IPv6 シングルスタックによる eduroam 構築

垣内 正年[1] 辻井 高浩[1] 藤川 和利[1]

概要：奈良先端科学技術大学院大学 (以下、NAIST) では、大学訪問者向けのネットワークとして IPv6 シングルスタックによる eduroam を構築した。プライベート IP アドレスの割り当ては通信セッションの記録が課題となった。そのため、eduroam 利用者には IPv6 グローバルアドレスを配布し、IPv4 サイトへの接続のために DNS64 / NAT64 を提供することとした。これにより、通信セッションの記録が必要となる NAT 変換を必要とするセッションを 3 分の 1 以下に削減できた。アドレス配布方法として DHCPv6 と SLAAC を試した結果、アドレス取得率はそれぞれ 81%、94%であった。本発表では、利用者に割り当てる IP アドレスの検討、構築したネットワークの構成・設定パラメータ、導入後の利用状況について説明する。

Deploying eudroam using IPv6 single-stack

MASATOSHI KAKIUCHI[1] TAKAHIRO TSUJII[1] KAZUTOSHI FUJIKAWA[1]

1. はじめに

奈良先端科学技術大学院大学 (以下、NAIST) では、大学訪問者向けのネットワークとして IPv6 シングルスタックによる eduroam を構築した。

共同研究者、インターンシップ学生などの大学訪問者を対象とするネットワーク接続環境の提供は、研究・教育活動のために不可欠である。一方、ネットワークセキュリティのために、利用者の認証、インシデント発生時の追跡性が求められる。利用者認証としては、学術無線 LAN ローミング基盤 eduroam が有効である。eduroam では、利用者登録は各研究者の所属機関で行われるため、ネットワーク接続環境を提供する際に訪問者に対する利用者受付対応が不要となる。追跡性のためには、グローバル IP アドレスを利用者に配布し IP アドレスの割り当てを管理する方法と、プライベート IP アドレスを利用者に配布し通信セッションをすべて記録する方法がある。

NAIST では、有線ネットワーク、無線 LAN ネットワーク共にグローバル IP アドレスを基本とするネットワークを構成している。しかし、大学訪問者向け eduroam ネットワークに対する新たな IPv4 グローバルアドレス割り当てはアドレスブロック利用状況から困難である一方、プライベート IP アドレスの割り当ては通信セッションの記録が課題となった。そのため、eduroam 利用者には IPv6 グローバルアドレスを配布し、IPv4 サイトへの接続のために DNS64 / NAT64 を提供することとした。これにより、通信セッションの記録が必要となる NAT 利用を削減することが可能となる。

本発表では、利用者に割り当てる IP アドレスの検討、構築したネットワークの構成・設定パラメータ、導入後の利用状況について説明する。IPv4 から IPv6 への移行は IPv4 アドレス枯渇により避けられず、IPv6 シングルスタック運用時に発見された知見は他のネットワークにおいても有用であると考えられる。

2. IPv6 シングルスタックによる eduroam 構築

eduroam は、欧州 GÉANT で開発された国際学術無線 LAN ローミング基盤であり、日本国内では国立情報学研究所（NII）が eduroam JP[*1]の名称で運用とサポートを行っている。eduroam を用いることにより、学術研究機関に所属する教職員・学生は所属元で発行された認証 ID を使用して訪問先機関においても無線 LAN を使用することが可能となる。接続設定が共通のため利用者は訪問先毎に設定を

[1] 奈良先端科学技術大学院大学 総合情報基盤センター
Information Initiative Center, NAIST

[*1] https://www.eduroam.jp/

表 1　IPv6 自動設定の方式

	NDP RS/RA (RFC 4861)	DHCPv6 (RFC 8415)
デフォルト GW	RS/RA	-
IP アドレス	SLAAC	Stateful DHCPv6
DNS 設定	RDNSS / DNSSL (RFC 8106)	Stateless DHCPv6

変更する必要がなく、訪問先ネットワーク管理者は訪問者毎に接続 ID を発行する必要がない。また、eduroam ネットワークを組織内ネットワークから分離しておくことにより、訪問者が組織内システムに不正にアクセスすることを防止できる。

NAIST ではグローバル IP アドレスを基本とするネットワークを構築しており、有線ネットワークでは教職員による事前申請、無線 LAN では学内統合認証 ID による Captive Portal 認証を行ったホストがネットワークを利用できる。そのため、学内統合認証 ID を保持しない訪問者は学内のネットワークを利用できなかった。

訪問者のネットワーク利便性向上、学外者向け学内統合認証 ID 発行の削減を目指し、NAIST 学内において 2018 年 6 月より eduroam 接続サービスを開始した。このサービスは既存ネットワーク基盤上に構築することとし、そのためにマルチ ESSID 対応無線 LAN 基地局、仮想ルータを使用して eduroam ネットワークを追加し、DNS、DHCP 等のサーバは既存サーバと共用とした。また、訪問者が学内システムにアクセスすることを防ぐため、学内とは異なる IP アドレスブロックを使用した。インシデント発生時の追跡性の担保のため、認証ログ、IP アドレス割り当て記録、通信セッションログを残すこととした。なお、想定収容数は 1000 ホストを目標とした。

2.1　IP アドレスの検討

利用者への配布する IP アドレスとして、主に次の形態が考えられる。

- IPv4 グローバルアドレス
- IPv4 プライベートアドレス
- IPv6 グローバルアドレス（のみ）

プライベートアドレスはグローバルアドレスを複数ホストで共用するため、インシデント発生時に追跡するためには TCP/UDP ポート番号、接続時刻等から NAT セッションログを調査する必要があるため、グローバルアドレスに比べ追跡性が劣る。しかし、想定収容数 1000 ホストのために必要となる IPv4 /22 グローバルアドレスブロックを学外利用者向けに確保することは困難であった。また、IPv6 グローバルアドレスのみの割り当ては IPv4 アドレスのみでサービスしているサーバを利用できない。DNS64 / NAT64 による IPv6 / IPv4 プロトコル変換技術を使用すると、IPv6 クライアントが IPv4 サーバに接続することが可能となる。そこで、IPv6 グローバルアドレスと DNS64 / NAT64 を使用することで、基本はグローバルアドレスを使用し、最低限の NAT により IPv4 のみのサービスも利用できるようにすることとした。

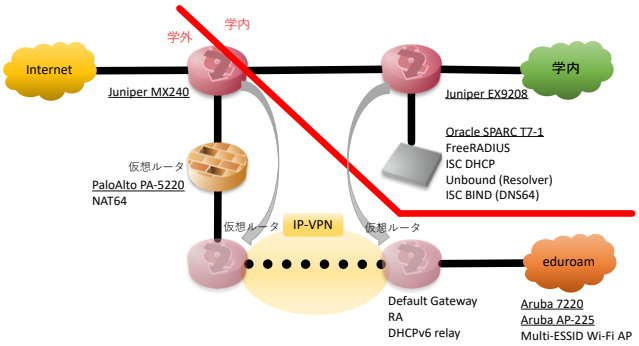

図 1　ネットワーク全体構成

2.2　IPv6 自動設定の検討

クライアントホストが IP ネットワークを使用する際に必要となる IP 基本設定として、デフォルトゲートウェイ、IP アドレス、DNS 設定がある。IPv6 において、表 1 に示す自動設定方式があり、ネットワーク環境とクライアントホストで方式が一致しない場合、ネットワークを利用できない。

IPv6 アドレス配布方法として、IPv6 Stateless Address Autoconfiguration (SLAAC)[1] と Dynamic Host Configuration Protocol for IPv6 (DHCPv6)[3] がある。SLAAC はサーバが不要、空きアドレス管理が不要という利点があるが、DHCPv6 はクライアントが使用するアドレスをサーバで管理・把握できる利点がある。本稿では SLAAC と DHCPv6 を試し比較することとした。

DNS 設定については、IPv6 ルータ広告 Recursive DNS Server (RDNSS) オプション / DNS Search List (DNSSL) オプション [2] と Stateless DHCPv6 を併用することとした。

3.　eduroam ネットワーク構成

図 1 にネットワーク構成を示す。仮想ルータ機能を使用し、学内ネットワークと eduroam のための学外ネットワークを分離し、無線 LAN 基地局のマルチ ESSID 機能により「eduroam」を提供した。RADIUS、DHCP、DNS サーバは既存サーバ上に構築した。

3.1　認証と通信制御

利用者認証は、RADIUS による EAP 認証を使用した。RADIUS サーバとして既存の FreeRADIUS にバーチャルサーバを追加してプロキシとして機能させ、認証処理を

eduroam JP サーバに問い合わせることにより eduroam 認証連携を行った。本学教職員・学生の認証 ID を管理する IdP は学内にサーバを構築せず、eduroam JP 認証連携 ID サービスを利用した。

通信制御において、eduroam は原則アクセス制限を行わないことになっている。しかし、クライアントホストからの誤った IPv6 ルータ広告・DHCPv6 アドレス配布は同一セグメント内の利用者の通信を妨げる重大な通信障害を引き起こすため、防御が必要である。また、インターネットではポートスキャン、ネットワークを通じた攻撃が常態化している。解決できない近隣探索による不要なマルチキャスト通信によるネットワーク性能低下、ネットワークセキュリティが不十分なホストに対するセキュリティインシデント発生の恐れがある。そのため、インターネット側からクライアントホスト宛の通信セッションは制限することが好ましいと考えられる。

無線 LAN 基地局 Aruba 7220 / AP-225 において、クライアントホスト宛の IPv6 ルータ要請 (ICMPv6 type 135)・DHCPv6 要求 (UDP 宛先ポート 547) を遮断するとともに、クライアントホストからの IPv6 ルータ広告 (ICMPv6 type 136)・DHCPv6 応答 (UDP 宛先ポート 546) を遮断した。また、RFC 3972 リンクローカルアドレス (169.254.0.0/16) によるクライアントホスト間通信を含めた IPv4 通信をブロックするため、IPv4 (ether type 0x800)・ARP (ether type 0x806) を遮断した。

通信セッション管理を行う PaloAlto PA-5220 において、インターネット側からクライアントホスト宛セッションを遮断した。PaloAlto PA-5220 は仕様上、同時セッション数 4 000 000 セッションの制限がある。総セッション数があふれた場合、eduroam において新規セッションの通信ができないだけでなく、PA-5220 上の全仮想ルータにも影響を及ぼす。そのため、クライアント IP アドレス毎に同時セッション数を 1000 セッションに制限し、1000 台のホストに対して最大セッション数が 1 000 000 セッションに収まるようにした。

3.2 クライアントホストのアドレス取得

SLAAC を使用する場合、クライアントホストのアドレスを把握するためには、ルータの IPv6 Neighbor Discovery テーブルの取得、もしくはネットワーク上の IPv6 Neighbor Discovery Protocol (NDP) パケットのキャプチャが必要となる。IPv6 Neighbor Discovery テーブルを使用する場合、クライアントホストを収容するルータにアクセスすることで情報取得可能だが、パケットキャプチャの場合、クライアントホストを収容する全ネットワークセグメントから NDP パケットのキャプチャが必要となる。

今回の構築では、SLAAC 使用時のクライアントホストのアドレス取得のため、ルータの IPv6 Neighbor Discovery テーブルを使用した。IPv6 Neighbor Discovery テーブルは、Simple Network Management Protocol (SNMP) により IP-MIB::ipNetToPhysicalTable (.1.3.6.1.2.1.4.35) を通してアクセスできる。5 分間隔で SNMP GETBULK を使用しルータから Neighbor Discovery テーブルを取得した。

表 2 認証 ID 数 (2018 年 11 月)

認証 ID 数	578	(100.0%)
成功数 (全体)	318	(54.1%)
成功数 (学内)	133	(23.0%)
成功数 (学外)	185	(32.0%)

表 3 認証ホスト数 (2018 年 11 月)

認証 MAC 数	720	(100.0%)
成功あり	494	(68.6%)
成功なし	226	(31.3%)

表 4 DHCPv6 アドレス取得数 (2018 年 11 月)

認証成功 MAC 数	494	(100.0%)
Reply NA DUID 数	401	(81.1%)

3.3 NAT64

NAT64 のプレフィックスとして NAT64 Well-Known Prefix 64:ff9b::/64 を使用した。NAT64 として用いた PaloAlto PA-5220 は、NAT オーバーサブスクリプションによりポート番号を 4 セッションで共有できる。そのため、想定収容数 1000 ホストに対し同時セッション数 1000 を提供するためには、次式により NAT アドレスプールが 4 個必要となる。

$$\frac{1000 \times 1000}{4 \times (65536 - 1024)} \sim 3.8$$

そのため、学内利用とは異なるアドレスブロックから 4 アドレス割り当てた。

4. ネットワーク利用状況

IPv6 シングルスタックによる eduroam 利用状況を確認するため、RADIUS 認証ログ、DHCPv6 ログ、通信セッションログを確認した。

4.1 Stateful DHCPv6 利用状況

Stateful DHCPv6 を使用していた 2018 年 11 月 1 日から 2018 年 11 月 30 日までの RADIUS 認証ログ、DHCPv6 ログからネットワーク利用状況を確認した。期間中、35 610 件の認証要求があり、認証成功は 21 391 件であった。

認証 ID 毎の結果を表 2 に示す。eduroam JP 認証連携 ID サービスの学内利用者アドレスを学内とし、それ以外を学外とした。この結果から、学内統合認証 ID を保有している学内利用者が一定数存在していることがわかる。原因として、学外で設定した eduroam をそのまま利用してい

表 5　認証ホスト数 (SLAAC)

認証 MAC 数	272	(100%)
成功あり	192	(70%)
成功なし	80	(29%)

表 6　SLAAC アドレス取得数

認証成功 MAC 数	192	(100%)
NDP グローバル MAC 一致数	182	(94%)
NDP グローバル MAC 不一致	10	(5%)

表 7　通信セッション数（2018 年 11 月 15 日）

総セッション数	196,446	(100.0%)
IPv6 native	137,345	(69.9%)
内、学内	99,522	(50.7%)
内、学外	37,783	(19.2%)
内、サイトローカル	40	(0.0%)
NAT64	59,101	(30.1%)

る例や、Captive Portal 認証が必要な学内無線 LAN より認証が容易な eduroam を使用している例が考えられる。

認証 MAC アドレス毎の結果を表 3 に示す。31.3%の MAC アドレスが認証できておらず、eduroam をまったく利用できていなかった。認証に失敗した ID を確認すると、他大学のゲスト ID と推測される ID や、サービスが終了している旧 eduroam 仮名アカウントが確認できた。一度設定した認証 ID が使用できなくなっても残されていることがわかる。

DHCPv6 アドレス取得数の結果を表 4 に示す。認証成功ホストの内 2 割弱がアドレス取得できておらず、Stateful DHCPv6 もしくは IPv6 非対応のため、ネットワークを利用できていない。

4.2　SLAAC 利用状況

SLAAC を使用していた 2019 年 4 月 22 日から 4 月 28 日までの RADIUS 認証ログ、IPv6 Neighbor Discovery テーブルからネットワーク利用状況を確認した。期間中、11 008 件の認証要求があり、認証成功は 5945 件であった。

認証 MAC アドレス毎の結果を表 5 に示す。70%の MAC アドレスが認証できていた。これらの MAC アドレスの内、IPv6 Neighbor Discovery テーブルからグローバルアドレスが発見された MAC 数の結果を表 6 に示す。認証成功ホストの内グローバルアドレス取得率は 94%であり、DHCPv6 の 81.1%から上昇した。

4.3　通信セッション

2018 年 11 月 15 日 (木) の通信セッションログから IPv6、NAT64 利用状況を確認した。図 7 にセッション数の結果を示す。IPv6 native は、NAT64 を使用せず IPv6 グローバルアドレスで直接クライアント–サーバが通信しているセッションであり、全体の約 7 割であった。これにより、IPv4 グローバルアドレスをクライアントホストに割り当てない状況で NAT 利用を約 3 割に抑えることができた。約半数が学内宛 IPv6 native であるが、その内 98.9%は宛先ポート 53 であり、DNS サーバとの通信セッションであった。DNS がほとんどを占める学内宛 IPv6 native を除くと、IPv6 natve と NAT64 の比率がほぼ 2:3 であり、現状 NAT64 が重要であることがわかった。

5.　IPv6 シングルスタックにおける障害例

IPv6 シングルスタックによるネットワークにおいて、いくつかの障害が発生した。

DNS64 / NAT64 変換は DNS 登録状況に応じて以下の様に動作する。

- IPv4 (A レコード) のみ
  → DNS64 変換により IPv6 アドレス生成･NAT64 変換
- IPv4/v6 (A/AAAA レコード) 両方
  →変換なし IPv6 直接通信

IPv6 でサービスしていないにも関わらず DNS に IPv6 アドレスが登録されている例があり、IPv6 シングルスタック環境からこのサーバにアクセスできなかった。また、一部のサーバでは HTTP (TCP ポート 80) では IPv4 / IPv6 両方でサービスしているが、HTTPS (TCP ポート 443) では IPv4 のみサービスしているため、URL の http://... と https://... の違いにより同じサーバでもアクセスの可否が異なる例があった。

IPv6 において、デフォルトゲートウェイの有効時間と IP アドレスの有効時間は別の設定項目となっている。RFC 4861 においてデフォルト値は、デフォルトゲートウェイ有効時間がルータ広告最大間隔の 3 倍である 30 分、アドレスプレフィックス有効時間が 30 日となっている。そのため、ルータ広告がパケットロス等により連続 3 パケット途絶えると、クライアントホストのアドレスは有効な状態でデフォルトゲートウェイ情報が無効となり、セグメント外と通信できなくなる。IPv6 シングルスタックにおいては IPv4 にフォールバックできないため、致命的な障害となる。本学の無線 LAN 環境では、デフォルトゲートウェイ有効時間をルータ広告最大間隔の 10 倍とすることで障害頻度が下がった。

DNS 権威サーバの AAAA レコードとして NAT64 Well-Known Prefix 64:ff9b::/64 が返される例があり、DNS キャッシュサーバから権威サーバの通信が一部 NAT64 経由となっていた。この問題は、Unbound `do-not-query-address` 設定、BIND `bogus` 設定などにより 64:ff9b::/64 を問い合わせ先アドレスから除外することにより回避できた。

6.　おわりに

本稿では、IPv6 シングルスタックによる eduroam 構築

と導入後の利用状況について説明した。eduroam 利用者には IPv6 グローバルアドレスを配布し、IPv4 サイトへの接続のために DNS64 / NAT64 を提供することにより、通信セッションの記録が必要となる NAT 変換を必要とするセッションを 3 分の 1 以下に削減できた。アドレス配布方法として DHCPv6 と SLAAC を試した結果、アドレス取得率はそれぞれ 81%、94%であった。この結果から、SLAAC を用いることで多くのホストに IPv6 アドレスを配布しネットワークに接続することができたが、一部接続できないクライアント、利用できないサーバが発見された。今後は利用できないクライアント・サーバを削減する手法・運用について検討し改善する予定である。

参考文献

[1] S. Thomson, T. Narten, T. Jinmei: IPv6 Stateless Address Autoconfiguration, RFC 4862 (Draft Standard), IETF, Sep. 2007.

[2] J. Jeong, S. Park, L. Beloeil, S. Madanapalli: IPv6 Router Advertisement Options for DNS Configuration, RFC 8106 (Proposed Standard), IETF, Mar. 2017.

[3] T. Mrugalski, M. Siodelski, B. Volz, A. Yourtchenko, M. Richardson, S. Jiang, T. Lemon, T. Winters: Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC 8415 (Proposed Standard), IETF, Nov. 2018.