動的 VLAN を用いた LAN の構築

○内藤茂樹 [A)]

[A)]分子科学研究所 技術課計算科学技術班

概要

分子科学研究所では平成 7 年度の ATM LAN 導入時から現在の GbE LAN まで、1VLAN 上で複数の IP サブネットを運用している。端末の移動が自由と言う長所があるが、ブロードキャストが全所的に流れてしまうと言う短所があり、ウィルス等のセキュリティ上の問題がある。しかし単純に IP サブネットを 1 つにするだけでは長短が逆転するだけで解決にならない。そこで本年度のネットワークのリプレース時に動的 VLAN を導入することにした。これによりブロードキャスト問題を回避するために IP サブネットを 1 つにしても、端末の自由な移動は可能となる。今回は動的 VLAN とそれを導入するまでの経緯、そして予定される運用形態を報告する。

1　動的 VLAN

始めに動的 VLAN について簡単に説明する。論理ネットワークには静的 VLAN によるものと動的 VLAN によるものがある。このうち静的 VLAN は各スイッチに設定された VLAN の変更を手動で行うものであり、スイッチの port 毎に使用する VLAN を設定する“port base VLAN”で構築するのが一般的である。

一方の動的 VLAN は、スイッチに接続される端末毎に使用する VLAN を割り当てるものである。したがって各端末固有の情報が必要となり、MAC アドレスを元にした“MAC base VLAN”、IP アドレスを元にした“IP base VLAN”、端末利用者を元にした“user base VLAN”等がある。なお“user base VLAN”の場合は、管理者の指定した WWW page にて認証させる等の、ユーザ認証機能を利用する場合が多いと思われる。どの方法であっても VLAN 情報はパケット毎に判別されるため、スイッチの同一 port の下流に、所属する VLAN の違う複数の端末が接続されていても問題は無い。また動的 VLAN は各方式を組み合わせることが可能である。例えば、最初に“user base VLAN”で認証を行い、その時点で端末の MAC アドレスをデータベースに登録する。そして次回接続時からはその情報を用いて、“MAC base VLAN”にて所属 VLAN を割り当てるなどの運用が可能である。

動的 VLAN を使うことのメリットは、所内を移動しても所属する VLAN が変わらないことにある。VLAN が変わらなければ端末のネットワーク設定を変える必要もない。しかもスイッチの同一 port の下流に複数 VLAN が収納可能なので、会議室等で、所属する VLAN の違う複数の端末が持ち込まれたとしても、設定変更をすることなく各端末がネットワークを共有して利用することが出来る。

2　ATM 時代の論理ネットワーク(ELAN)

ATM LAN 時代の論理ネットワークについては、平成 9 年 9 月に核融合科学研究所で行われた技術研究会で「ATM Network の SVC 運用への移行」と言う題名で発表した。ATM では LAN エミュレーションによるエミュレーテッド LAN(ELAN)にて論理ネットワークを構築していた。これは ATM によるネットワークの上に仮想的な Ethernet 環境を構築するものである。

構築当所目指していた論理ネットワークの構成は、研究系毎に 1 つの ELAN を割り当て、その上で 1 つの IP サブネットを運用する形式だった。これにより各研究系は仮想的ではあるが独立したネットワークに分離されるとともに、棟や階の区別無く同じネットワークを使用できることを目指した。分子研では居室と実験室が別の棟にあり、また各棟の各階に複数の研究系が存在しているので、ネットワークの割り当てを棟別、階別から研究系別に切り替えるには必要な機能だった。それと同時に所内の何処に移動しても同一 IP アドレスでネットワークの利用が可能という、“どこでもネットワーク”を実現するにも必要な機能だった。

ところが、支線スイッチで制御可能な ATM 論理パスの上限値が思いのほか低く、必要となる全ての ELAN を収容できない支線スイッチが出来てしまうことが判明し、この計画は白紙となった。

しかし、いまさら棟別、階別でのネットワークでは FDDI と 10BASE-5 によるネットワークと変わらず、また“どこでもネットワーク”は不可能である。そこで考え出されたのが 1 つの ELAN に複数の IP サブネットを割り当てて、全所的に一つの ELAN で運用する方法である。棟や階の違いに縛られることもなく、また研究系毎に 1 つの IP サブネットを割り当てることも可能なうえ、“どこでもネットワーク”も実現出来る。しかも、どの研究系にも属さない会議室でネットワークを使用するときでさえ、同じ ELAN 内なので IP アドレスを変更する必要が無い。しかし、ブロードキャスト/マルチキャストが全端末に届いてしまうという新たな問題を内含することになった。

3　現在の論理ネットワーク(VLAN)

平成 13 年度に ATM から Giga Bit Ethernet を用いたネットワークにリプレースした。当時 VLAN を実現する方法として、“MAC base VLAN”と“port base VLAN”、そして“user base VLAN”があった。動的な論理ネットワークを運用するために、仕様策定当所は動的 VLAN での運用を考えた。その年の Networld/Interop で、ルーセント・テクノロジーのブースにて“user base VLAN”での運用が可能との説明を受けたからだ。ただし対応するベンダーがルーセント・テクノロジー(スイッチ部門は後にアバイヤとして分離)以外になく、どの業者もルーセント・テクノロジーで入札しようとしなかったのと、仕様策定委員会でそのような最新技術を導入することに対する慎重論が出たため、導入は見送りとなった。結局“MAC base VLAN”にも慎重論が出たため、単純な“port base VLAN”での構築となった。

したがって動的 VLAN ではなく静的 VLAN での運用となった。VLAN 数の制限は無くなったが、会議室も含めた“どこでもネットワーク”の実現が重要視されたため、VLAN を研究系毎に細分化することは見送られた。結局構築した論理ネットワークは、ATM 時代の ELAN の焼き直しでしかなかった。

4　新しい論理ネットワーク(動的 VLAN)

現在リプレース中のネットワークでは“MAC base VLAN”と“user base VLAN”を組み合わせて動的 VLAN を運用する。原則端末は IP アドレスの申請をするときに MAC アドレスの情報を管理者に提示する。そして管理者は IP アドレスを割り当てると共に、MAC アドレスをデータベースに登録する。各スイッチはそのデータベースの情報を参照して、各 port の下流から受信したパケットに VLAN を割り当てる。したがって IP アドレスを管理者から割り当てられた端末にとっては、動的 VLAN は“MAC base VLAN”にて運用されていることになる。一方短期滞在の共同研究者の方等は事前に IP アドレス申請をしておくことが難しい場合がある。そのような場合に共同研究者が持ち込む端末は、データベースに MAC アドレスが登録されていないために“MAC base VLAN”を利用出来ない。したがって“user base VLAN”を使う。ゲスト用のユーザ名を使って認証を受ければ、ゲスト用の VLAN が割り当てられる。勿論職員も IP アドレスの手続きが完了する前に端末を使いたい場合等に“user base VLAN”を使うことが可能である。その場合、各自のユーザ名とパスワ

ードにて認証を行えば、その端末に各自が所属すべき VLAN が割り当てられる。

実際の運用では、まず“MAC base VLAN”での割り当てを試される。データベースに MAC アドレスが登録されていれば、この段階で VLAN が割り当てられて、ネットワークを利用することが可能になる。もし失敗した場合には“user base VLAN”での割り当てが試される。認証に成功すれば正しい VLAN が割り当てられるが、失敗した場合は利用出来るサービスが限定された VLAN を割り当てられる。一応設定次第では全ての試みに失敗した端末がネットワークに接続するのを拒否することも可能である。

また、今回のネットワークでは不正な DHCP サーバを排除する機構を取り入れる。この機構を使う場合には各端末は DHCP クライアントである必要がある。そのため分子研では各端末の設定を、固定 IP 利用から DHCP 利用へと変更する作業が必要となった。ただし、DHCP 利用でも MAC アドレスと IP アドレスは 1 対 1 に対応付けて運用されるため、IP アドレスが接続の度に変わることはない。また OS や機器によっては DHCP に対応出来ないものもあるが、そのような端末はスイッチの各 port にフィルターを設定して対処する。したがって DHCP 非対応の端末は動的 VLAN の恩恵を受けることが出来ないことになるが、基本的にそのような端末は部屋の移動をしないため特に問題にはならないと思われる。

以下、簡単に今回導入予定のネットワーク機器を挙げておく。

機器名称	製品名	備考
岡崎基幹ノード装置	CISCO Catalyst6509	
支線ノード装置	日立電線 Apresia5428GT/4348GT	上 1GbE、下 10/100/1000BASE-T
山手地区棟別集線支線ノード装置	日立電線 Apresia13000-X24-PSR	LX/SX 交換用
特殊支線ノード装置	日立電線 Apresia13100-48X-PSR	上 10GbE、下 10/100/1000BASE-T
VPN 装置	CISCO ASA5510	
無線 LAN 制御装置	Aruba 3600	
無線 LAN 基地局	Aruba 121	

今回のリプレースで各部局におかれていた部局基幹ノード装置は廃止され、岡崎基幹ノード装置 1 台に全ての支線ノード装置を接続する形態に変更する。各支線ノード装置は 1GbE で岡崎基幹ノード装置と接続され、各部屋の情報コンセントには 10/100/1000BASE-T を供給する。なお各部局内の高速なネットワークが必要な箇所には、特殊支線ノード装置を設置して岡崎基幹ノード装置と 10GbE で接続する。

5　まとめ

今回のリプレースにて VLAN の運用を静的なものから動的なものに変更した。またその方法も“MAC base VLAN”と“user base VLAN”を組み合わせることによって、非常に柔軟なものになった。分子科学研究所にとっては、それまで利用していた“どこでもネットワーク”の思想を受け継ぎながら、細かく VLAN を区切ることによって、ブロードキャスト問題を回避できたことが大きい。これは利便性はそのままで、よりセキュアなネットワークになったことを意味する。そしてそれは ATM LAN を構築した平成 8 年に計画したネットワークの、一応の完成でもある。この十数年間の技術の進歩に感謝したい。

今後はさらに新技術の導入等を計り、よりセキュアな、且つより利便性の高いネットワークの構築/運用を目指していきたいと思う。