IPv6対応ネットワーク評価ツールの設計

4U－4　屏　雄一郎　藤長　昌彦　伊藤　嘉浩　石倉　雅巳　浅見　徹
株式会社　KDD研究所

1. はじめに

次世代インターネットプロトコルとして数年前に開発が始まったIPv6[1]は，現在FreeBSDなど各種OSへの実装[2]やIPv6実験網の構築[3]が進んでおり，これを利用できる環境が徐々に整いつつある．このため，近い将来IPv6ネットワークの性能や信頼性等を評価する必要性が高まってくると考えられる．筆者らは既にIPv4用ネットワーク評価ツールKITS(KDD Internet Test System)[4]を開発しているが，それをIPv6対応とすることにより，IPv6ネットワークにおいてもKITSの機能を利用したネットワーク評価を行うことができる．しかしIPv6特有の機能に関して評価を行うためには，現在のKITSの機能を拡張する必要がある．

本稿ではIPv6に特有な機能の評価について考察し，KITSをベースに，IPv6特有の機能の評価が可能なネットワーク評価ツールを設計した結果について述べる．

2. KITS概要

筆者らが開発したKITSは以下のような特徴を有しており，netperfやttcp等既存のIPv4ネットワーク評価ツールよりも柔軟なネットワーク評価を可能としている．

- 送信側，受信側双方で起動（送信側トラヒック送信，受信側解析）
- 任意のパケット長、パケット間隔でTCPやUDPの疑似トラヒックを生成可能
- 任意のトラヒック生成関数を定義可能
- パケット損失率や遅延時間等の統計情報の測定，表示
- マルチキャスト対応（UDP）

またKITSはC言語で記述され，UNIX socketインタフェースの上に実装されているため，BSD用のIPv6パッケージであるKAME[5]等を用いれば，容易にIPv6対応とすることが可能である．

A Design of the IPv6 Network Evaluation Tool
Yuichiro Hei, Masahiko Fujinaga Yoshihiro Ito, Masami Ishikura and Tohru Asami
KDD R&D Laboratories
hei@kddlabs.co.jp

3. IPv6概要

IPv6におけるアドレス長は，IPv4における32ビットから128ビットに拡張された．またIPv6の基本ヘッダは，IPv4のそれと比較して簡略化されたものになっており，ヘッダチェックサム等は削除され，ストリーム通信のサポート等を目的として新たにトラヒッククラス，フローラベルフィールドが導入されている．

アドレス体系に関しては，IPv4におけるユニキャスト，マルチキャストに加えて，エニーキャストアドレスが新たに導入されている[6][7]．エニーキャストアドレスはマルチキャストアドレスと同様，ホストのグループを識別するが、エニーキャストアドレス宛てに送出されたパケットは，そのグループに属するすべてのホストではなく，グループ内のいずれか一つのホストに配送される．

4. 設計方針

4.1 IPv4とIPv6の指定

IPv4アプリケーションをIPv6対応とする際，IPv4とIPv6のどちらのプロトコルを使用するかについて考える必要がある．その指定法として以下のものが考えられる．

- IPv4用とIPv6用の二つの実行ファイルを作成する
- アプリケーション実行時に，オプションでIPv4,IPv6の指定を行う
- アドレス（プロトコル）非依存な実行ファイルを作成する

通常のアプリケーションでは，ユーザがIPv4かIPv6かを意識する必要がないという点で，アドレス非依存な実装を行うのが望ましいが，ネットワーク評価ツールとしては，明示的にIPv6を指定する機能が必要であるため，実行時にオプションでIPv4，IPv6の指定を行うこととした．

4.2 トラヒッククラスとフローラベル

IPv6基本ヘッダには，QoS(Quality of Service)保証を効率的に行うために，8ビットのトラヒッククラスフィールドと20ビットのフローラベルフィ

ールドが導入されている．現在この二つのフィールドの具体的な使用法は定まっておらず，これらのフィールドに対応したネットワーク機器も存在していない．しかし今後これらのフィールドをサポートする機器が出てくることは十分考えられるので，IPv6ネットワーク評価ツールではこれらのフィールド値を適切に設定できる機能が必要となる．

またトラヒッククラスフィールドは途中のノードで変更される可能性があるため[1]，受信ホストでフィールド変更の有無が検出可能であることが望ましい．そこでオリジナルの値を送出パケットのデータ部に格納しておき，受信ホストでの値の変更の検出を可能とした．ただしこの手法では，中継ノードが二つ以上の場合，どのノードで値が変更されたかを検出することはできない．

4.3　エニーキャストへの対応

現在エニーキャストを利用したアプリケーションは提案されていないが，IPv6ネットワーク評価ツールにおいては，エニーキャスト通信の評価，あるいはアプリケーション開発のためのツールとして対応しておく必要がある．

エニーキャストアドレスのアドレス空間はユニキャストと同じものを用いるため[6]，送信ホストは宛先アドレスだけでは，それがエニーキャストなのかユニキャストなのかを判断することはできない．しかしネットワーク評価を行う場合には，どちらの評価を行うかをあらかじめ決めていると仮定できるので，エニーキャストとユニキャストの区別は起動時のオプションで指定できるようにすればよい．

またエニーキャストアドレス宛てにパケットを送出した場合，そのパケットをどのホストが受信するかは動的に変更される可能性がある．従ってIPv6ネットワーク評価ツールにおいて，どのホストがエニーキャストパケットを受信したかを調査できるようにする必要がある．

図1はエニーキャスト通信における受信ホスト調査の処理の流れを示している．まず送信ホスト、受信ホストにおいて，エニーキャストオプションを指定してKITSを起動する．次に送信ホストが宛先アドレスをエニーキャストアドレスAとしてUDPパケットを送出する．仮に受信ホスト1がそのパケットを受信したとすると，そのホストは送信ホストに向けて，送信元，宛先アドレスをそれぞれR1，Sとした応答パケット（UDP）を送出する．これによりエニーキャストアドレスA宛てに送出したパケットが到達したホストを知ることができる．

またあるエニーキャストアドレス宛てに連続してパケットを送出した場合，障害や経路情報の変化，あるいは負荷分散の目的等により，通信途中で受信ホストが変更になる可能性があるが，上述の処理を連続して行うことにより，受信ホストが変更になる契機などを調査することができる．

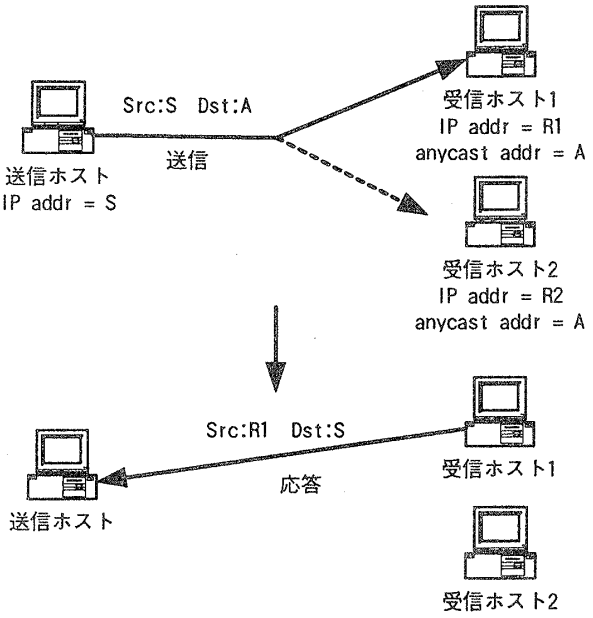

図1：エニーキャスト通信での受信ホストの調査

5.　まとめ

本稿では，IPv6ネットワークの評価において必要となる機能に関して検討し，評価ツールの設計について述べた．今後実装を行い，実験室環境における評価試験を行う予定である．

参考文献

[1] S.Deering and R.Hinden, "Internet Protocol,Version 6 (IPv6) Specification", RFC2460, Dec. 1998
[2] http://playground.sun.com/pub/ipng/html/ipng-implementations.html
[3] http://www.6bone.net
[4] 伊藤他，"リアルタイム通信特性評価用トラヒックジェネレータ／アナライザの評価"，信学技報IN97-47，June 1997
[5] http://www.kame.net
[6] R.Hinden and S.Deering, "IP Version 6 Addressing Architecture", RFC2373, July 1998
[7] C.Partridge, T.Mendez and W.Milliken, "Host Anycasting Service", RFC1546, Nov. 1993