

IPv6時代におけるネットワーク状態評価手法の提案

北口 善明^{1,a)} 石原 知洋² 高嶋 健人³

概要: ネットワーク運用において、ユーザからの障害報告として「つながらない」というものがある。「つながらない」状況の問題点を突き止める場合には、ユーザ側からのネットワーク観測が有効であるが、ユーザからは得てして「つながらない」という漠然とした状況しか得られないものである。そこで、ネットワーク障害点を的確に検出するために、ユーザ側からの観測を元に状態を評価し、ネットワーク運用者が迅速に問題点を把握できる手法を提案する。本手法では、ネットワーク障害を複数のレイヤに整理し、「ネットワーク接続性記述の定義」を明確にすることで、的確にユーザ環境の情報伝達を可能にする。本稿では、「ネットワーク接続性記述の定義」に向けた計測レイヤ定義を示し、プロトタイプによる実装と評価について報告する。

キーワード: ネットワーク状態評価, ネットワーク運用, 無線 LAN, 可視化

Proposal of evaluation method for network condition in the era of IPv6

YOSHIAKI KITAGUCHI^{1,a)} TOMOHIRO ISHIHARA² TAKETO TAKASHIMA³

Abstract: In a network-troubleshooting situation, an end user tend to tell highly unclear reports like as 'just can not connect'. In most cases, it's hard to measure from a client side to clarify the detail of the network trouble. We proposed a mechanism for measuring network condition from client-side and gathering results to grasp the detail of the network trouble. We classify elements of a network trouble by layer, and thereby define a description of network connectivity. Our proposed description enables accurate information exchange between a network operator and end users. In this paper, we describe the definition of measurement layer. We also report prototype implementation and its evaluation.

Keywords: Network Condition Assessment, Network Operation, Wireless LAN, Visualization

1. はじめに

キャンパスネットワークやイベントネットワークの運用において無線アクセスネットワークを提供する場合、ユーザから「つながらない」とのクレームを受ける時がある。「つながらない」という現象の原因としては、提供されるネットワークにおける物理的な障害の他に、エンドユーザの端末に付与されるアドレスの問題やDNSにおける名前解決の不具合など、様々な要因が考えられる。このような

「つながらない」状況の問題点を突き止める場合には、ユーザ側からのネットワーク観測が有効であるが、ユーザからは得てして「つながらない」という漠然とした状況しか得られないものである。

一方、ネットワークの運用者側からの対応としては、ネットワークや提供サービスの状態を監視する手法は多く存在しており、Nagios^{*1}などのオープンソースアプリケーションが一般的に利用されている。ただし、これらの手法では、サーバの挙動やIP的な到達性の確認が主となるため、ユーザが被っている障害の状態やサービス障害点を確認することが困難であった。

さらに、今後利用が加速すると予想されるIPv6を利用

¹ 金沢大学 総合メディア基盤センター
Kakuma-machi, Kanazawa, Ishikawa 920-1192, Japan

² 東京大学大学院 総合文化研究科

³ フリーランス

a) kitaguchi@imc.kanazawa-u.ac.jp

*1 <http://www.nagios.org/>

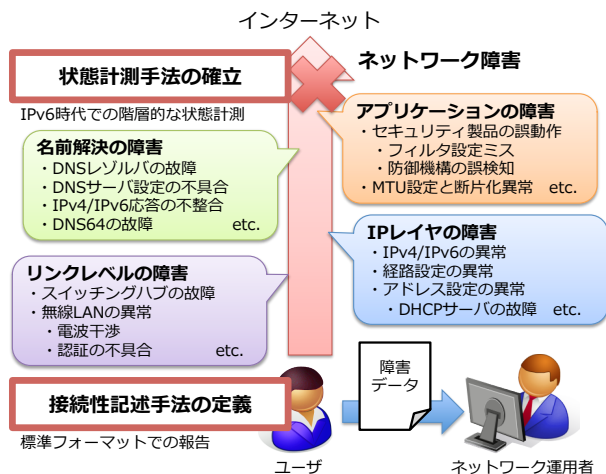


図 1 ユーザ視点によるネットワーク状態計測手法のイメージ

Fig. 1 Overview of the evaluation method for network condition from user segment

したデュアルスタックネットワークでは、IPv4 と IPv6 それぞれの挙動を把握する必要があり、問題発生時の障害点の把握が一層難しくなることが予想されている。特に、クライアント OS 上においてドメイン名と IP アドレスの変換を行う DNS レゾルバの実装に関してはクライアント OS 毎に異なる場合があることが示されている [1]。これらの課題を受け、我々は、ユーザが利用している実環境からの状態観測情報をネットワーク運用者に的確に伝える手法の確立が必要と考えるに至った。

ユーザ環境のネットワーク問題を評価する仕組みとして、Aggarwal 氏らによるホームネットワークの設定ミスを判定する研究がある [2]。ユーザ側からの計測により、ネットワークにおける問題を推測する観点は同様であるが、IPv6 に関する考察は行われておらず、ネットワーク接続性記述手法に関する言及はない。著者らは、IPv4/IPv6 デュアルスタック環境におけるネットワーク評価の複雑さを解決するために、ユーザ側に設置したセンサーノードを活用した評価実験を実施し、継続的な計測の有用性を示すことができた [3]。特に対象としたネットワークが IPv6 のみのネットワークであるなど、これから利用が進むと想定される運用形態における評価手法に関して整理することができ、ユーザ側からの評価手法の有用性を確認している。

このように、ネットワークシステムの運用上における課題を解決するために、我々はエンドユーザが利用している実環境からの状態観測情報をネットワーク運用者に的確に伝える手法の確立が必要と考えている。図 1 に提案するネットワーク状態計測手法の概要を示す。本稿では、ネットワーク運用者が迅速に問題点を把握できる手法の確立を目的とした、ユーザ視点におけるネットワーク状態の観測手法を提案する。

2. IPv6 時代のネットワーク運用モデル

本研究では、特に今後利用が増すと考えられる IPv4/IPv6 デュアルスタック環境を評価対象とし、複雑なネットワークにおいても十分利用可能なものを目指している。そこで、IPv6 時代のネットワーク運用モデルを先に整理し、これまでに指摘されている障害例をまとめる。

2.1 IPv6 移行技術と課題

IPv6 は従来の IPv4 との相互通信を直接行う互換性をもっておらず、IPv4 とは独立したネットワークを構築する必要がある。IPv6 の仕様が策定された当初から、IPv4 主流の環境下での展開手法が提示されており、以下の三種に大別できる。

- デュアルスタック
- トンネリング
- トランスレータ

デュアルスタックは、IPv6 のプロトコルスタックを現状の IPv4 機器に追加し、IPv4 と IPv6 双方の通信を可能にする形態である。現在は IPv4 での通信が主流であるため、機器の IPv6 対応とはデュアルスタック機能を有することと等しく、多くのネットワーク機器はデュアルスタック可能となっている。デュアルスタック運用における問題点としては、ネットワーク障害が発生した際の問題切り分けが複雑になることが挙げられる [4]。また、ネットワーク運用に際しても双方のプロトコル監視が求められ、運用コストやセキュリティリスクの増加も課題となる。そのため、IPv4 と IPv6 を完全に分離して構築するパラレルスタックモデルも提示されており、安定性・セキュリティ性が重要な部分への導入が想定されている [5]。

トンネリングは、IPv4 インターネット上に仮想的な IPv6 ネットワークを構築するために用いられ、ネットワークが IPv6 対応していない環境で多く利用される形態である。IPv6 が利用開始された初期段階において多く利用された形態で、ネットワーク間を接続するものから、クライアントサーバモデルまで数多くの手法が存在する。代表的な自動トンネリング技術として挙げられる 6to4 [6] は、ネットワークのデュアルスタック化が進んでいない環境で多く利用される技術であり、Windows 端末 (Windows Vista 以降) では初期状態において 6to4 接続を積極的に実施する設定となっている。トンネリング運用における影響として、搬送するプロトコルにカプセル化して通信するため、通信パケットの MTU が小さくなることから通信のオーバーヘッドが大きくなる点が挙げられる。また、搬送するプロトコルの障害により、トンネリング内部のプロトコルにも影響が出るため、サービス品質を保つことが難しくなる。

トランスレータは、IPv4 ネットワークと IPv6 ネット

ワーク間の直接通信を実現する装置を指し、その装置により中継されるネットワーク形態を提供する。主なトランスレータの実装方式には、Proxy 方式と TRT (Transport Relay Translator) 方式および NAT64 方式の三種類がある。トランスレータを用いることで、サーバシステムの IPv6 対応を行わずに IPv6 のサービス提供を行うことや、IPv6 のシングルスタック運用下における IPv4 サービス利用などが可能となる。どちらも、ネットワーク運用をシングルスタックにすることで、デュアルスタックにおける問題切り分けをシンプルにすることができる利点がある。ただし、トランスレータは IPv4 の NAT と同様に、通信方向の制限や通信の接続状態を保持・管理する制御が必要になるため、運用コストの増大や障害の原因となっている通信の特定が困難になるとの指摘もある [5]。

2.2 IPv6 対応ネットワークにおける障害例

前節で述べたように、ネットワークを IPv6 対応するためには多くの方式が存在しているが、ほとんどの場合、ユーザ側のネットワークはデュアルスタックになるケースが多い。その場合に発生する代表的な障害例を参考文献 [4] より引用し、提案手法にて解析する手段を考察する。

(1) IPv6 から IPv4 へのフォールバックに関する課題

デュアルスタック実装の多くは IPv6 通信を優先し、IPv6 通信に問題がある場合に IPv4 に切り替えて通信するフォールバック処理を有している。この処理が実装によっては機能しない、もしくはフォールバックに時間がかかるなどの問題が発生する可能性がある。問題の根幹は、OS の実装に依存する部分が大きく、そのため、フォールバック処理が適切に動作するかを計測にて評価する必要があると考える。また、この問題を解決する手段として登場した Happy Eyeball[7] の動作に関しても評価することが重要である。

(2) DNS の問い合わせに関する課題

DNS の IPv6 対応には二種類の意味があり、IPv6 の名前解決に必要な AAAA レコードの登録 (コンテンツの IPv6 対応) と IPv6 による通信を受け付ける (トランスポートの IPv6 対応) となる。そのため、IPv4 および IPv6 双方で保持するコンテンツが異なる場合や、AAAA レコードに対して適切に応答できない場合に問題が生じることとなる。障害を検知するためには、双方のプロトコルで端末に登録されているネームサーバに対して名前解決を試み、A レコードおよび AAAA レコードを正しく取得できることを計測にて評価する必要があると考える。

(3) PMTUD BlackHole に関する課題

IPv6 では途中経路でのパケット断片化が禁止されており、通信開始時において通信路の最小 MTU を計測する (PMTUD: パス MTU 探索) が必須である。

PMTUD では ICMPv6 の "Packet Too Big" を利用するため、ICMPv6 パケットが遮断された環境下ではこの PMTUD BlackHole 問題により通信が成り立たない場合がある。この問題は IPv4 における DF ビットが設定された場合にも発生するもので、通信先に対してパス MTU の値を評価しておくことが重要となる。

3. 評価手法の検討

本研究では、ユーザ環境においてネットワーク障害点を検出する手段を、OSI 参照モデルのようにレイヤに分けて整理することで、迅速な障害把握を実現するシステム構築を目指している。本章では、ネットワーク状態を評価する際に用いる計測レイヤの概念を定義する。

3.1 計測レイヤの定義

計測レイヤは、ネットワーク運用のモデル化に必要な概念として考えており、ネットワーク状態を階層的に表現し、それぞれのレイヤにて発生しうる障害を体系的に表現するために用いる。インターネットは OSI 階層モデルと同様に TCP/IP 階層モデル (4 層) により通信プロトコルが整理されているので、このモデルに沿う形で整理を進めた。以下に、これまでの我々の取り組み [3] を元に再定義した 6 層の計測レイヤを説明する。

(1) データリンク層 (datalink)

OSI 参照モデルにおける Layer 2 と同じ層で、隣接機器との接続性を確認するための計測層である。ネットワークインタフェースの down/up により、リンクアップできるまでを確認する。無線ネットワークにおいては、Association が確立されるまでの計測となる。計測と合わせて、リンクアップにおける接続パラメータの収集を行う。具体的には以下の項目となる。

- 共通項目
MAC アドレス、インタフェース MTU
- 有線ネットワーク
メディアタイプ 等
- 無線ネットワーク
サービスセット識別子 (SSID)、チャンネル、受信信号強度 (RSSI)、ノイズ信号強度 等

現時点では、無線ネットワークは無線 LAN に限定しているが、スマートフォンなどのデバイスへの展開を考慮すると、3G/LTE での評価項目を検討する必要があると考えている。

(2) インタフェース設定層 (interface)

OSI 参照モデルの Layer3 における IP アドレス設定を確認する層である。IPv4 の場合は DHCP による自動アドレス設定の確認、IPv6 の場合は RA による SLAAC もしくは DHCPv6 による自動アドレス設定の確認を行う。IPv6 の自動アドレス設定に関しては、SLAAC

のみ、SLAAC+ステートレス DHCPv6, SLAAC+ステートフル DHCPv6 など様々なパターンが存在するため、評価対象のネットワークによる運用モデルにより評価項目が大きく異なる可能性がある。また、RA に設定されるフラグによる挙動が OS 毎に異なることが指摘されており、仕様上の整理が進められている [8]。インタフェースに設定された情報として以下の項目を収集する。

- IPv4 情報
IPv4 設定情報, IPv4 アドレス, ネットマスク, IPv4 デフォルトルータ, IPv4 ネームサーバ等
- IPv6 情報
IPv6 設定情報, IPv6 リンクローカルアドレス, RA プレフィックス情報, RA フラグ情報, IPv6 アドレス, プレフィックス長, IPv6 デフォルトルータ, IPv4 ネームサーバ等

(3) ローカルネットワーク層 (localnet)

同一セグメント (ローカルネットワーク) における IP の到達性を確認する層である。ローカルネットワークにおけるサービス発見として mDNS (Bonjour, Avahi) や LLMNR (Windows) を用いたサービス確認もこの層になる。到達性の確認対象はデフォルトルートとネームサーバとし、通信遅延時間 (RTT) の計測を合わせて実施し収集する。

(4) グローバルネットワーク層 (globalnet)

組織外の外部サーバへの IP 的な到達性を確認する層である。到達性の確認 (ping による RTT と traceroute によるパス計測) と合わせて、パス MTU を計測する。確認する対象のサーバとしては、本計測用に準備するサーバの他に、名前解決層で用いる Google パブリック DNS サーバ等を用い、それぞれのサーバ毎に到達性確認を実施する。

(5) 名前解決層 (dns)

アプリケーションを利用する際に必須となる機能として、ドメイン名から IP アドレスを取得する名前解決があり、この名前解決の確認を行う層がこの層である。名前解決はデュアルスタックになると IPv4 と IPv6 双方での確認が必要であり、また、OS が提供する resolver API 毎に挙動が異なることが想定される。そのため、以下の調査を DHCP/DHCPv6 等で得られたネームサーバと Google パブリック DNS サーバに対して実施する。

- OS 標準の resolver API を用いた名前解決
- レコードおよびトランスポートを指定した名前解決
上記それぞれにおいて A レコードのみ, AAAA レコードのみおよび双方を持つサーバドメイン名の名前解決を実施する。NAT64/DNS64 によるトランスレータが動作している環境の評価もこの層で行う。

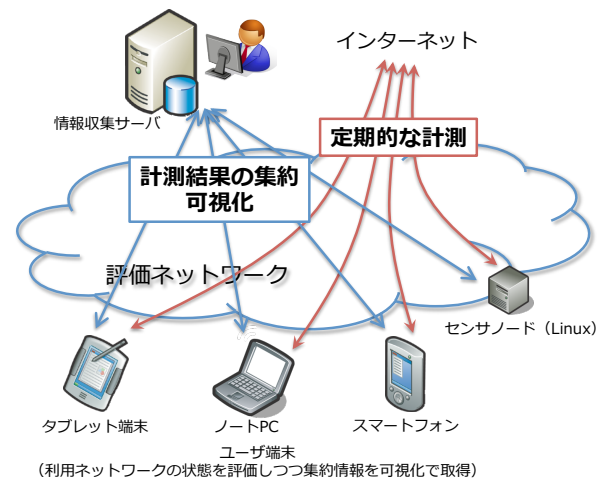


図 2 提案手法の計測イメージ

Fig. 2 Measurement overview of the proposed method

(6) ウェブアプリケーション層 (web)

OSI 参照モデルにおける Layer5 以上の層に相当する機能を確認する層で、ウェブアプリケーションに特化して評価を行う。この層では、組織外の外部サーバに対して HTTP での通信が可能か確認する。この他に確認する項目として以下を想定する。

- HTTP 通信における通信速度
- Happy Eyeball による閲覧確認
- DF ビットが有効なウェブサーバへの通信確認 (IPv4)
- ISP における通信の最適化処理の影響確認

4. 提案手法の設計と実装

先にも述べたように、ユーザが「つながらない」と感じる障害はネットワークのどの階層での障害であるかを求める事が重要である。図 2 に、提案手法の計測イメージを記す。ユーザ側からのネットワーク状態評価を行うためには、様々なユーザ端末への対応が求められ、合わせて、ユーザにとって魅力的な情報を提示することが重要と考える。ユーザへの情報提供手法としては、計測アプリ自身の表示と合わせて、計測結果を集約した情報の開示も考えられる。今回のプロトタイプシステムでは、情報収集サーバにて集約した情報の可視化のみを行っている。

4.1 評価項目の定義

前章にて定義した階層に対して、具体的な評価項目を表 1 のように定義した。各層における障害検知の評価項目は boolean 型 (bool) として定義しており、障害判断の大項目として利用することを想定している。information 型 (info) として定義した評価項目は、発生している障害の詳細を解析するためや次のレイヤにおける評価項目を実施する判断を決定するためなどに用いる項目である。今回は、プロトタイプ実装可能な項目を中心に列挙している。

表 1 定義した計測レイヤと評価項目
Table 1 The measurement layer and test case

階層名	型	種別	評価項目
datalink	bool	共通	インタフェース UP: OSI 参照モデルにおける Layer2 におけるリンクアップを確認
	info	共通	インタフェースタイプ: インタフェースのタイプを示す情報 (Ethernet, Wi-Fi, LTE など)
	info	共通	インタフェース MTU: インタフェースの MTU 情報
	info	共通	MAC アドレス: インタフェースの MAC アドレス (識別子として利用)
	info	有線	メディアタイプ: オートネゴシエーション機能等で決定される通信速度や通信モードの情報
	info	無線	サービスセット識別子 (SSID): 利用している無線ネットワークの SSID 情報
	info	無線	チャンネル: 利用している無線ネットワークのチャンネル情報
	info	無線	信号受信強度 (RSSI): 利用している無線ネットワークの RSSI 情報
	info	無線	ノイズ信号強度: 受信しているノイズの信号強度情報
	info	無線	データレート: 利用している無線ネットワークのデータレート情報
interface	info	IPv4	インタフェースの IPv4 設定: 対象インタフェースの IPv4 における設定情報
	bool	IPv4	IPv4 自動アドレス設定 (DHCP): DHCP によるアドレス設定を確認
	info	IPv4	IPv4 アドレス: インタフェースに設定された IPv4 アドレス情報
	info	IPv4	ネットマスク: インタフェースに設定された IPv4 ネットマスク情報
	info	IPv4	IPv4 デフォルトルータ: インタフェースに設定された IPv4 のデフォルトルータ情報
	info	IPv4	IPv4 ネームサーバ: 対象インタフェースの自動アドレス設定にて取得した IPv4 ネームサーバ情報
	info	IPv6	インタフェースの IPv6 設定: 対象インタフェースの IPv6 における設定情報
	info	IPv6	IPv6 リンクローカルアドレス: インタフェースに設定された IPv6 のリンクローカルアドレス情報
	bool	IPv6	IPv6 自動アドレス設定 (SLAAC/DHCPv6): SLAAC および DHCPv6 によるアドレス設定を確認
	info	RA	RA のフラグ情報: インタフェースで受信する RA に設定される O フラグ、M フラグの情報
	info	RA	RA のプレフィックス情報: インタフェースで受信する RA に設定されるプレフィックス情報
	info	RA	RA のフラグ情報: インタフェースで受信する RA に設定されるプレフィックス情報のフラグ情報
	info	IPv6	IPv6 アドレス: インタフェースに設定された IPv6 アドレス情報
	info	IPv6	IPv6 デフォルトルータ: インタフェースに設定された IPv6 のデフォルトルータ情報
info	IPv6	IPv6 ネームサーバ: 対象インタフェースの自動アドレス設定にて取得した IPv6 ネームサーバ情報	
localnet	bool	IPv4	IPv4 デフォルトルータ到達性: IPv4 のデフォルトルータへの到達性を確認 (ping)
	info	IPv4	IPv4 デフォルトルータ往復遅延: IPv4 デフォルトルータへの往復遅延時間情報
	bool	IPv4	IPv4 ネームサーバ到達性: IPv4 ネームサーバへの到達性を確認 (ping)
	info	IPv4	IPv4 ネームサーバ往復遅延: IPv4 ネームサーバへの往復遅延時間情報
	bool	IPv6	IPv6 デフォルトルータ到達性: IPv6 のデフォルトルータへの到達性を確認 (ping)
	info	IPv6	IPv6 デフォルトルータ往復遅延: IPv6 デフォルトルータへの往復遅延時間情報
	bool	IPv6	IPv6 ネームサーバ到達性: IPv6 ネームサーバへの到達性を確認 (ping)
	info	IPv6	IPv6 ネームサーバ往復遅延: IPv6 ネームサーバへの往復遅延時間情報
globalnet	bool	IPv4	外部サーバへの IPv4 到達性: 外部サーバへの IPv4 による到達性を確認 (ping)
	info	IPv4	外部サーバへの IPv4 往復遅延: 外部サーバへの IPv4 の往復遅延時間情報
	info	IPv4	外部サーバへの IPv4 通信経路: 外部サーバへの IPv4 の通信経路情報 (traceroute)
	info	IPv4	外部サーバへの IPv4 パス MTU: 外部サーバへの IPv4 通信路における最大 MTU サイズの値
	bool	IPv6	外部サーバへの IPv6 到達性: 外部サーバへの IPv6 による到達性を確認 (ping)
	info	IPv6	外部サーバへの IPv6 往復遅延: 外部サーバへの IPv6 の往復遅延時間情報
	info	IPv6	外部サーバへの IPv6 通信経路: 外部サーバへの IPv6 の通信経路情報 (traceroute)
	info	IPv6	外部サーバへの IPv6 パス MTU: 外部サーバへの IPv6 通信路における最大 MTU サイズの値
dns	bool	IPv4	IPv4 による A レコード名前解決: IPv4 を用いた FQDN に対する A レコードの名前解決を実施
	bool	IPv4	IPv4 による AAAA レコード名前解決: IPv4 を用いた FQDN に対する AAAA レコードの名前解決を実施
	bool	IPv6	IPv6 による A レコード名前解決: IPv6 を用いた FQDN に対する A レコードの名前解決を実施
	bool	IPv6	IPv6 による AAAA レコード名前解決: IPv6 を用いた FQDN に対する AAAA レコードの名前解決を実施
	bool	dual	OS リゾルバによる名前解決: 利用する OS のリゾルバに対する名前解決 (ANY) を実施
	info	dual	OS リゾルバによる名前解決オーダ: 利用する OS のリゾルバに対する名前解決 (ANY) の結果順序
web	bool	IPv4	外部ウェブサーバ (IPv4) への HTTP 通信: 外部ウェブサーバへの IPv4 による HTTP 通信を確認
	info	IPv4	外部ウェブサーバ (IPv4) への HTTP 通信速度: 外部ウェブサーバへの IPv4 による HTTP 通信速度情報
	bool	IPv6	外部ウェブサーバ (IPv6) への HTTP 通信: 外部ウェブサーバへの IPv6 による HTTP 通信を確認
	info	IPv6	外部ウェブサーバ (IPv6) への HTTP 通信速度: 外部ウェブサーバへの IPv6 による HTTP 通信速度情報
	info	dual	Happy Eyeball の挙動: 利用する OS が提供する Happy Eyeball API の挙動を確認
	info	IPv4	透過型プロキシサーバの検出 (IPv4): IPv4 通信路に存在する透過型プロキシサーバの検出
	info	IPv6	透過型プロキシサーバの検出 (IPv6): IPv6 通信路に存在する透過型プロキシサーバの検出

