

コミュニケーション
第13研究室
卒業研究発表

1ADT1320

菅田 宙央

○研究目的

- LANは現在、大手企業においてほぼ100%、中小企業においても年々導入率は高まる傾向にある。
- LANとは限られたスペースに敷設される小規模なネットワークを意味するが、これが敷設されると次には遠隔地に敷設されたLAN同士の相互的な接続環境へのニーズが高まる。
- 今回はVPNを利用し、リモートアクセスによる外部からLAN内の周辺機器を扱う為の構成を検討する。



- 今回は、
YAMAHA RTX1000
というルータの機能を用い、
PPTPによるリモートアクセ
スVPNを形成する。

VPNとは

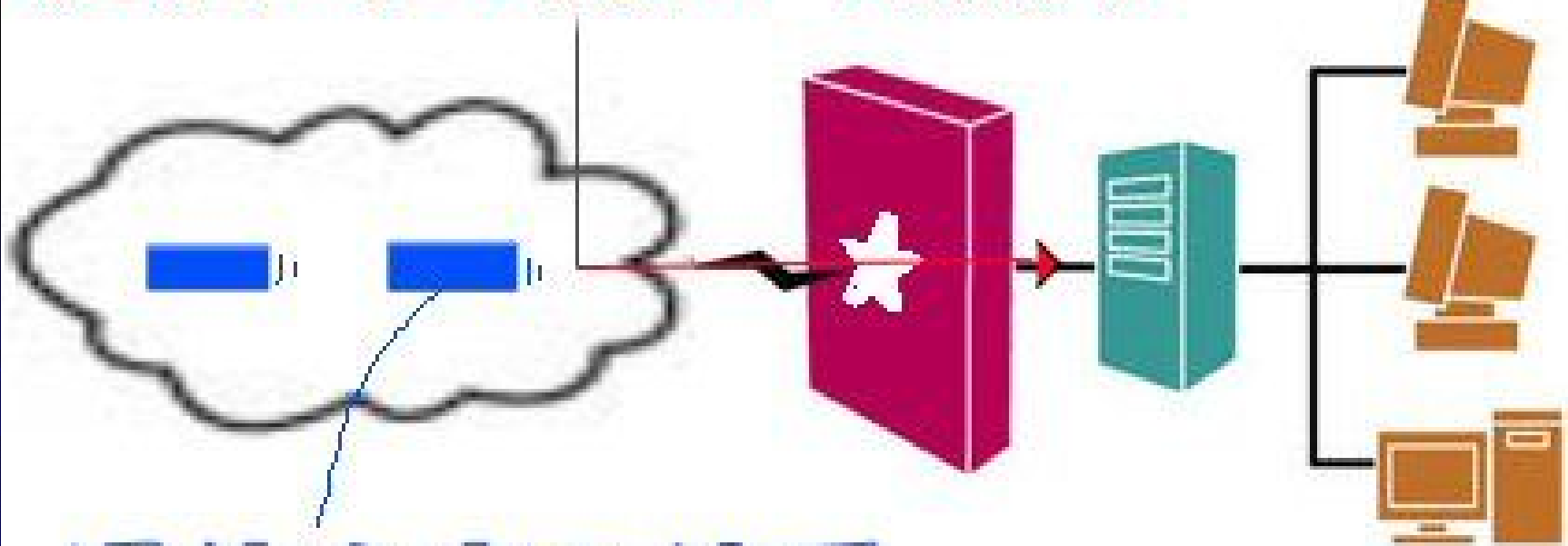
- Virtual Private Network (仮想専用線)。
- 多くのユーザーによって利用されるネットワークを用いつつ、専用回線のように排他的なネットワークを構築する技術。
- トンネリングや暗号化などといった技術を用いる。
- 比較的安価でセキュリティの高いネットワークを実現する事ができる。
- 家庭と企業を結ぶなど、離れた既存のLAN同士を結んで運用する事ができる。

トンネリング・暗号化

- ファイアウォール下のLANの内と外とで通信する場合に大切なことは、
 - ・ 通信内容を読み取られないようにすること
 - ・ 不必要な通信を受け取らないことである。

無防備な通信

通信時の孔から侵入

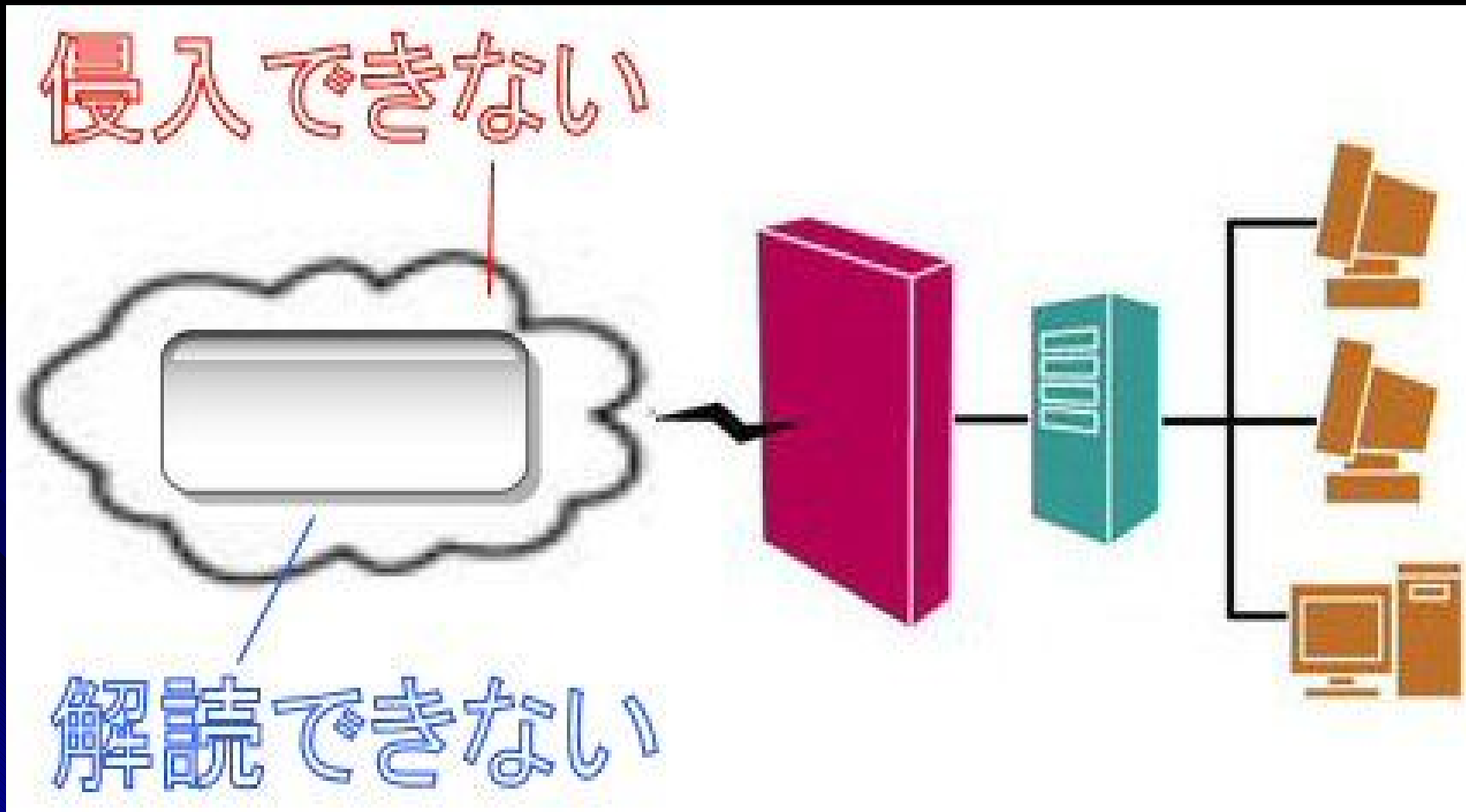


通信内容を傍受

トンネリング・暗号化

- そのためにVPNで用いられるのが、
 - ・ 本来のデータの上に更に別のプロトコルのパケットで覆って包んでしまうカプセル化。
 - ・ 鍵をかけて開けないようにする暗号化。
- これらの処理により、端点同士が直結する専用線のような環境＝トンネリングを形成することができる。

トンネリング形成



PPTP (Point to Point Tunneling Protocol)

- PPTPとは、レイヤー2のデータリンク層で動作するトンネルのVPNプロトコルのこと。
- PPTPトンネルは、拡張GRE (Generic Routing Encapsulation) ヘッダを使ったIPのカプセル化をおこなっていて、PPTPによる通信を行う場合はまず制御コネクションを張り、その後IPトンネルを生成する。
- Microsoft社によって提案され、同社のWindowsNTシリーズには標準でPPTPの機能が付属する。

イーサアクセスVPNルーター YAMAHA RTX1000

- 最大100Mbit/sの高速アクセス性能と回線自動バックアップ機能を1台で実現
- VPN機能
- ■希望小売価格
<税込>123,900円
(本体価格 118,000円)
- 都内某所の平日売りで79,800円



RTX1000によるVPNの構築

- NATを張り、外からLAN内を見られなくする。
【Network Address Translationネットワーク・アドレス変換：組織内でのみ通用するIPアドレス(ローカルアドレス)と、インターネット上のアドレス(グローバルアドレス)を透過的に相互変換する。】
- PPTPのanonymous設定を行い、クライアント側からのIPを問わずアクセスできるVPN環境を作る。
- LAN内のLAN内の周辺機器を使用できるようにする。
- 今回の周辺機器にはプリンタを使う。

使用プリンタ



- Canon
Satera N2100
- 現在印刷機としては、使用不能
- ただしネットワークプリンタとしてはポートも開き、通信時の反応もあるため実験に使用。
- 定価：¥186,900（税込）
- 現在製造中止

プリンタのIPとポート番号

標準 TCP/IP ポート モニタの構成



ポートの設定

ポート名(P): IP_192.168.1.51

プリンタ名または IP アドレス(A): 192.168.1.51

プロトコル

Raw(R)

LPR(L)

Raw 設定

ポート番号(N): 9100

LPR 設定

キュー名(Q):

LPR バイト カウントを有効にする(B)

SNMP ステータスを有効にする(S)

コミュニティ名(C): public

SNMP デバイス
インデックス(D): 1

OK

キャンセル

設定: フィルタリング & IPマスカレード

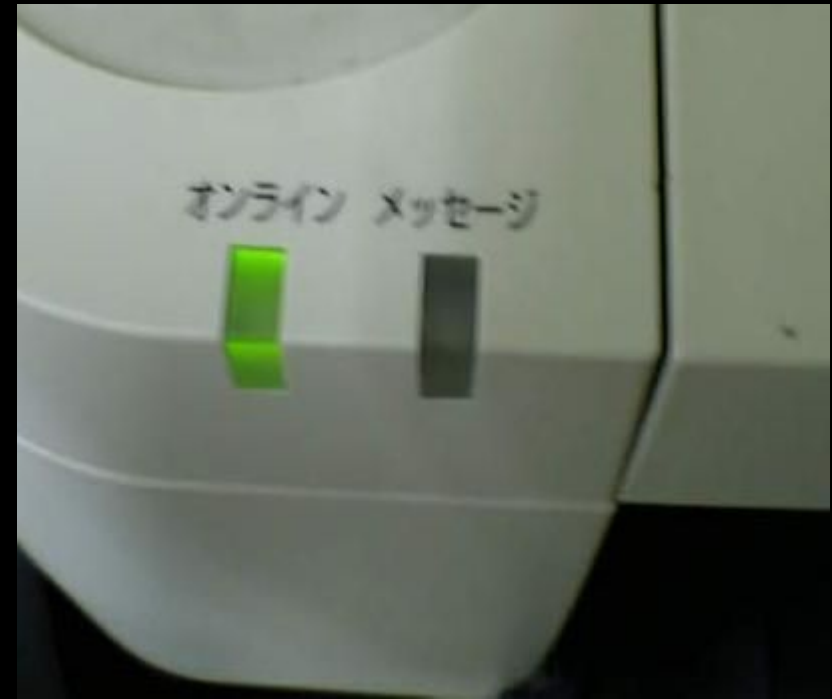
```
C:\ Telnet 192.168.1.1
ip filter 101080 pass * 192.168.1.1 gre * *
ip filter 101081 pass * 192.168.1.1 tcp * 1723
ip filter 101099 pass * * * * *
ip filter 500000 restrict * * * * *
nat descriptor type 1 nat-masquerade
nat descriptor address outer 1 primary
nat descriptor address inner 1 192.168.1.1-192.168.1.254
nat descriptor masquerade static 1 2 192.168.1.70 tcp 21
nat descriptor masquerade static 1 3 192.168.1.70 tcp 22
nat descriptor masquerade static 1 4 192.168.1.70 tcp smtp
nat descriptor masquerade static 1 5 192.168.1.70 tcp www
nat descriptor masquerade static 1 6 192.168.1.70 tcp pop3
nat descriptor masquerade static 1 20 192.168.1.70 tcp ftpdata
nat descriptor masquerade static 1 21 192.168.1.70 tcp telnet
nat descriptor masquerade static 1 30 192.168.1.1 tcp 1723
nat descriptor masquerade static 1 31 192.168.1.1 gre
nat descriptor masquerade static 1 50 192.168.1.13 tcp 12865
nat descriptor masquerade static 1 51 192.168.1.13 udp 12865
nat descriptor masquerade static 1 60 192.168.1.51 tcp 9100
nat descriptor masquerade static 1 61 192.168.1.51 udp 9100
```

設定: pptp & tunnel

```
C:\ Telnet 192.168.1.1
pp select anonymous
pp bind tunnel1
pp auth request mschap-v2
pp auth username vpntest vpntest
ppp ipcp ipaddress on
ppp ipcp msexp on
ppp ccp type mppe-any
ppp ccp no-encryption reject
ip pp remote address pool 192.168.1.175
ip pp mtu 1280
ip pp secure filter in 6714
ip pp nat descriptor 1
pptp service type server
pp enable anonymous
tunnel select 1
tunnel encapsulation pptp
tunnel enable 1
```

実験

- ・natを張らない状態
- ・natを張った状態
- ・natかつvpnを張った状態
- それぞれの状態について、LAN外からアクセスしたときの反応を調べる。

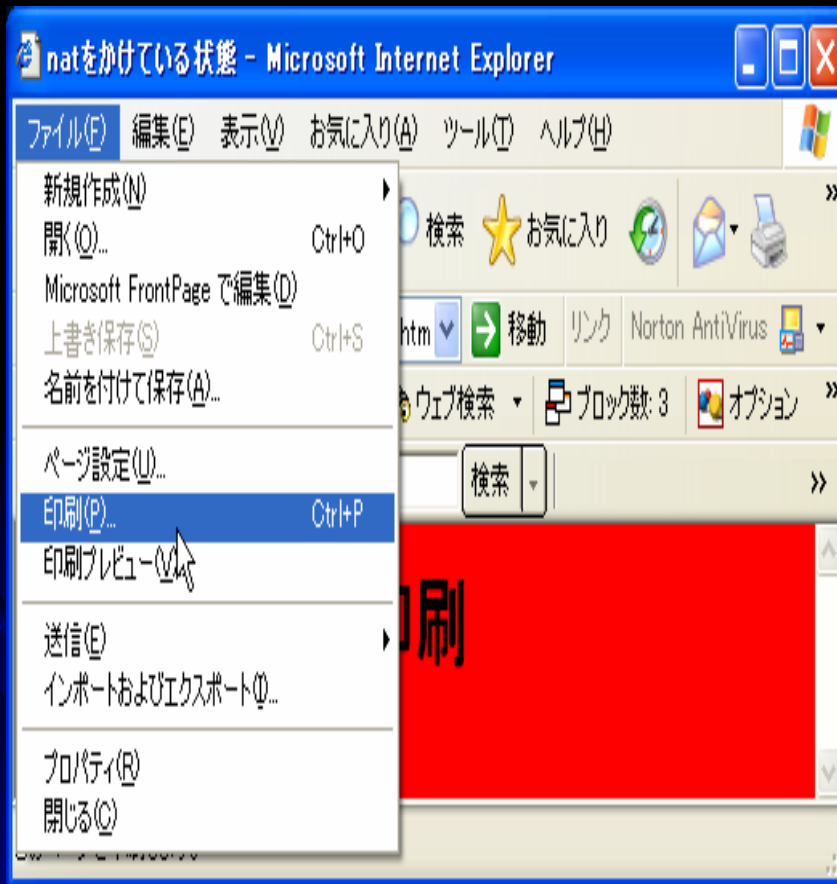


natを張らない状態

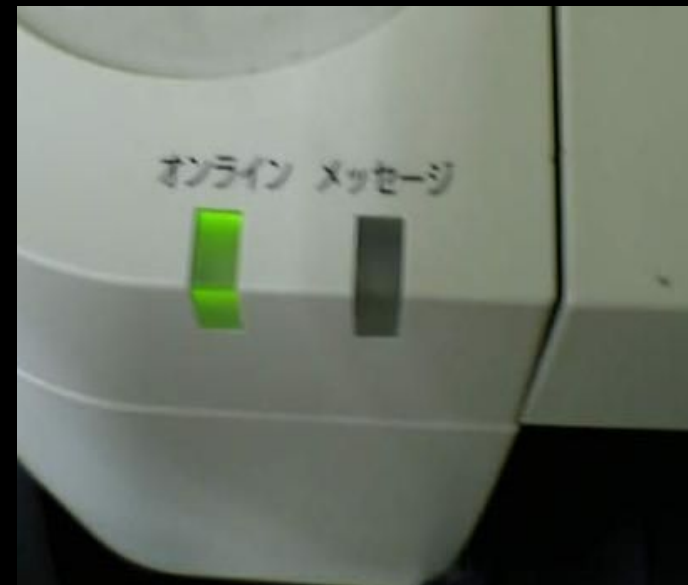


⇒反応あり。
プリンタを使用できる。

natを張った状態




⇒プリンタに反応なし。
データを送れず、使用
不可能。



WindowsXPからPPTP接続

vpnr1 ^ 接続



ユーザー名(U): vpntest

パスワード(P): *****

次のユーザーが接続するとき使用するために、このユーザー名とパスワードを保存する(S):

- このユーザーのみ(N)
- このコンピュータを使うすべてのユーザー(A)

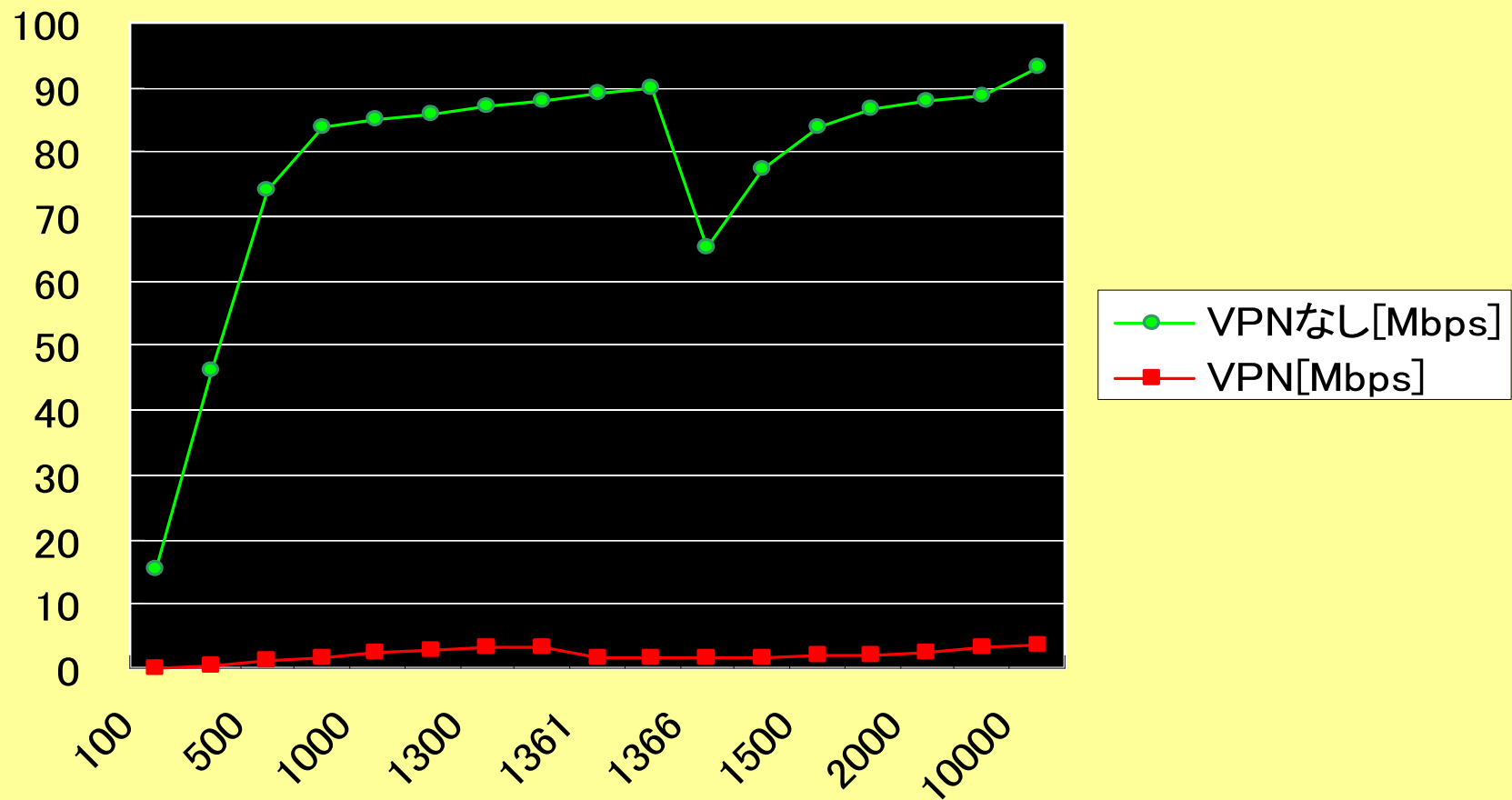
接続(C) キャンセル プロパティ(O) ヘルプ(H)

natかつvpnを張った状態



⇒反応あり。
プリンタを使用できる。
⇒LAN内と直接つながっているような状況に

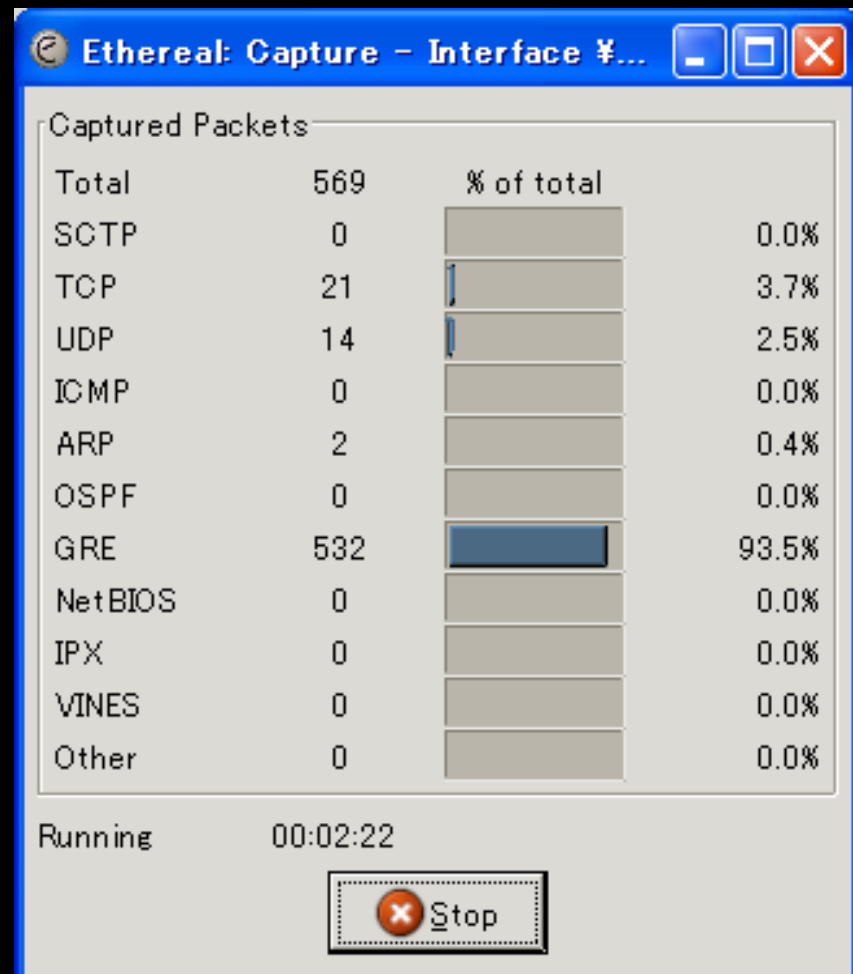
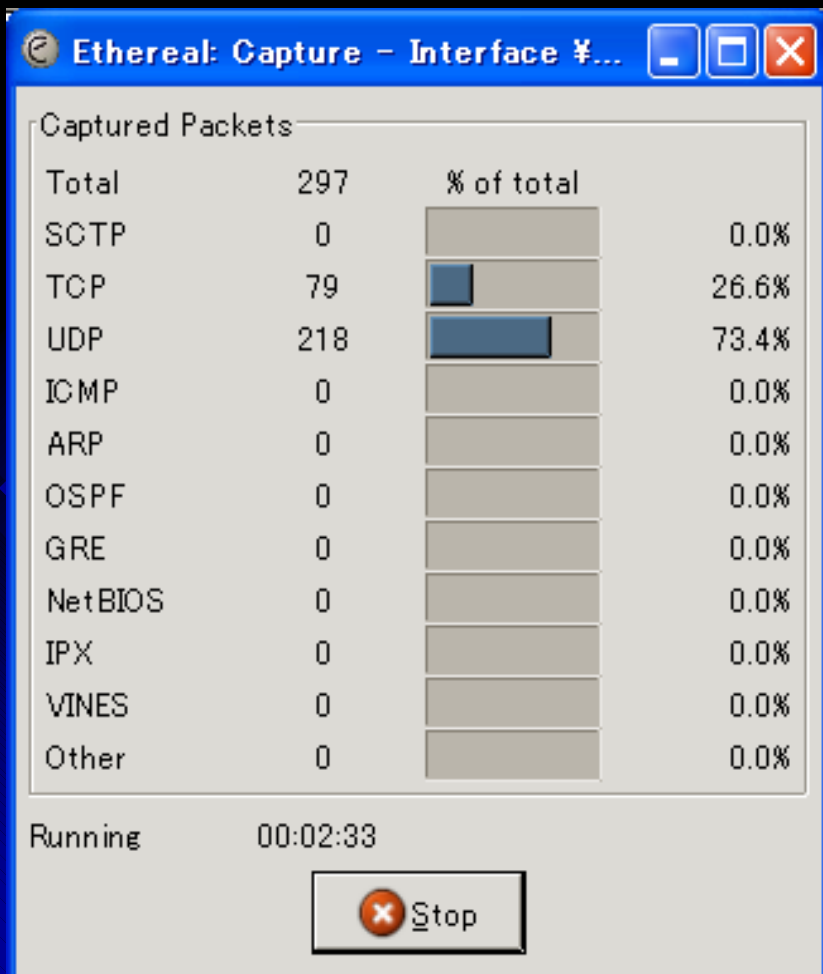
スループット比較



使用プロトコル比較 (etherealによる)

- natを張らない状態

- natかつvpnを張った状態



考察

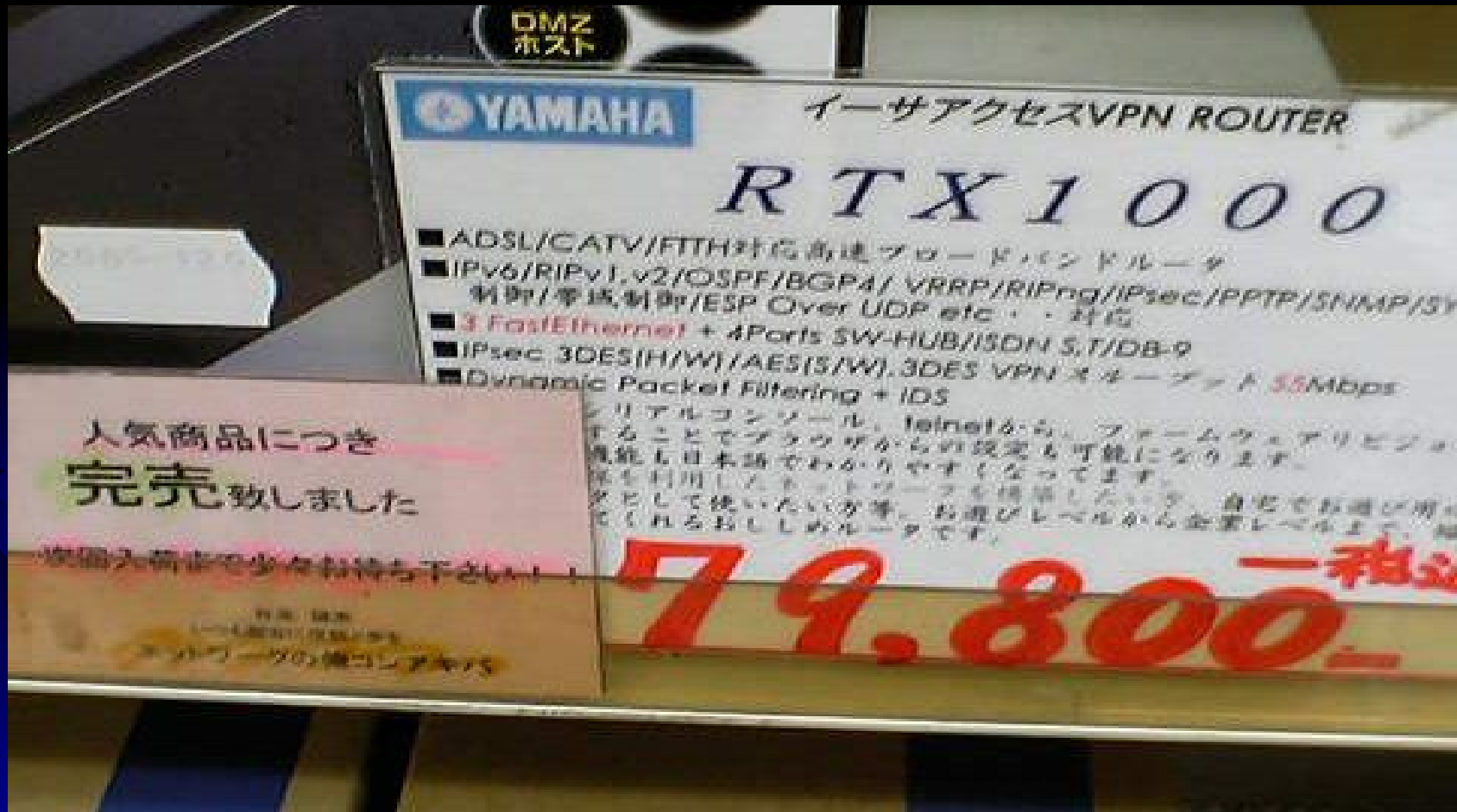
- 実験結果により、LAN外からプリンタという一製品ではあるが、周辺機器を扱うシステムを構築できた。
- ソフトウェアによる処理のため、動作速度は格段に遅くなる。
⇒他のVPNソフトや、ルータ等のハードウェアによる高速化の検討も考えられる。
(体感的には、プリンタ程度ではそれほど高速の通信は必要ないように思われた)

謝辞

- 今回の実験に際し、アドバイスや機器の使用など、周囲の方々のご助力を賜り、まことに感謝しています。

ちなみに

- 週末に確認しに行ったのですが



売り切れてました。