

仮想化を利用したネットワーク基礎教育のための自習環境

須藤清一・岡山理科大学理学部応用数学科
〒700-0005 岡山市理大町 1-1
TEL:086-256-9445 FAX:086-256-9445
E-mail:suto@merry.xmath.ous.ac.jp

1. 背景

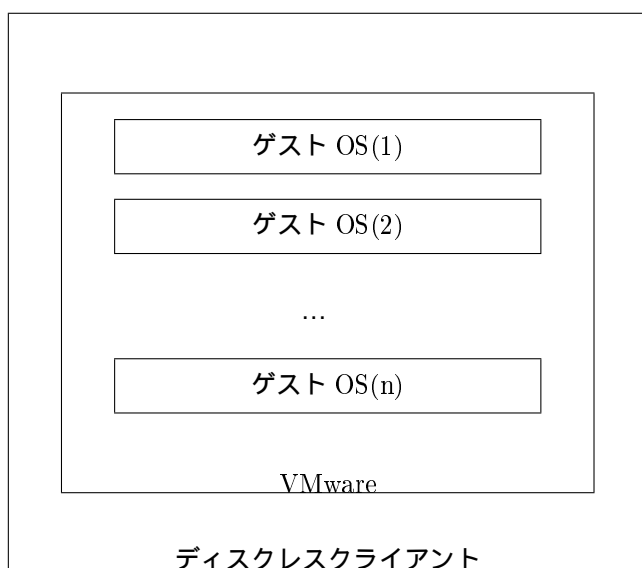
ネットワーク管理についての講義を担当するにあたって、インターネットを支える基礎技術の学習、特にルーターと DNS サーバーの構築を主たる目標とすることにした。

講義内容の修得状況の確認として、授業時間中の演習以外に、学生の自習環境を用意する必要があったが、ルーターも DNS サーバーも、インターネットに直接接続している既存のネットワーク上で、初学者に教員が直接監督することなく関連作業をさせることは極めて危険である。一方で自習専用の閉じたネットワークを物理的に構築することは、確保可能なスペースの問題で不可能だった。

2. 仮想化を利用したシンクライアントシステム

岡山理科大学理学部応用数学科には学生が常時自由に利用できる計算機室があって、そこでは仮想化ソフトウェアの VMware[1] を利用したシンクライアントシステム[2] が稼働している。

複数の授業や学生の自習に利用することを想定しているために、各クライアントコンピューターで起動する VMware のゲスト OS を、利用者が複数の候補から選択することが可能になっており、さらにネットワーク環境を利用者毎・起動されるゲスト OS 毎に変えることが可能になっている。



3. 仮想化を利用した閉じたネットワーク

OpenVPN[3] という VPN 構築用のフリーソフトウェアが存在する。一般的な VPN ソフトウェアは IP による

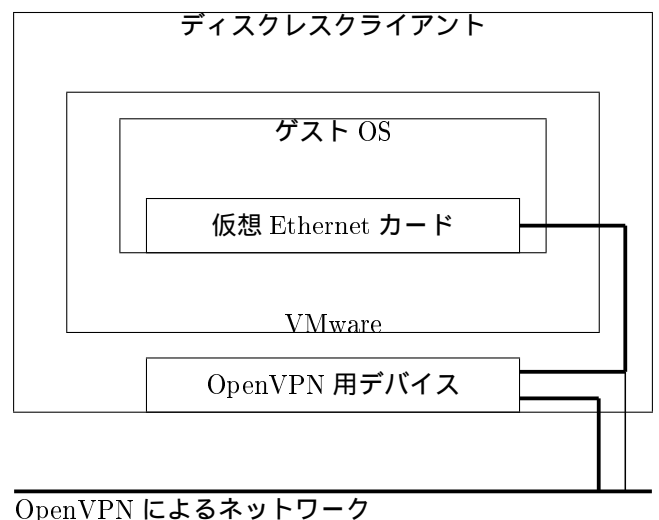
通信のみのトンネルにしか対応していないことが多いが、OpenVPN の特徴の 1 つとして bridged ネットワークのサポートが挙げられる。これは単純化して言えば、IP のデータを実際に運んでいる Ethernet 等の物理層に相当するネットワークを、既存の IP ネットワーク上に仮想的に構築できるということである。

また一般的な VPN ソフトウェアは 1 対 1 の通信路しかサポートしていないことが多いが、OpenVPN は 1 個のサーバーと複数のクライアント間の VPN を構築することができる。この場合サーバー役の OpenVPN は仮想的なハブとして働く。

OpenVPN の上記 2 つの特徴によって、広域ネットワークに接続する LAN、という一般の LAN にルーターを設置する時の状況が、仮想的に再現できることになる。

ただしこれだけでは、ネットワークデバイスがトンネル用の仮想デバイスであることを常に意識しなければならず、初学者向けの環境としてはやや物足りない。さらに本物のネットワークと同一ホストの同一 OS でネットワークの設定変更可能な権限を、十分なスキルを持たない利用者に与えることは、管理者サイドからみれば非常に危険である。また利用者にとっても自分の作業の影響範囲を見積ることができず、安心して作業に集中することができない。

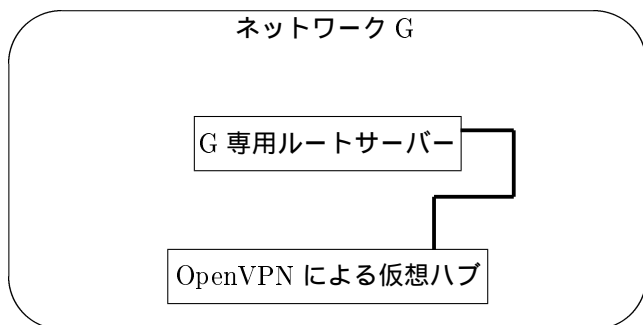
しかし OpenVPN による仮想ネットワークと、シンクライアントシステムに用いている VMware の、任意の bridged ネットワークデバイスをゲスト OS の Ethernet カードに見せ掛ける機能を組み合わせると、利用者には完全に Ethernet にしか見えないネットワーク環境が出来る。



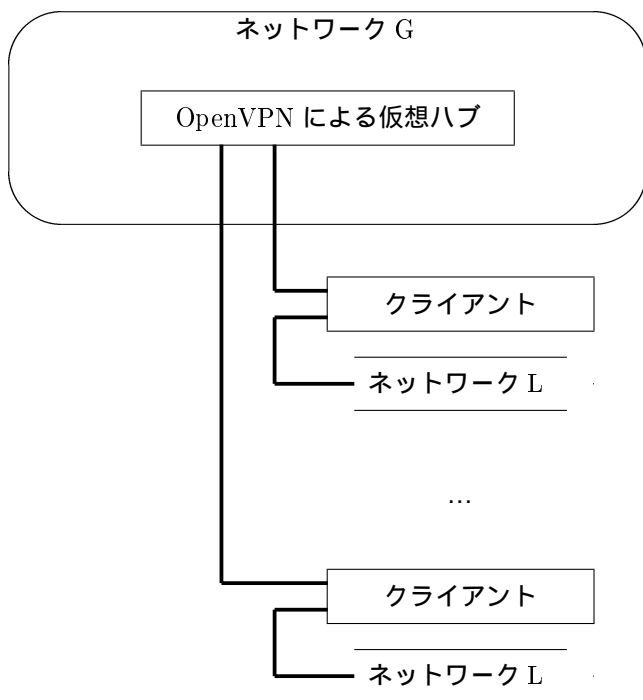
さらに利用者の権限をゲスト OS 内に閉じ込めることで、利用者がどんな作業をしても、その影響が既存のネットワークに及ばないようにすることができる。

4. 自習環境への応用

あらかじめ 1 対多通信用の OpenVPN サーバーを起動しておく。以下、このサーバーをハブとする仮想ネットワークを G とする。また DNS のキャッシュサーバーの構築の学習のために、このネットワークに接続している 1 つのホスト上で、DNS サーバーを稼働させておき、アクセス制御機能を利用して、G や下記のクライアント個別の仮想ネットワーク L からの問い合わせに対してのみルートサーバーとして答えるように設定しておく。



計算機室のクライアントの利用者がネットワーク管理作業学習用のゲスト OS を選択し起動すると、まず G に接続される。さらに利用者毎に異なる別の仮想ネットワーク (以下 L とする) が新たに構築される。



ルーター構築の学習時には G と L の 2 つのネットワークに接続するネットワークデバイスの設定や、その間の

データグラムを中継するための経路表の設定等を行うことになる。

DNS サーバー構築の学習時には、広域ネットワークを模する G と LAN を模する L の 2 つのネットワークが存在することで、権威サーバーとキャッシュサーバーを個別に構築し、それぞれに必要なアクセス制御について実際的な体験ができる。

受講生に期待される予備知識と、講義時間中に可能な作業量による制限から、現行では上のような構成を取っているが、さらに複雑にも単純にも変更することが可能である。例えば、上の G に相当するネットワークを複数個構築し、広域バックボーンネットワークにおけるルーティングについて、gated のようなルーティングデーモンを実際に稼働させて学習するような応用も考えられる。

5. 自習環境の利用状況

基本的には授業時間内のみで完結するように講義スケジュールを組み立てており、講義中に必ず自習せよと指示しているわけではないが、履修している学生のほとんどが授業時間外に自発的に演習の課題の復習に取り組むようになった。自習しない学生と単位を取れない学生はほぼ一致している。

ネットワーク管理という危険な作業を、初学者でも安全に実行できる環境を与えることで、自習のための障害を取り除き学習効果を高められたのではないかと考えている。

6. 改善すべて点

自習環境のネットワークが既存のネットワークから完全に切り離されているので、WWW 上の情報を自習時に自分で調べるためには、一旦自習環境を終了するか 2 台のクライアントを占有するかして、既存のネットワークに接続している環境を別に立ち上げる必要がある、という無駄が生じている。安全性を確保しつつインターネットの情報を取得できるようになれば、学生にとっては利便性が増し学習意欲も向上すると思われる。

参考文献

- [1] VMware Inc., VMware, <http://www.vmware.net/>.
- [2] 須藤 清一, 森 義之, 汎用 PC をシンクライアント化することによる、安全かつ多目的なコンピュータ利用環境, OUS フォーラム 2005.
- [3] OpenVPN Technologies Inc., OpenVPN - Open Source VPN, <http://openvpn.net/>.