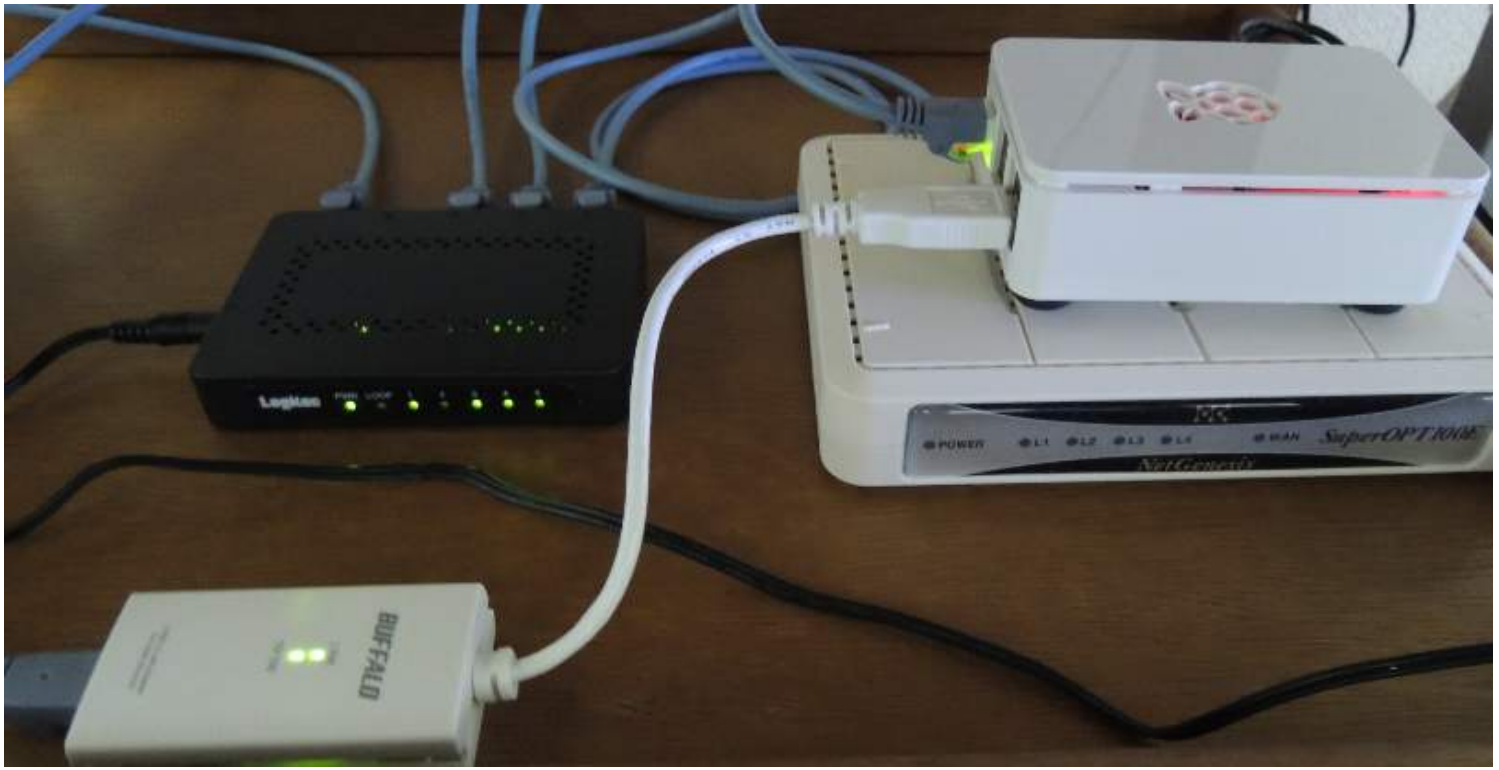
ブロードバンドルーターの構築

- Raspberry Pi 2 Model B＋Raspbianによる
  有線ブロードバンドルーター構築ログ

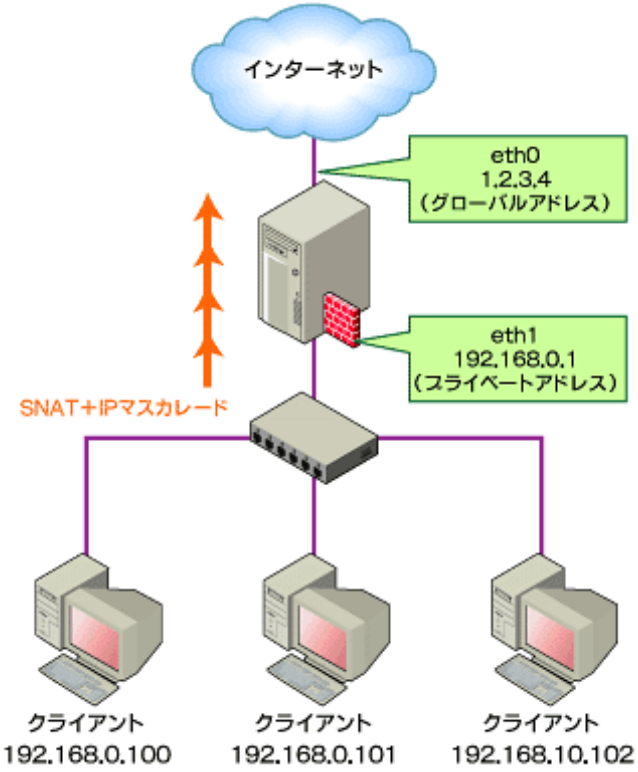


必要な機能

①. PPPoEによるインターネットへの接続機能

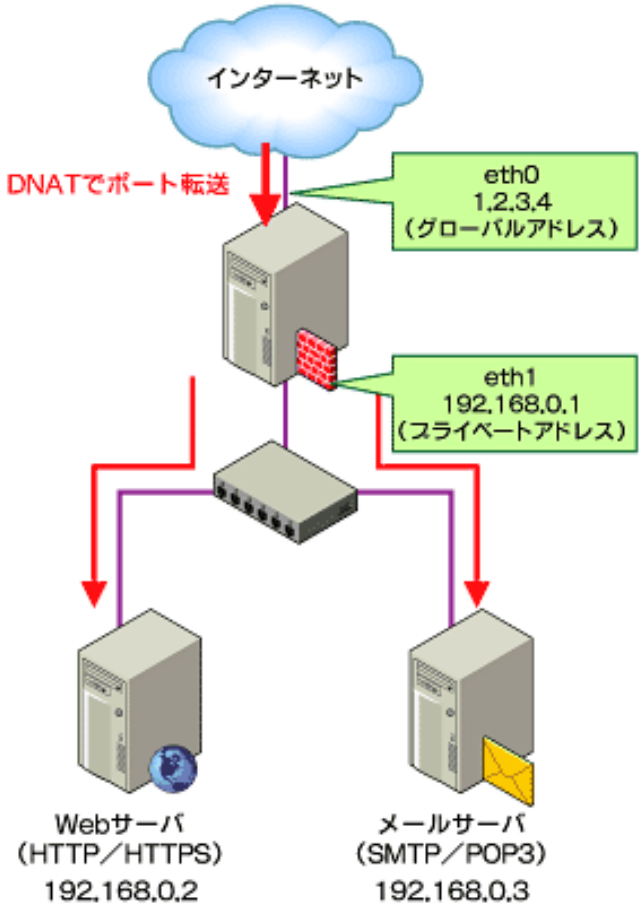
②. IPアドレス変換（Source NAT＋IPマスカレード）機能

③. IP パケット・フィルター・ファイアウォール機能



④. LAN内のサーバー公開（Destination NAT)機能

LAN内に設置したmail,Web,VPNサーバが外部と直接通信できるように必要なポートにつきアドレス変換。



⑤. DHCPサーバ機能

DHCPクライアント（IPアドレス自動割付）として接続されたパソコンやタブレット等にIPアドレス，デフォルトゲートウエイ，DNSサーバ情報などを付与。

⑥. DNSキャッシュサーバ機能

ルーターがLAN側専用のDNSサーバとして動作する機能。

⑦. NTPサーバ機能

ルーターがLAN側専用のNTPサーバとして動作する機能。

追加ハードウエア

- WAN側のLANコントローラーとしてUSB LANアダプター LUA3-U2-ATXを選定

ソフトウエア

機能	追加パッケージ	備考
PPPoE	pppoe PPP over Ethernet driver	/usr/sbin/pppd /usr/lib/pppd/2.4.6/ （rp-pppoe.so他）
	pppoeconf PPP認証、インタフェース初期設定ツール	
Source NAT	無し （OSの機能を利用）	カーネル組込Netfilter
パケットフィルタファイアウォール		
Destination NAT		

ソフトウエア（続き）

機能	追加パッケージ	備考
DHCPサーバ	dnsmasq	50台以下のコンピュータが繋がったネットワークでの使用を想定して作られた軽量なDNSキャッシュ＆DHCPサーバ
DNSキャッシュサーバ		
NTPサーバ	無し （OSの機能を利用）	OS標準装備 /usr/sbin/ntpd

pppoeconf を用いた PPPoE 接続設定

- pppoeconf は PPPoE 接続を対話式で設定

ファイル	機能
/etc/ppp/peers/dsl-provider	pppoeconf がpppoe に合わせて生成した pppd の設定ファイル
/etc/ppp/options	pppd のための一般的な実行パラメータ
/etc/ppp/pap-secret	PAP のための認証データ
/etc/ppp/chap-secret	CHAP のための認証データ

PPPoEのオプション設定

/etc/ppp/options

- persist

  常時接続設定

（リンクダウンした場合に自動で再接続）

- maxfail 0

  リンクダウンした場合の再接続リトライ回数＝∞

dnsmasqの設定

/etc/dnsmasq.conf

```
interface=eth0
dhcp-range=192.168.1.20,192.168.1.40,12h
dhcp-option=option:netmask,255.255.255.0
dhcp-option=option:router,192.168.1.254
dhcp-option=option:dns-server,192.168.1.254,8.8.8.8
```

dnsmasq関連ファイル

/etc/resolve.conf　　（ppp接続時自動更新）

nameserver 202.238.95.9

nameserver 202.238.95.22

/etc/hosts　　（予め用意）

127.0.0.1　　localhost

192.168.1.254　gw.xxx.yyy

192.168.1.1　　host1.xxx.yyy

192.168.1.2　　host2.xxx.yyy

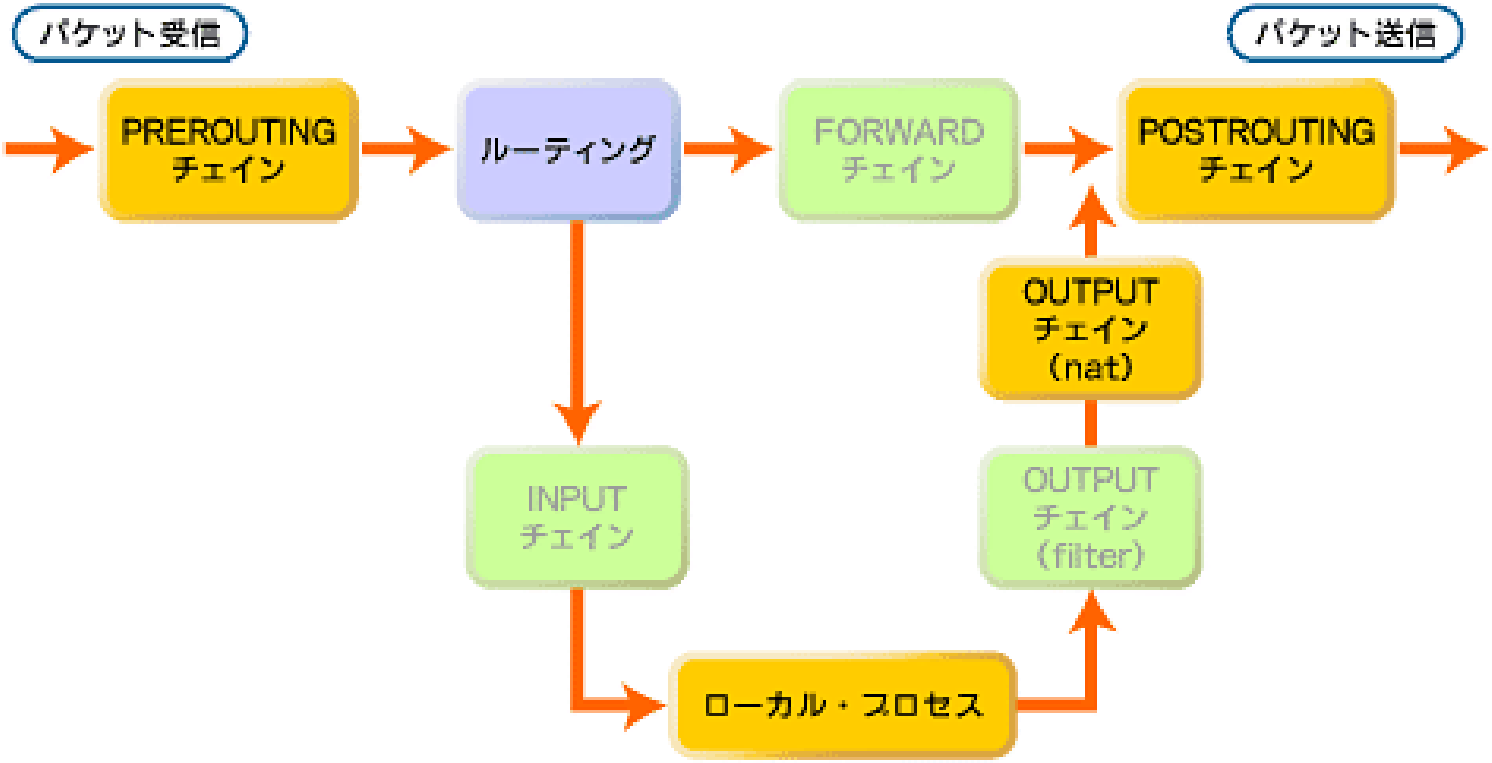
Netfilterの設定

- 表に基き、**iptables**コマンドによる設定スクリプトを作成

項目	内容
パケットフィルタ INPUTチェイン	ESTABLISHED,RELATEDの通信及び LAN側からのアクセスのみ許可。
パケットフィルタ OUTPUTチェイン	LAN側IPアドレス宛てのパケットは許可。 内部アドレスやプライベートアドレスが外部ネットワークに漏れないようにブロック。
パケットフィルタ FORWARDチェイン	LAN側IPアドレス宛てのパケットはステートフル性を確認し、 「--state　ESTABLISHED,RELATED」となっているものに通過許可 。

項目	内容
パケットフィルタ FORWARDチェイン	Windowsファイル／プリンタ共有機能で利用されるパケットとRPCパケットをブロック。
POSTROUTINGチェイン （Source NAT）	内部ネットから外部ネットへ出ていくパケットのソースIPを書き換える。（IPマスカレード ）
PREROUTINGチェイン （Destination NAT）	サーバをLAN側に設置したまま、外部ネットから接続できるようポート転送を行う。 HTTP／HTTPS／SMTP／POP3S／Submission等をサーバー宛にポート転送。 VPNパススルー関連等をポート転送。

filter＋natテーブルの構造



・**PREROUTINGチェイン**
ディスティネーションアドレスの書き換え／DNAT
・**POSTROUTINGチェイン**
ソースアドレスの書き換え／SNAT
・**OUTPUTチェイン**
ローカルで生成されたパケットのディスティネーションアドレスの書き換え／DNAT

iptablesコマンドによる設定スクリプトイメージ

```
#! /bin/sh
↓
local_net='192.168.1.0/24'
my_local_ip='192.168.1.254'
my_test_ip='192.168.1.253'
↓
WAN='ppp0'
LAN='eth0'
↓
#echo 1 > /proc/sys/net/ipv4/ip_forward
↓
###############
#Flush & Reset
###############
iptables -F
iptables -t nat -F
iptables -X
↓
###############
#Deafult Rule
###############
iptables -P INPUT DROP
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -i $LAN -s $local_net -d $my_local_ip -j ACCEPT
iptables -A INPUT -i $LAN -s $local_net -d $my_test_ip -j ACCEPT
↓
#DHCP permission
iptables -A INPUT -i $LAN -p udp --dport 67:68 --sport 67:68 -j ACCEPT
↓
iptables -P OUTPUT ACCEPT
↓
iptables -P FORWARD DROP
iptables -A FORWARD -i $LAN -o $WAN -s $local_net -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
↓
##################
#VPN pass-through
##################
iptables -A FORWARD -i $WAN -o $LAN -p esp -j ACCEPT
```

INPUT チェイン

- 基本は全て廃棄

  iptables -P INPUT DROP

- ESTABLISHED,RELATEDの通信は許可

  iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

- LAN内のクライアントからのDHCP要求は許可

  iptables -A INPUT -i $LAN -p udp --dport 67:68 --sport 67:68 -j ACCEPT

OUTPUT チェイン

- 基本は全て許可

  iptables -P OUTPUT ACCEPT

- 内部アドレスやプライベートアドレスが外部ネットワークに漏れないようにブロック

  iptables -A OUTPUT -o $WAN -d 192.168.0.0/16 -j DROP

  iptables -A OUTPUT -o $WAN -d 127.0.0.0/8 -j DROP

FORWARD チェイン 1

・基本は全て廃棄

iptables -P FORWARD DROP

・Windowsファイル・プリンタ共有 関連は外部に出さない

iptables -A FORWARD -p tcp -i $LAN -o $WAN --dport 137:139 -j DROP

iptables -A FORWARD -p udp -i $LAN -o $WAN --dport 137:139 -j DROP

iptables -A FORWARD -p tcp -i $LAN -o $WAN --dport 445 -j DROP

iptables -A FORWARD -p udp -i $LAN -o $WAN --dport 445 -j DROP

FORWARD チェイン ２

・LAN内から外部（WAN）への接続は制限しない。

```
iptables -A FORWARD -i $LAN -o $WAN -s $local_net -j
ACCEPT
```

・ESTABLISHED,RELATEDの通信は許可

```
iptables -A FORWARD -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

FORWARD チェイン ３

・IPsec VPN関連はパススルー

```
iptables -A FORWARD -i $WAN -o $LAN -p esp -j
ACCEPT

iptables -A FORWARD -i $WAN -o $LAN -p ah -j
ACCEPT
```

POSTROUTING チェイン

・SNAT（IPマスカレード）設定

```
iptables -t nat -A POSTROUTING -o $WAN -s
$local_net -j MASQUERADE
```

PREROUTING チェイン

・LAN内のサーバーを公開（DNAT）

```
server_ip='192.168.1.1‘
http_port='80‘

iptables -t nat -A PREROUTING -p tcp -i $WAN --dport 80 -j DNAT
 --to-destination $server_ip:$http_port

iptables -A FORWARD -i $WAN -o $LAN -p tcp -d $server_ip
--dport $http_port -j ACCEPT
```

上記と同様にHTTPS／SMTP／POP3S／Submission
等を公開。

テーブルリスト表示（iptables –L –v）

```
Chain INPUT (policy DROP 100 packets, 9828 bytes)
 pkts bytes target     prot opt in     out     source               destination
50757 6091K ACCEPT     all  --  any    any     anywhere             anywhere            state RELATED,ESTABLISHED
18293 1317K ACCEPT     all  --  eth0   any     192.168.1.0/24       192.168.1.254
   97 38465 ACCEPT     udp  --  eth0   any     anywhere             anywhere            udp spts:bootps:bootpc dpts:bootps:bootpc
    4   480 ACCEPT     all  --  lo     any     anywhere             anywhere

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  eth0   ppp0    anywhere             anywhere            tcp dpts:netbios-ns:netbios-ssn
    3   234 DROP       udp  --  eth0   ppp0    anywhere             anywhere            udp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eth0   ppp0    anywhere             anywhere            tcp dpt:microsoft-ds
    0     0 DROP       udp  --  eth0   ppp0    anywhere             anywhere            udp dpt:microsoft-ds
    0     0 DROP       tcp  --  eth0   ppp0    anywhere             anywhere            tcp dpt:sunrpc
    0     0 DROP       udp  --  eth0   ppp0    anywhere             anywhere            udp dpt:sunrpc
  13M 1909M ACCEPT     all  --  eth0   ppp0    192.168.1.0/24       anywhere
  23M   31G ACCEPT     all  --  any    any     anywhere             anywhere            state RELATED,ESTABLISHED
    0     0 ACCEPT     esp  --  ppp0   eth0    anywhere             anywhere
    0     0 ACCEPT     ah   --  ppp0   eth0    anywhere             anywhere
  194 10728 ACCEPT     tcp  --  ppp0   eth0    anywhere             hmm.blue            tcp dpt:http
   40  2148 ACCEPT     tcp  --  ppp0   eth0    anywhere             hmm.blue            tcp dpt:https
   25  1300 ACCEPT     tcp  --  ppp0   eth0    anywhere             hmm.blue            tcp dpt:5555
    0     0 ACCEPT     tcp  --  ppp0   eth0    anywhere             hmm.blue            tcp dpt:telnets
    8  3776 ACCEPT     udp  --  ppp0   eth0    anywhere             hmm.blue            udp dpt:isakmp
    8   992 ACCEPT     udp  --  ppp0   eth0    anywhere             hmm.blue            udp dpt:ipsec-nat-t
  224 12416 ACCEPT     tcp  --  ppp0   eth0    anywhere             hmm.blue            tcp dpt:smtp
    0     0 ACCEPT     tcp  --  ppp0   eth0    anywhere             hmm.blue            tcp dpt:submission
   18   936 ACCEPT     tcp  --  ppp0   eth0    anywhere             hmm.blue            tcp dpt:pop3s
  244 13776 ACCEPT     tcp  --  ppp0   eth0    anywhere             hmm.blue            tcp dpt:ssh

Chain OUTPUT (policy ACCEPT 3116 packets, 1255K bytes)
 pkts bytes target     prot opt in     out     source               destination
   17  3300 ACCEPT     all  --  any    lo      anywhere             anywhere
    0     0 DROP       all  --  any    ppp0    anywhere             10.0.0.0/8
    0     0 DROP       all  --  any    ppp0    anywhere             176.16.0.0/12
    0     0 DROP       all  --  any    ppp0    anywhere             192.168.0.0/16
    0     0 DROP       all  --  any    ppp0    anywhere             loopback/8
```

インタフェースの自動起動

/etc/network/interfaces

```
auto eth0
iface eth0 inet static
address 192.168.1.254
netmask 255.255.255.0

auto eth1
iface eth1 inet manual
auto dsl-provider
iface dsl-provider inet ppp
pre-up /bin/ip link set eth1 up  # line maintained by pppoeconf
provider dsl-provider
```

カーネルIP経路テーブル

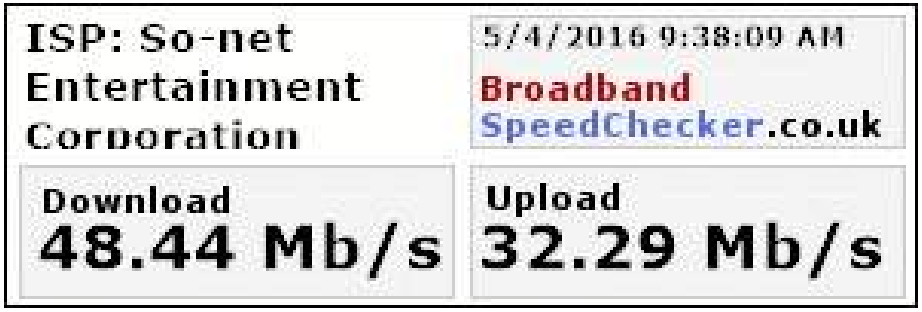
受信先サイト	ゲートウェイ	ネットマスク	フラグ	Metric	Ref	使用数	インタフェース
0.0.0.0	0.0.0.0	0.0.0.0	U	0	0	0	ppp0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
61.211.63.199	0.0.0.0	255.255.255.255	UH	0	0	0	ppp0

ポートスキャン結果

Test result:

```
Starting Nmap 6.00 ( http://nmap.org ) at 2016-04-21 06:10 EEST
Initiating Ping Scan at 06:10
Scanning [redacted] (182.171.221.98) [4 ports]
Completed Ping Scan at 06:10, 0.27s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 06:10
Scanning [redacted] (182.171.221.98) [100 ports]
Discovered open port 443/tcp on 182.171.221.98
Discovered open port 22/tcp on 182.171.221.98
Discovered open port 25/tcp on 182.171.221.98
Discovered open port 995/tcp on 182.171.221.98
Discovered open port 80/tcp on 182.171.221.98
Discovered open port 587/tcp on 182.171.221.98
Completed SYN Stealth Scan at 06:10, 2.70s elapsed (100 total ports)

[+] Nmap scan report for [redacted] (182.171.221.98)

Host is up (0.25s latency).
Not shown: 94 filtered ports

PORT    STATE SERVICE

22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https
587/tcp open  submission
995/tcp open  pop3s


Nmap done: 1 IP address (1 host up) scanned in 3.09 seconds

           Raw packets sent: 202 (8.864KB) | Rcvd: 49 (2.770KB)
```

スループット測定



マイクロリサーチ社製　MR-OPT100Eとの比較で、

同等以上の性能を発揮。

多彩なパケットモニターツール等も使用可能