP version 6)は、今後のインターネットの利用が益々重要になり拡大してゆくためには必須の技術である。しかしながら、IPv6の通信プロトコル仕様は複雑かつ膨大で、その仕様適合性の検証および評価は大きな問題となっている。本システムの開発ではIPv6の最新仕様を反映し、統合的な検証および評価を実現し、また257種類のテストを自動化することができた。この結果、検証および評価を大幅に効率化することが可能となり、開発に並行して実施した実証実験でもその効果を確認することができた。

The IPv6 (IP version 6) technology is the base technology for information network of next generation, providing the essential functions to business environments (in its large scale and reliability). In this project (TAHI), we have developed the comprehensive IPv6 verification and evaluation technologies to establish the software system of IPv6 that will be the base technology of the Internet. We also have examined and reviewed our development results by performing conformance and interoperability tests with networking products implementing IPv6.

1. はじめに

次世代のインターネット基盤は、今後も継続する接続機器の増加と、通信量の増加に柔軟に対応できなくてはならない。さらに、利用の多様化を背景としたデジタル通信の質およびサービス機能を実現し、信頼性のある産業・生活基盤としての役割の確立が急務である。IPv6 (IP version 6) 技術は、事業活動を支えることのできる次世代情報基盤として必要な機能(大規模性および信頼性)を提供することが可能な次世代情報ネットワークの基盤技術である。我々は、IPv6システムの普及を推進するために、情報処理振興事業協会の支援を受け、1998年にIPv6システムの検証・評価ソフトウェア体系を技術開発するプロジェクト(TAHI, <http://www.tahi.org/>)を発足させた。

2. 目的

本プロジェクトにおいては、IPv6の最新の技術および機能を、系統的・総合的に検証・評価するための検証・評価技術の技術開発、および実証実験を行うことを目的

とした。また、その技術開発成果を迅速にフリーで公開することにより、IPv6システムの研究開発を活発化することを狙いとした。また、検証ソフトウェアの技術開発に当たり、IPv6プロトコルスタック開発を実施するKAMEプロジェクト(<http://www.kame.net/>)と密接に協調し、本技術開発で得られた結果や問題点の解決策を、KAMEプロジェクトにフィードバックすることで、KAMEプロジェクトが開発するIPv6ソフトウェア体系を世界標準として完成させることにも寄与することとした。

3. 本検証・評価システムの特長と機能

本プロジェクトでは、さまざまなIPv6関連機能を統合化し、さらに最先端の技術および機能を継続的に取り込みながら、統合化した次世代インターネットプロトコル検証・評価システムを技術開発した。以下に、その特長と構成を記述する。

(1) 本検証・評価システムの特長

- IPv6の最新仕様を迅速に反映し、統合的な検証・評価を実施可能とした。
- 数多くのテスト項目を自動化し、効率的な検証・評価を実現可能とした。

*1 ITビジネス開発事業部 技術開発部

*2 テスト&メジャメント事業部 ComTest開発部

(2) 本検証・評価システムの機能

- ・仕様適合性検証機能
 検査対象がIPv6の仕様に適合しているか否かを、1対1の関係で検査システムが検証・評価する機能。
 (ネットワーク上に「行儀の悪い」プロトコルスタックが存在しても、その振る舞いに影響されない実装を検証・評価する堅牢性検証機能を含む)
- ・相互接続性検証機能
 検査対象が、実際のネットワークの中で、相互接続性を有するか否かを検証・評価する機能。(相互接続性に影響を与える性能測定を含む)
 本書では、仕様適合性検証機能に着目して、述べる。

4. 仕様適合性検証機能

(1) 概要

仕様適合性検査とは、あるシステムが特定の仕様を満たした実装を行っていることを厳密に検査することである。本プロジェクトではIPv6に関する仕様適合性の検査システムを開発した。本検査システムは、任意のIPv6パケットを任意のタイミングで送出し、検査対象の反応を観察し、分析し、記録して、検査対象の仕様適合性を判定する。

本検査システムは、下記仕様に関する仕様適合性を検査する。

- ・基本仕様 (RFC2460)
 - ・アドレス体系 (RFC2373)
 - ・ICMPv6 (RFC2463)
 - ・PathMTU探索 (RFC1981)
 - ・近隣探索 (RFC2461)
 - ・アドレス自動設定 (RFC2462)
 - ・IPv6/IPv4トンネル (draft-ietf-ngtrans-mech-04)
 - ・IPsec AH/ESP (RFC2401, RFC2402, RFC2403, RFC2404, RFC2405, RFC2406)
- 更に、本検査機能を利用することで、検査対象の堅牢性についても検査する。
- ・検査対象に不正パケットを送りつける。
 - ・検査対象の資源を消耗するようなネットワーク条件を作る。

(2) システムに対する要求事項

IPv6の仕様は多岐にわたるため、検査項目が多くなる。それらを効率良く検査するためには、人の手が介在せずに検査を実施する必要がある。そのため、次の要件を満たす必要がある。

- ・物理的な接続 (図1) は替えないで検査できること
 - ・多数の検査を自動的に実施できること
- また、仕様は、ホストとルータで実装に違いがあるが、その両方について検査できる必要がある。さらに、インターネット標準を記述するRFC (Request For

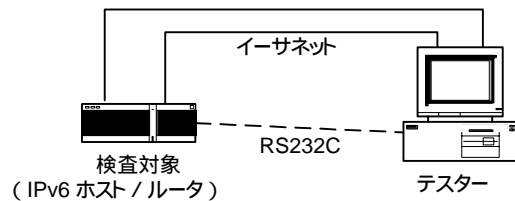


図1 検査システムの物理的接続

Comments)では、あらゆる実装の可能性を残すため、仕様の解釈に幅を持たせている。このため、仕様の解釈は実装により異なる可能性があり、検査アルゴリズムがこの状況に柔軟に対応できねばならない。そして、最終的に得られる検査結果を明確にするため、パス/フェイルで判定できる必要があり、フェイルとなった場合の問題点解析のため、全ての入出力パケットの記録を残す必要がある。

(3) システム仕様

検査対象とする物理層は、イーサネットとし、前述した要求を満たすため、検査システムの基本は以下とした。

- ・大量の検査を実行する必要があるため、全ての検査を自動的に実行する。
- ・検査を開始するにあたり、検査対象固有の初期化処理を行う必要がある。 (例えば、特定な経路表エントリの追加や削除など) 検査に対する副作用を避けるため、この制御はネットワークとは異なる媒体 (RS232C) を介して行う。
- ・任意の仮想的なネットワークを再現するため、MACアドレスやIPアドレスを含めて、任意のパケットを定義できる。
- ・ルータを検査するために、複数のイーサネット・インタフェースを検査対象にできる。
- ・検査対象の出すパケットを全て取り込む。
- ・定義したパケットを、任意のタイミングで送出できる。
- ・定義した複数のパケットを待ち条件として定義できる。
- ・待ち条件パケットに一致するパケットを取得できたか否かを判別できる。
- ・検査対象とする物理層はイーサネットなので、パケットの送出と受信時刻が500ミリ秒の分解能とする。
 パケット送信に関しては以下の仕様が必要となった。
- ・IPヘッダーが入れ子になったパケット送出できる。これにより、トンネル化したパケットや多重IPsecしたパケットなどの検査条件を再現できる。
- ・不正なパケット (例えば、CRC値、アライメント) を送出できる。これにより、不正なパケットなどの検査条件を再現できる。
 また、パケット受信に関しては以下の仕様が必要と

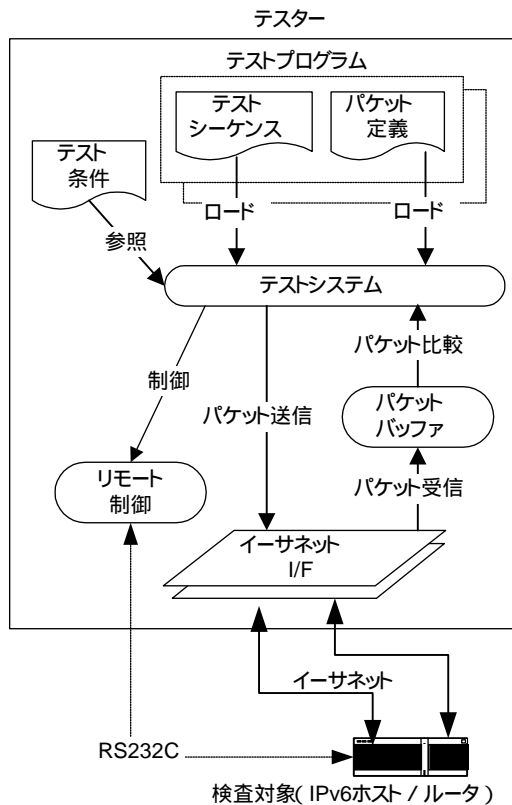


図2 検査システムの構成

なった。

- 検査対象が不定な状態の可能性に備え、複数の異なるパケットで待てる。
- IPv6の仕様では、ヘッダーオプション(IPv6 Extension Headers)やICMPオプション(Router Advertisement MessageのPrefix OptionやMTU OptionやSLLA Option)のフォーマットは規定されているが、その順序は実装依存となっている。同一の検査プログラムでこのような差異を吸収するため、メタなパケット定義を導入する。
- ONEOF(定義1, ..., 定義N): 受信したパケットが定義1~Nの内の一つが含まれていれば真とする。
- COMB(定義1, ..., 定義N): 定義1~Nが全て含まれていれば真。ただし、定義1~Nの順番は問わない。
- 仕様で規定されたアライメント(例えば、ヘッダーの32ビット境界)とパディングが実装されているか否かの比較判定ができる。
- トンネル化されたパケットや多重IPsec化されたパケットを判定する必要があるため、IPヘッダが入り子になったパケットを比較判定できる。
- パケット内部の詳細なフィールドでの差異を調べる必要がある。IPsecパケットの場合には、暗号化されたパケットを復号化し、比較判定する。

(4) システム構成

本検査システムのシステム構成は、以下とした(図2)。

- ・ テスター
本テストシステムは、PC互換機、FreeBSD2.Xまたは3.X)上で動作する。
- ・ テストシーケンス
Perlで記述した検査アルゴリズム。
- ・ パケット定義
独自言語で記述した送信/受信パケットの定義ファイル。
- ・ テスト条件
テスターや検査対象のMACアドレスなど、個々の検査環境毎にカスタマイズする必要のある定義ファイル。
- ・ テストシステム
パケットの送信、パケットの比較、リモート制御機能の制御など、テストの基本的な機能を司るプロセス。
- ・ パケットバッファ
イーサネット上を流れたパケットを記録するバッファ・プロセス。
- ・ リモート制御
検査対象固有の制御をアウトバウンド(RS232C経由)で行うプロセス。

(5) テストプログラム

IPv6の仕様適合性検査として、ホスト用とルータ用(表1)を作成した。両者とも、200テスト以上から成り、5時間以上の時間を要する。

個々のテストに関する特長等を以下にまとめる。

- ・ 基本仕様
例外条件が発生した場合の記述を十分に定義していないので、このような事象が発生した場合の判定を緩くせざるを得なかった。また、フローラベルやトラフィッククラスを実験的な使用段階と位置付けているので、この部分の判定条件も同様に緩く設定した。
- ・ アドレス体系
link-localスコープ以外のマルチキャストアドレスの検査は、マルチキャスト経路制御を考慮する必要がある。

表1 IPv6テストプログラム

分類	ホスト		ルータ	
	テスト数	テスト時間	テスト数	テスト時間
基本仕様	52	9分	61	11分
アドレス体系	7	4分	7	4分
ICMPv6	17	8分	22	9分
PathMTU探索	5	26分	4	24分
近隣探索	59	2時間43分	44	1時間43分
アドレス自動設定	58	1時間4分	30	1時間6分
IPv6/IPv4トンネル	6	5分	9	5分
IPsec AH/ESP	48	43分	50	47分
堅牢性	5	48分	5	48分
合計	257	6時間10分	232	5時間17分

る。現時点で、マルチキャスト経路制御は実験的要素が含まれるので、これらの検査の対象外とした。

・ ICMPv6

主に検査対象がエラーを検出した結果の振る舞いを定義している。従って、本仕様の適合性を検査するためには、本仕様以外をも考慮した検査アルゴリズムと検査データを用意する必要があった。

・ PathMTU探索

詳細な挙動を実装に委ねている部分が多い。検査の開始前に必要な、検査対象の初期化も実装に依存する。故に、検査はこれらの実装を考慮した結果となっている。

・ 近隣探索

近隣探索の状態遷移が複雑なので、テスト数が多くなった。特に、Neighbor Advertisement Messageはフラグ等の条件が複雑なので、これに関する状態遷移の検査時間は、テスト数が5つにもかわらず、テスト実行時間が1時間もかかる。近隣キャッシュ状態が正しく遷移したことを調べることで、その状態を遷移させてしまうので、検査データとアルゴリズムに工夫を要した。

・ アドレス自動設定

システム立ち上げ時のlink-localアドレスに関するアドレス重複の検査は難しかった。これは、link-localアドレスの割り当てられるタイミングが、検査対象の実装や設定に大きく依存しているためであった。

・ IPv6/IPv4トンネル

トンネルにおけるフラグメントに関しては、本仕様の他に、IPv6実装者らで合意されたデファクト仕様が存在する。このため、本検査では両方に対応した。

・ IPsec AH/ESP

IPsecの検査数は、IPsecの設定条件(すなわちSecurity Associationの組み合わせの数)に比例する。この組み

合わせの数は大きい。組み合わせの対象となる項目が10~20)ので、代表的な例と思われる条件に絞り、検査時間を現実的な長さに抑える必要があった。例えば、ホストとルータに対してそれぞれ、主に使われるであろうモードのテストを作成した。(ホストにはトランスポートモードのみ、ルータにはトンネルモードのみ)また、オンリンクでのIPsec通信は、近隣探索と複雑に絡み、IETF(Internet Engineering Task Force)でも議論が続けられているため、オフリンクのSAのみとした。

・ 堅牢性

この検査は、多くの条件を組み合わせる必要があるため、テスト数も限りがない。その中から効率良いテストを選択するには、検査対象の実装を想像する必要があった。

5. おわりに

今後、インターネットに接続される機器は、携帯端末、情報家電、自動車、センサー等多岐にわたり、それぞれがグローバルなアドレスを持ってエンド・ツー・エンドで通信をする時代も間近に迫っている。また、電子商取引等のセキュアな通信や、大容量のマルチメディア・コンテンツの配信等がインターネットを利用して計画されている。これらの実現のために、IPv6の普及が期待されており、IPv6を応用する製品の品質と、相互運用性を確保するために、本検証・評価システムがいくらかでも貢献できればと望んでいる。

なお、本開発は、情報処理振興事業協会(IPA)の平成10年度次世代デジタル応用基盤技術開発事業に公募・採択されたものである。

* 本文中のシステム名及び製品名は、各社の商標或いは登録商標です。

IPv6(Internet Protocol Version 6)とは

現在インターネットで普及しているプロトコルIPv4(Internet Protocol Version 4)の問題点の解決と、最新のネットワーク技術の適用を目指した、次世代インターネット・プロトコルである。IPv4のアドレス空間は、32ビット(約40億アドレス)で、これは地球上の人口より小さく、既に世界的にアドレスは枯渇している。

この問題を解決するために、プライベートアドレスとNAT(Network Address Translation)を組み合わせた技術が普及した。しかし、これらの技術では、インターネット本来のメリットであるエンド・ツー・エンド通信が不可能になるため、インターネットの技術的発展および商業的発展の阻害が指摘されている。

次世代インターネットプロトコルの特徴は以下である。

- ・ 128ビットのアドレス空間(40億×40億×40億×40億アドレス)による、アドレス枯渇の解消とエンド・ツー・エンド通信の復活

- ・ パケットの暗号化(ESP: Encapsulated security payload)、および認証(AH: Authentication Header)によるセキュリティ機能の実現

- ・ アドレス自動設定によるプラグ&プレイの実現
- ・ フローラベルによる優先度付通信の実現 等

1996年以降、実証実験のための「6 bone(IPv6バックボーン)」と呼ばれる世界規模のネットワークが構築され、移行するためのあらゆるテストが行われている。日本では同年6月よりWIDEプロジェクトによりWIDE 6 boneが構築され、検証が進められている。このなかで検証を担当しているのがTAHIプロジェクトである。

既に、マイクロソフト社やシスコシステムズ社を初めとして、多くの世界的OSベンダやネットワーク機器ベンダが、製品としてIPv6のサポートを開始し、本格的な普及が期待されている(<http://www.ipv6.org/>を参照)。また国内ではOCNなどが実験的に、IIJが商用のIPv6接続サービスを開始した。