実機を用いたネットワークの基礎技術の習得

○太田芳博、伊藤康広、福井清悟

工学系技術支援室　情報通信技術系

概要

近年主流の仮想化技術を用いるサーバ管理においては、各種 OS が稼動する仮想マシンの他に、仮想スイッチが物理サーバ内部に存在しており、OS そのものだけでなくネットワーク技術の理解が必須である。しかし現実には、ある程度決められた手順に沿って設定を行うだけであり、単に仮想化されたプラットホームにおけるサーバ管理業務を行うだけではネットワーク技術の習得という点では十分と言えない。そこで、１）学内各所からのネットワークに関する問い合わせ及び業務依頼に対して一次対応が可能な知識、技術を習得すること、２）業務引継により前任者が構築したネットワークの整理、再構築を行うことを目標とし、実機を用いたネットワーク研鑽を行ったので報告する。

1　書籍での学習

一般的に、計算機にかかる業務を「情報」という単語でひとくくりにされることが多い。しかし、その一語でカバーされる範囲は大変広く、情報通信技術系に所属する技術職員といえども、普段の業務において経験したことのない「情報技術」も存在するのが現状である。本研鑽に参加した技術職員についても、ネットワークに関する知識レベルは異なっていた。そこで実機を用いた実習を行う前に、ネットワークに関する知識レベルを一定の水準までそろえることを目的として、まずは書籍を用いたネットワーク用語の学習を行った。学習用の書籍としては主に、「シスコ技術者認定試験公式ガイドブック」[1]を用い、下記の項目について重点的に学んだ。

・TCP/IP ネットワーキングレイヤモデル
・各レイヤで動作するネットワーク機器について
・IPv4 アドレッシングとサブネットの概念
・VLAN（仮想 LAN）
・ネットワーク間ルーティング

2　実機を用いた学習

実機での学習は、Cisco Systems 社（以下、Cisco 社）製のネットワーク機器を使用した。これは、企業向け L2 スイッチ、ルータなどのネットワーク機器において、Cisco 社が非常に高い市場シェアをもっていることに着目したためである。また、機器に搭載されている Cisco IOS についても、CCNA（Cisco Certified Network Associate）などの技術者認定試験が存在しており、学習のための情報も非常に豊富なことから、ネットワーク技術を基礎から学ぶのに適していると考えた。実際に用いたネットワーク機器を表 1 に、構築した最終的なネットワーク構成図を図 1 に示し、設定した項目と内容について順に説明する。

表 1. 実機学習に用いた Cisco ネットワーク機器

機種	説明
Catalyst2960-8G	ギガビット対応レイヤー2 スイッチ
Cisco841M	小規模サイト向けサービス統合型ルータ

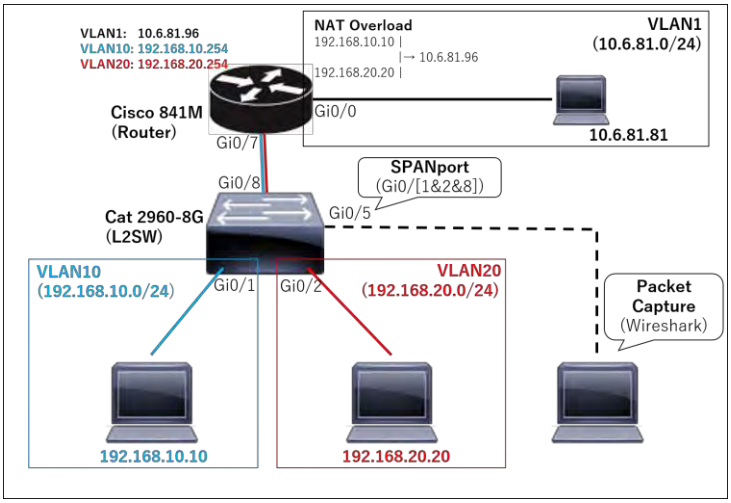

図 1： 研鑽用ネットワーク構成図

2.1 VLAN

まず、Catalyst2960-8G（以下、Cat2960）のみを用いて、VLAN の設定を行った。工場出荷時は、Cat2960 のすべての物理ポートはすべて VLAN 1（vlan id:1）に所属しているため、特に VLAN 設定を行わない場合は単なる 8 ポートのスイッチングハブとしての利用も可能である。今回は、Cat2960 の 1 番ポートを VLAN10、2 番ポートを VLAN20 とし（VLAN10，VLAN20 の vlan id としてそれぞれ 10，20 を設定する）、それぞれの VLAN にはネットワークアドレスとして、192.168.10.0/24、192.168.20.0/24 を割り当てて使用することにした。VLAN 設定後、1 番ポートに 192.168.10.10，2 番ポートに 192.168.20.10 を割り振った PC を接続したが、物理的に同じ機器にケーブル接続されていても、VLAN 設定により論理的には異なるネットワークに接続されていることになるため、2 台の PC 間で通信ができないことを確認した。

2.2 ルーティング

VLAN10、 VLAN20 に接続された PC 間で通信を行うためには、レイヤ 3 での動作であるルーティングが必要である。しかし Cat2960 はレイヤ 2 で動作する機器であり、ルーティングの機能を持っていない。そこで別途、Cisco841M を用いてルーティングを行うことにした。まず、Cat2960 の 8 番ポート及び、Cisco841M の 7 番ポートを VLAN10，VLAN20 の trunk ポート設定とした。trunk ポート設定での接続の場合、双方の機器に設定する vlan id は合わせておく必要がある。 次に、Cisco841M において、VLAN10，VLAN20 のそれぞれに SVI（Switched Virtual Interface）を作成し、IP アドレスを設定した。具体的には VLAN10 に 192.168.10.254、VLAN20 に 192.168.20.254 を割り振った。これらは、それぞれの VLAN に接続された PC に設定するデフォルトゲートウェイのアドレスとなる。 ルータに直接接続されたネットワーク同士のルーティングに関しては通常、明示的にルーティング情報を追加する必要はなく、Cat2960 の 8 番ポートと Cisco841M の 7 番ポート

を結線するだけで、異なる VLAN に所属する 192.168.10.10 と 192.168.20.20 の間で通信ができることを確認できた。

2.3　NAT

異なるネットワーク間の通信はルータなど、ルーティング機能を持ったレイヤ 3 で動作する機器を介することで通信ができるようになることを確認したが、これまでの設定では、PC に割り振ったお互いのプライベートアドレス同士で通信が行われている。しかし、通信相手がインターネット上で稼動している機器の場合、グローバルアドレスを用いるインターネットでは規約上、プライベートアドレスのルーティング設定ができないため、このままではインターネットへの通信はできない。この場合、NAT（Network Address Translation）の設定を行い、グローバルアドレスから送信しているように見せる必要がある。

本研鑽では、Cisco841M の VLAN1 を 10.6.81.0/24 のネットワークとし、このネットワークをインターネット側と考えることにした。その上で、2.1 節で行った設定と同様に、VLAN1 に SVI を作成し、10.6.81.96 を割り振った。次に VLAN1 に所属している 0 番ポートには IP アドレスを 10.6.81.81 に設定した PC を接続し、インターネット側にあるサーバとして見なすことにした。これで、Cisco841M には 3 つのネットワークが接続されていることになる。次に、VLAN20 から VLAN1 への通信においての NAT 設定を行った。具体的には、Cisco841M 上の VLAN1 の SVI に設定した 10.6.81.96 からのアクセスとなるような NAT 設定を行い、正しく通信できることを確認した。さらに、VLAN10 からも同様の NAT 設定を行うことで、VLAN1 に存在するサーバへの接続には、すべて 10.6.81.96 からのアクセスとなる、NAT オーバーロード変換の動作確認も行った。

2.4　ポートモニタリング

ここまでで、VLAN10 の PC と VLAN20 の PC 間の通信は、Cisco841M を経由しているが、trunk ポート間を流れる Ethernet フレームは、IEEE802.1Q ネットワーク規格により、vlan id の情報が付加されたものになっているはずである。これは、物理的には 1 本の接続であるが、論理的には複数の通信路が接続されているため、どの VLAN の通信データであるかがわかるようにつけられるタグ情報である。実際にタグ情報付きの Ethernet フレームが流れているかを確かめるため、ポートモニタリングを行った。具体的には、Cat2960 の 5 番ポートを SPAN ポート（ミラーポート）として設定し、1，2，8 番ポートに流れる Ethernet フレームをすべて複製して流す設定とした。その上で、5 番ポートには、パケットキャプチャソフトウェアである Wireshark をインストールした PC を別途接続して、パケットの観測を行ったところ、Ethernet フレームの中に vlan id を観測することができた（図 2）。

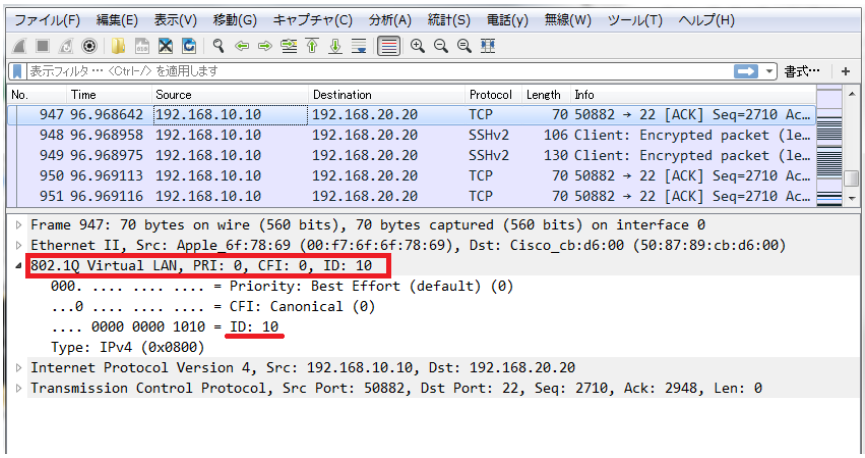

図 2：　Ethernet フレーム内の VLAN タグの確認

3　実践研修

最後に、本研鑽でこれまで学習した結果を元に、老朽化していた居室 LAN のネットワーク機器の置換と、若干のネットワーク構成の変更を行った。機器変更前と変更後のネットワーク図を図 3 に示す。従来は、Cisco ASA5505 ファイアウォール（以下、ASA5505）と YAMAHA RTX810 ルータ（以下、RTX810）の 2 台を使った構成となっていたが、これを新たに購入した Cisco ASA5506X（以下、ASA5506）で置き換える構成に変更した。

ASA5506 は、ライセンスを追加購入することで IPS, マルウェア防御などに対応する、一台でセキュリティ対応が可能な統合アプライアンス製品である。しかし、今回は特にライセンスの追加購入はせず、セキュリティ機能としては、基本搭載されているファイアウォール機能のみを用いた。

具体的には、3 つの異なるネットワーク（ 1)居室 VLAN，2)業務用 VLAN，3)NICE)への接続をそれぞれ 1 つずつの物理インタフェースに割り当てた上で、インタフェース間の通信許可・拒否設定を行うことで、セキュリティを確保した。以下に ASA5506 で設定した主な項目について説明する。

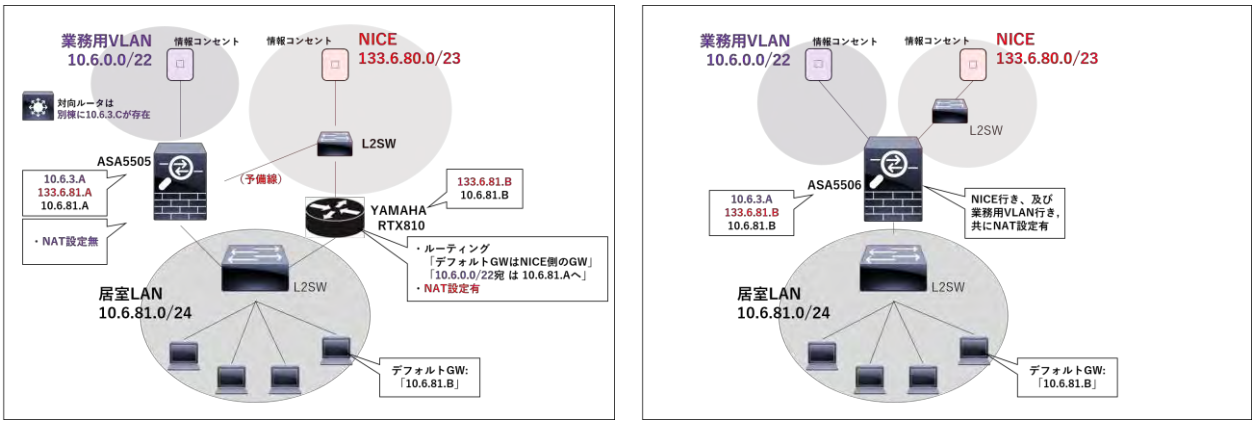

図 3：　居室ネットワーク構成（変更前（左）と変更後（右））

3.1　セキュリティレベルの設定

それぞれの物理/論理インタフェースに対し、セキュリティレベルとして 0 から 100 までの値を設定することで、内部的なインタフェース間の通信を容易に制御することができる。この時、セキュリティレベルの大きいインタフェースから小さいインタフェースへの通信開始は無条件で遮断される（なお、同じレベルが設定された場合は、標準設定では通信できない）。

居室 LAN を接続するインタフェースには 100，NICE 及び、業務用 VLAN を接続するインタフェースには 0 を設定することで、NICE 側、業務用 VLAN 側からは他のネットワークへの通信ができない設定とした（図 4）。

3.2　IP アドレスの設定

セキュリティレベルの設定に加えて、各インタフェースに対して IP アドレスを設定した。今回は、旧構成で使用していた機器である ASA5505，RTX810 の 2 台に割り振られていた IP アドレスを整理した上で、改めて ASA5506 に対して IP アドレス設定を行った。

3.3　アクセスリストの設定

ファイアウォール機能を使い、各インタフェースからの通信に対する許可/遮断ポリシーを設定する。今回は 3.1 節にてインタフェース単位でセキュリティレベルを設定したため、居室 LAN につながったインタフェースからの通信開始しかできない状態になっているが、ここでは、どのような通信を通過させるかを定義した。今回は、「居室 LAN にある IP アドレス 10.6.81.0/24 の機器から、その他のすべてのインタフェースに対してすべての IP アドレスへの通信をすべて許可」という設定をした。なお、その他のインタフェース側からの通信については念のためではあるが、「すべての通信を遮断する」という設定をした。

3.4　NAT の設定

居室 LAN 側から NICE 側への通信、及び居室 LAN 側から業務用 VLAN 側への通信を行う場合、各インタフェースに設定した IP アドレスを用いるように NAT の設定をした。グローバルネットワークである NICE 側への通信に関しては NAT の設定が必須であるが、業務用 LAN への通信に関してはプライベートアドレス同士の通信であるため、NAT の設定は必須ではない。本報告においての報告は割愛するが、業務用 VLAN 内に別途設置されている既存 L3 スイッチのルーティング設定を調査した上で、全体設計として今回は NAT の設定を行う方がよいと判断した（図 5）。

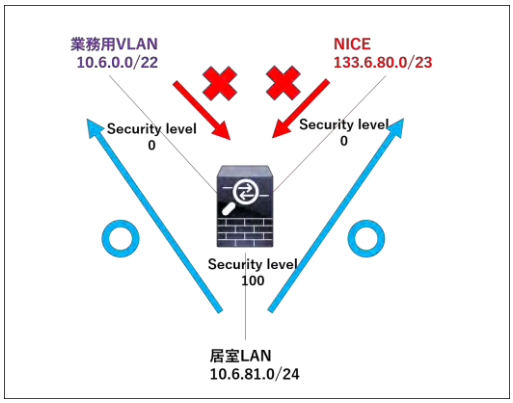

図 4：　security level の設定

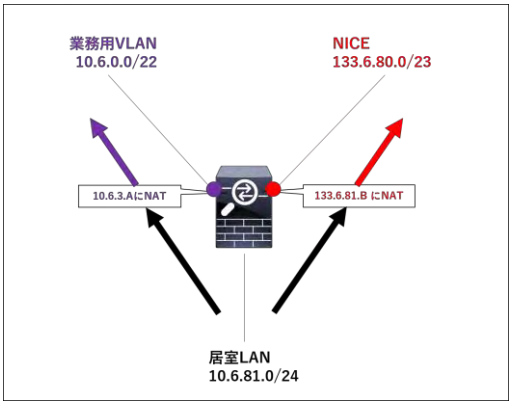

図 5：　NAT 設定

4　まとめ

本研鑽により、ネットワークを基礎から学習し、実機を使ってのネットワークの動作確認、さらには業務に関係するネットワークの機器更新までを行うことができ、ネットワーク機器を設定できる若手の技術職員が育成できた点において、大変有意義な研修であったと感じている。

工学部情報支援室で構築されたシステムでは、稼動年数から考えるとそろそろ交換の時期が近づいている機器も多く、さらに Cisco 社以外のネットワーク機器も稼動している。本研鑽を通じて学んだことを生かして、既存システムの再設計も進める予定である。なお、本研鑽は、全学技術センター技術研鑽プログラムの補助を受けて行った。

参考文献

[1]　Wendell Odom[著], クイープ株式会社[訳], “シスコ技術者認定試験公式ガイドブック Cisco CCENT/CCNA ICND1 100-101J”, インプレスジャパン

[2]　Chris Sanders[著], 高橋基信,宮本久仁男[監訳], 岡 真由美[訳], “実践パケット解析 第 2 版 -Wireshark を使ったトラブルシューティング”, オライリージャパン