一般口演
一般口演23
ネットワーク・ IoT・バーコード
2018年11月25日(日) 13:40 〜 15:40 C会場 (4F 411+412)

[4-C-3-3] ダイナミック認証 VLAN 導入時の IPv6 ネットワーク設計
○大垣内 多徳, 山下 芳範 （福井大学医学部附属病院医療情報部）

福井大学医学部附属病院では、2014年の新病棟開業以降、病院再整備事業による院内ネットワーク設備の更新に合わせて、 MAC アドレス認証に基づくダイナミック VLAN の導入を進めてきた。本院のダイナミック VLAN の導入は、運用・構築コストの低減と医療安全の両立を目指したもので、事前に申請された MAC address からの RADIUS 認証要求に応じて、所属 VLAN をスイッチに通知することで単一ポートで複数 VLAN の同時利用が可能な機能を利用している。一方、本学は IPv6 を積極的に導入しており、ネットワークの基本サービスは IPv4/IPv6 いずれでも利用可能である。今回、 IPv6のアドレス自動設定機能とダイナミック VLAN との親和性について、問題が確認された。この問題は、複数の VLAN に所属する端末が同一ポートに接続されている場合、異なる VLAN のルータ広告(RA)が端末に届くため、結果的に使用できないアドレスが端末に設定されるというものである。現時点では端末がデュアルスタックであるため、 IPv6 の利用不可とサービス不可は直結していないが、今後 IPv6 シングルスタックの機材が導入された場合は、大きな問題となる可能性が考えられるため、現状の確認と対策の検討をおこなった。その結果、本院ネットワークの実績では、約8%のコンセントでは、異なる VLAN に所属する端末が同時に接続されたことがあり、 IPv6 での利用に影響が出た可能性があることが確認された。本件に対応する方法としては、 RA からネットワーク情報を取り除き、 statefull な dhcpv6 を用いてアドレス設定を行うことが考えられる。すでに端末認証のために MAC アドレスの収集を含む端末管理を行っているため、 dhcpv6 のサービスを行う準備中である。さらに dhcpv6 サービスを導入することで、匿名アドレス使用による端末追跡の困難さの軽減も実現できると考えられる。

ダイナミック認証 VLAN 導入時の IPv6 ネットワーク設計

大垣内 多徳[*1]、山下 芳範[*2]、
*1 福井大学総合情報基盤センター、
*2 福井大学医学部附属病院医療情報部

Ipv6 Netowrk design with Dynamic VLAN

OGAITO Tatoku[*1], YAMASHITA Yoshinori[*2]
*1 Center for Information Initiative, University of FUKUI
*2 Department of Medical Informatics, University of FUKUI Hospital

We have introduced dynamic VLAN with MAC address authentication to our hospital network from 2014. This makes it possible to accomodate terminals belong to different VLANs to a single socket, and realizes medical safety, operation and construction cost reduction at same time. In the analysis of the results for three and a half years after introduction, we found out that there were some problems with IPv6 communication of some terminals, so we investigated. As a result, we found that dynamic VLAN using multiple VLANs on a signle socket has low affinity with IPv6 stateless address setting, and by introducing IPv6 statefull address setting by DHCPv6 leads to resolve the problem.

Keywords: Network, Ipv6, Dynamic VLAN

1. 緒論

福井大学医学部附属病院では、2014 年から始まった病院再整備事業にあたり、院内ネットワークのあり方を検討し、構築を行ってきた。その中で、院内ネットワークの利用目的や利用範囲が多様化する事に備え、高可用性と構築・運用コストの低減および医療安全の実現をめざして、同一情報コンセント(端子)で複数 VLAN が利用可能な、端末の MAC address を用いたダイナミック認証 VLAN を導入した[1),2)]。

一方、福井大学では IPv6 の導入を積極的に行っており、全学ネットワークは IPv4/IPv6 のいずれも利用でき[3)]、総合情報基盤センターが提供する情報サービスはデュアルスタックで運用されている。アドレス管理は IPv4 については、届けられた MAC address に対して固定アドレスを払い出す運用を行っているが、IPv6 については、サーバについては固定アドレスを払い出すものの、一般端末についてはルータ広告(RA)[4)]を用いた IPv6 stateless[5)] 設定を採用している。この様な運用のため、IPv6 ready な端末は、利用者が意識することなく、IPv6 の利用が可能である。

附属病院内に対するダイナミック認証 VLAN の導入後の評価の中で、一部の端末の IPv6 通信に不具合が発見された。この不具合を解析した結果、筆者が設計時には認識していなかったダイナミック認証 VLAN が IPv6 運用へ与える影響が明らかとなり、対策を行ったので、本稿で報告を行う。

2. 目的

ダイナミック 認証 VLAN を導入した環境で Ipv6 通信に不具合が発生する要因を明らかとし、安定的な通信を行うための方法を策定し、有効であることを確認する。

3. 方法

本院では 2014 年 9 月 13 日に運用を開始した新病棟のネットワークからダイナミック認証 VLAN を導入し、病院再整備の中でネットワーク機器の更新が行われた箇所へ適用範囲を拡大し、2018 年 3 月までに外来、中央診療部門を含む院内全域が対象となっている。導入当初の半月のデータを除外し、2014 年 10 月から 2018 年 3 月までの MAC address 認証の成功 log を用いて、端末の接続タイミング、スイッチ名、ポート名、MAC address を抽出し、時系列に並べることで、院内の端子でのダイナミック VLAN の利用状況をまとめ、単一端子に異なる VLAN に所属する端末が接続した状況を確認する。

また、複数の VLAN が割り当てられた状態の端子を用意した上で端末を接続し、アドレス付与状況、経路設定の状態、通信の可否についてパケット取得を含む調査を行うことで、通信不可の原因を特定し、対応方法についての検討を行う。

4. 調査結果

4.1 動的 VLAN 割当に関する情報

2014 年 10 月 1 日から 2018 年 3 月 31 日までの認証結果は、成功が 6,407,829 件、失敗が 44,748,171 件であった。この 640 万件の成功ログをスイッチのポート単位に分類したところ、認証要求が発生したスイッチのポート数(これは端子数に等しい)は、2,531 個となった。このうち、対象期間内において複数の VLAN が割り当てられたことのある端子数は 210 であり、その割合はおよそ 8.3% となった。これらのポートに接続されていた端末数は、延べ 3,173 台であった。

4.2 複数 VLAN 割当時の RA

通信ができないことが確認された端末は、すべて複数 VLAN が割り当てられたことのある端子に接続されており、かつ当該端末が問題なく通信ができる場合もあることが確認された。そのため、ダイナミック認証 VLAN 自体の問題ではなく、複数 VLAN が割り当てられた時の端末の振舞について調査を継続した結果、次にあげるような事柄が起きていると考えられた。

MAC アドレス認証によるダイナミック VLAN 運用時のパケットは、当該ポートへの入力(端末から受信する)パケットについては認証された MAC アドレスに結びつけられた VLAN として扱われる一方、当該ポートへの出力(端末に送信する)パケットとしては、その時点で有効な VLAN に所属するパケットの全てがタグを付与されることなく流れる。RA は、マルチキャストパケットであるため、その端子に所属する全ての端末に、すべての VLAN に対するものが流れることとなる。端末は、受信した RA に含まれるネットワーク情報から自アドレスを生成するため、結果的に各端末は接続した端子に割り振られている全ての VLAN に対応したアドレスを持つこととなる。IPv6 で

は一つのノードが複数のルーティング可能なアドレスを保持することは合法であり [6]、各ノードは宛先に応じて適切な送信元アドレスを選択する事が求められている [7]。一般に gateway の指定は link local address が用いられるので、ノードから見ると、いずれの送信元アドレスを用いる場合であっても next hop は同じであることにも問題とはならない。したがって、端末側の情報を確認しても、異常であると判断することは難しい。

しかしながら、送信されたパケットのその後の取扱いは、正規の VLAN であるか否かによって異なる。本学の場合、センタールーティングを行っているため、全ての VLAN 上でゲートウェイは、インタフェース ID を除き同一のリンクローカルアドレスを持っている。そのため、送信された全パケットは正しいルータには到達するものの、ルータが受信した VLAN とネットワークアドレスが一致するものは、ダイナミック VLAN で割り当てられた VLAN に設定されているものだけであるため、他のパケットはルータ位置で破棄され、宛先に届くことはない。そのため、端末の選択した送信アドレスによって、IPv6 通信ができる場合とできない場合が生じることとなる。

さらに、RFC 6724 では宛先アドレスと最長マッチするようなアドレスを送信アドレスとして選択する事が要求されているが、筆者が確認した中では Windows 7 の端末は、2 種類目に受信した RA に含まれているネットワーク情報に基づいたアドレスを全ての送信先への通信に用いていた。端末が接続され、IPv6 アドレスを決定する際に、ルータ要請(RS)メッセージが送信される。このパケットは、割り当てられた VLAN にのってルータに到達するため、それに対する RA の回答には正しいネットワーク情報が含まれている。RA はその後定期的に送信されているが、そこに異なるネットワーク情報が含まれていた場合、通信できないアドレスが後から設定され、Windows7 の場合は、こちらを使って通信を行うため、同一セグメント以外のすべての宛先と通信を行うことができなくなる。一方、Windows10, Linux, MacOS では、RFC6724 に則った最長マッチの原則で送信元アドレスが選択されており、異なるセグメントであっても通信できる場合があることが確認された。

5 対応の検討と結果

Pv6 では、端末設定の自動化がプロトコル策定時から検討されており、導入が簡単なため、広く用いられていると考えられる。しかし、アドレス自動設定の方法としては、stateless 以外にも、IPv4 の DHCP と同様使用されているアドレスを管理する IPv6 statefull 設定が存在する。これらの設定方法は、RA の中の managed flag(M フラグ) という値を通じて、各ノードに通知される。そのため、筆者は評価を行った端子に属する VLAN に対して、M フラグを有効としたうえで、当該セグメントに DHCPv6 サーバを構築して、各端末の動作を確認した。

その結果、Windows 7 を含め、確認した全ての端末で、正規 VLAN に対応したアドレスのみが設定され、端子に複数の VLAN が割り当てられた状態でも通信が問題なくできることが確認された。

6 考察

まず、認証 VLAN 導入に関する評価であるが、割り当てられた VLAN の利用履歴からは当該端子の利用目的が変更されたと見なされるものも含まれていたが、それらも含めて当初目指した「どの端子であっても繋げば正しく繋がる」という環境が実現できていると評価できると考える。これは、病院環境に認証 VLAN を導入する事で、医療安全、利用者利便性と構築運用コストの低減を両立することができることを示している。

また、認証 VLAN と IPv6 通信環境について、IPv6 のアドレス設定方法として IPv6 stateless 設定を用い、接続端子に複数 VLAN が同時に割り当てられている場合に問題が起きていることを明らかとした。この問題は、筆者の調査解析の中で明らかとなったが、利用者からの申告は受けていない。これは、これは、OS による、IPv4 への切り替えが行われているためであると考えられる。そのため、実際には IPv6 による通信ができないと OS 側で判断するまでの期間、通信の開始が遅れているものと思われる。

RA で M フラグを有効とした上で、DHCPv6 サーバを導入する事で、複数 VLAN が同時に割り当てられる場合でも、IPv6 通信が安定的に行われることが示された。認証 VLAN を行うためには、接続される端末の MAC アドレス管理を行う必要があるため、管理コストが著しく増大するわけではないが、本学で運用中の L3 スイッチには DHCPv6 リレー機能がないため、DHCPv6 サーバに全 VLAN を接続して安定運用できるかどうかの評価が必要である。一方、statefull 運用をおこなうことで、現在発生している IPv6 匿名アドレス使用端末の追跡困難さの軽減も実現されると期待される。

7 結論

IPv6 運用環境に、ダイナミック認証 VLAN を導入する際には、各ノードのアドレス設定方法として IPv6 stateless を採用すると通信不具合が発生する。認証情報を利用した DHCPv6 サーバを導入する事で、この問題は回避でき、また匿名アドレスの追跡困難さの軽減も期待できる。

参考文献

1) 大垣内 多徳, 半田 憲嗣, 山下 芳範. 病棟におけるダイナミック認証 VLAN 導入のための事前評価. 医療情報学(Suppl.) 2014; 34: 664-667

2) 大垣内 多徳, 半田 憲嗣, 山下 芳範. 病棟におけるダイナミック認証 VLAN の導入. 医療情報学(Suppl.) 2015; 35: 766-769

3) 大垣内 多徳, 半田 憲嗣, 澤田 雅子, 福井 一俊, 山下 芳範.福井大学学内ネットワークシステムの設計と構築. 情報処理学会 研究会報告 2010; 2010-IOT-10, No2: 1-6

4) T. Narten, E. Nordmark, W. Simpson, H. Holiman. Neighbor Discovery for IP version 6(IPv6). https://tools.ietf.org/html/rfc4861 (cited 2018-Aug-01)

5) S. Thomson, T. Narten, T. Jinmei. Ipv6 Stateless Address Autoconfiguration. https://tools.ietf.org/html/rfc4862 (cited 2018-Aug-01)

6) R. Hinden, S.Deering. IP version 6 Addressing Architecture. https://tools.ietf.org/html/rfc4291 (cited 2018-Aug-01)

7) D. Thaler, Ed., R. Draves, A. Matsumoto, T. Chown. Default Address Selection for Internet Protocol Version 6(IPv6). https://tools.ietf.org/html/rfc6724 (cited 2018-Aug-01)