Vyatta 徹底評価！

浅間 正和(有限会社銀座堂)
谷津 航(株式会社まほろば工房)

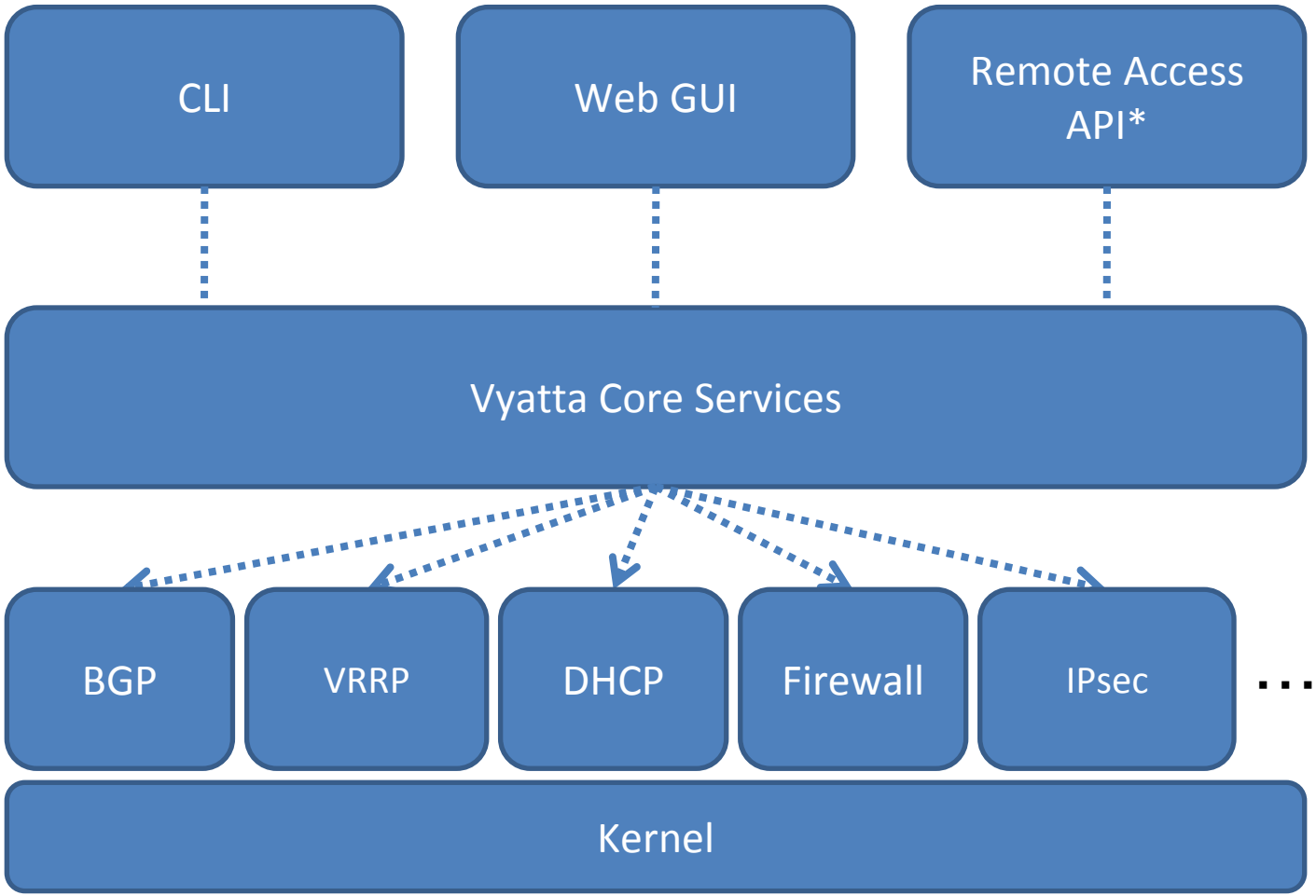
Vyattaとは

Vyattaとは

- Vyatta社曰く、いろいろできるネットワークOSである。
- 仮想/クラウド/物理環境に於いて、
  - ルータができる
  - ファイアウォールができる
  - VPN接続器ができる
  - IPSができる
  - BGPも実装してる
  - DSLから10Gbpsまで対応してる
  - XenやVmware上で動く
  - 冗長機能を持っている
  - etc.

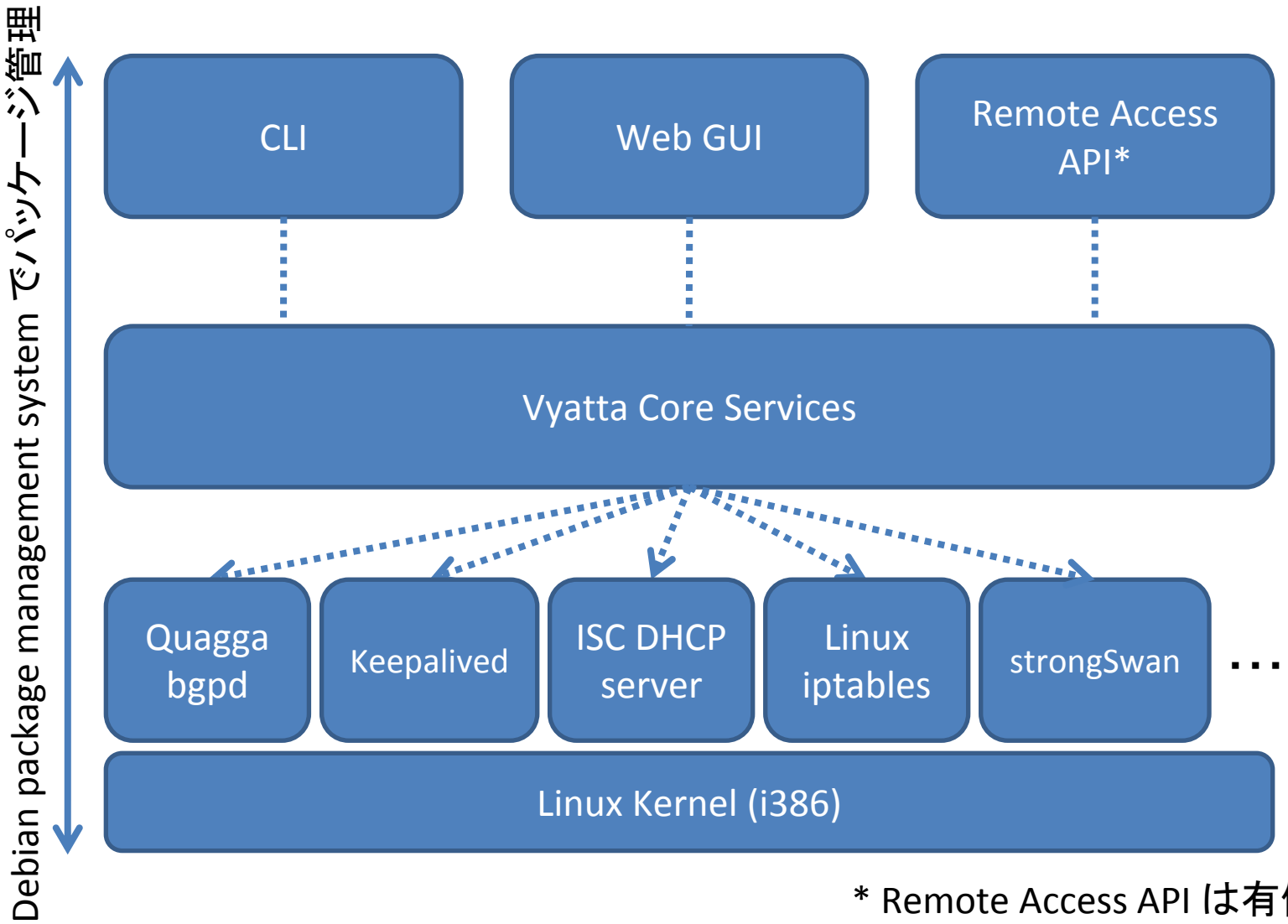
- そんなにすごいのか？

Vyattaの構成



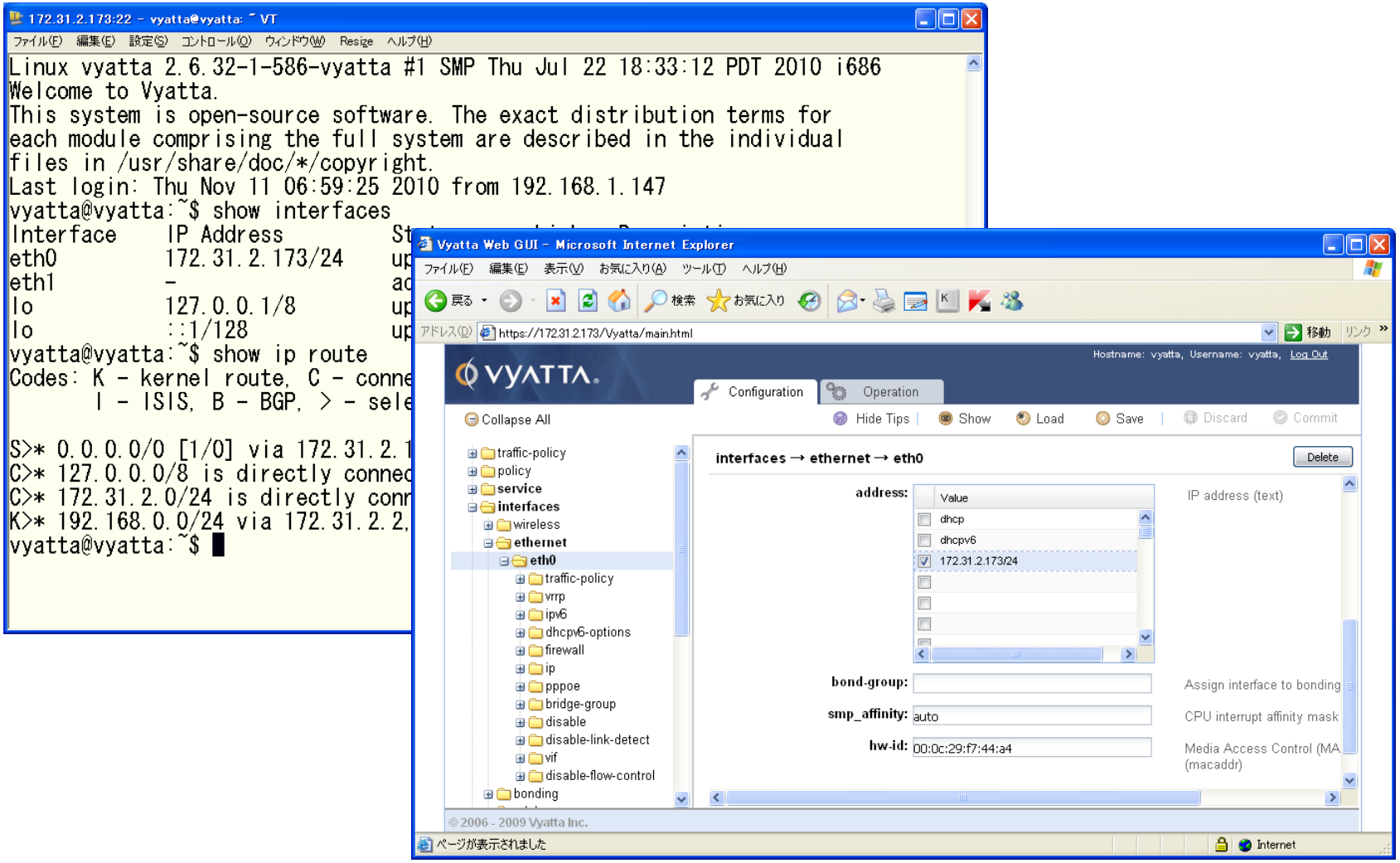
* Remote Access API は有償版のみ

Vyattaの構成



* Remote Access API は有償版のみ

VyattaのUI


172.31.2.173:22 - vyatta@vyatta: ~ VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) Resize ヘルプ(H)
Linux vyatta 2.6.32-1-586-vyatta #1 SMP Thu Jul 22 18:33:12 PDT 2010 i686
Welcome to Vyatta.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
Last login: Thu Nov 11 06:59:25 2010 from 192.168.1.147
vyatta@vyatta:~$ show interfaces
Interface IP Address
eth0 172.31.2.173/24
eth1 -
lo 127.0.0.1/8
lo ::1/128
vyatta@vyatta:~$ show ip route
Codes: K - kernel route, C - conne
I - ISIS, B - BGP, > - sele
S>* 0.0.0.0/0 [1/0] via 172.31.2.1
C>* 127.0.0.0/8 is directly connec
C>* 172.31.2.0/24 is directly conn
K>* 192.168.0.0/24 via 172.31.2.2,
vyatta@vyatta:~$
Vyatta Web GUI - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
https://172.31.2.173/Vyatta/main.html
Hostname: vyatta, Username: vyatta, Log Out
VYATTA.
Configuration
Operation
Collapse All
Hide Tips
Show
Load
Save
Discard
Commit
traffic-policy
policy
service
interfaces
wireless
ethernet
eth0
traffic-policy
vrrp
ipv6
dhcpv6-options
firewall
ip
pppoe
bridge-group
disable
disable-link-detect
vif
disable-flow-control
bonding
interfaces → ethernet → eth0
Delete
address:
Value
dhcp
dhcpv6
172.31.2.173/24
IP address (text)
bond-group:
Assign interface to bonding
smp_affinity:
auto
CPU interrupt affinity mask
hw-id:
00:0c:29:f7:44:a4
Media Access Control (MA
(macaddr)
© 2006 - 2009 Vyatta Inc.
ページが表示されました
Internet

Vyattaの機能

IPv4 / IPv6 Routing	» BGPv4, BGPv6 » OSPFv2, OSPFv3*	» RIPv2 » Static Routes	» IPv6 Policy » IPv6 SLAAC
IP Address Management	» Static » DHCP Server » DHCP Client	» DHCP Relay » Dynamic DNS » DNS Forwarding	» DHCPv6 Server » DHCPv6 Client » DHCPv6 Relay
Encapsulations	» Ethernet » 802.1Q VLANs » PPP	» PPPoE » IP in IP » Frame Relay	» MLPPP » HDLC » GRE
Firewall	» Stateful Inspection Firewall » Zone-based Firewall » P2P Filtering	» IPv6 Firewalling » Time-based Firewall Rules » Rate Limiting	» ICMP Type Filtering » Stateful Failover
Tunneling / VPN	» SSL-based OpenVPN » Site to Site VPN (IPSec) » Remote VPN (PPTP, L2TP, IPSec)	» OpenVPN Client Auto-Configuration » Layer 2 Bridging over GRE » Layer 2 Bridging over OpenVPN	
Additional Security	» Network Address Translation » Sourcefire VRT Intrusion Prevention » VyattaGuard Web Filtering	» DES, 3DES, AES Encryption » MD5 and SHA-1 Authentication » RSA, Diffie Helman Key Mgmt	» NAT Traversal » Role based access control
WAN / LAN Device Drivers	» WAN Device Drivers - ADSL, T1, T3 » Intel 10/100Mbps - 10Gbps	» IEEE 802.11 wireless » Drivers in 2.6.31 Linux Kernel	» Synchronous Serial - V.35, X.21, RS-422, EIA530
Performance Optimization	» WAN Link Load Balancing » Ethernet Link Bonding » Web Caching	» MLPPP » ECMP » Bandwidth Management	
QoS Policies	» Priority Queuing » Network Emulator » Round Robin	» Random / Weighted Random » Classful Queuing » Ethernet Header Matching	» VLAN Tag » IPv6 Address » Port Mirroring
High Availability	» Stateful Firewall / NAT Failover » VRRP » HA Clustering	» Configuration Replication » RAID 1	» IPSec VPN Clustering » Protocol Fault Isolation
Administration & Authentication	» Integrated CLI » Web GUI » Vyatta Remote Access API	» Telnet » SSHv2 / SSH Public Key » Binary Image Install	» RADIUS » TACACS+* » Single Configuration File
Diagnostics & Logging	» tcpdump » Wireshark Packet Capture » BGP MD5 Support	» Serial Loopback Commands » Netflow / sFlow » LLDP	» Syslog » SNMPv2c » SNMP for IPv6

Vyattaの機能

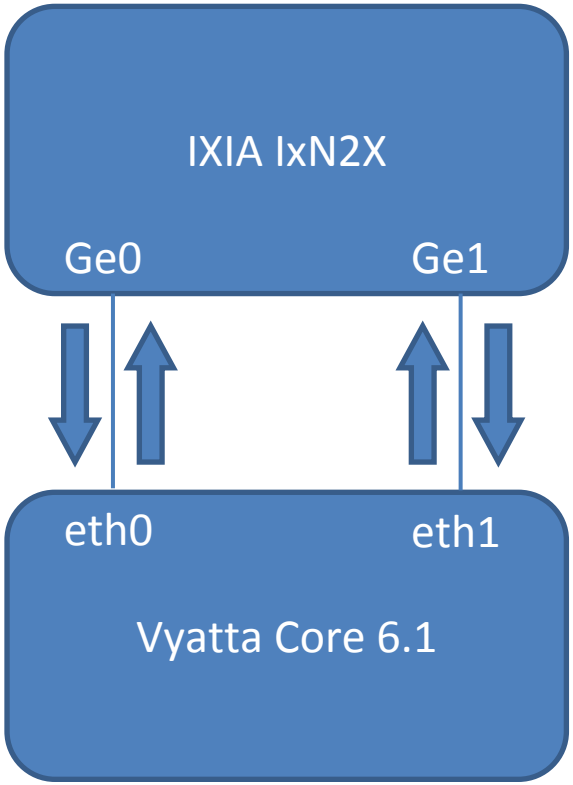
- 機能抜粋(適用例)
  - バックボーンルータとして
    - BGP
    - OSPF
  - ファイアウォールとして
    - NAT
    - Firewall機能(ステートフル)
  - VPN終端器として
    - IPsec

機能は十分に
搭載している

→ IAマシン(VM含む)にVyattaをインストールすると、
ルータの機能・操作性が得られる。

パケット転送性能

測定構成

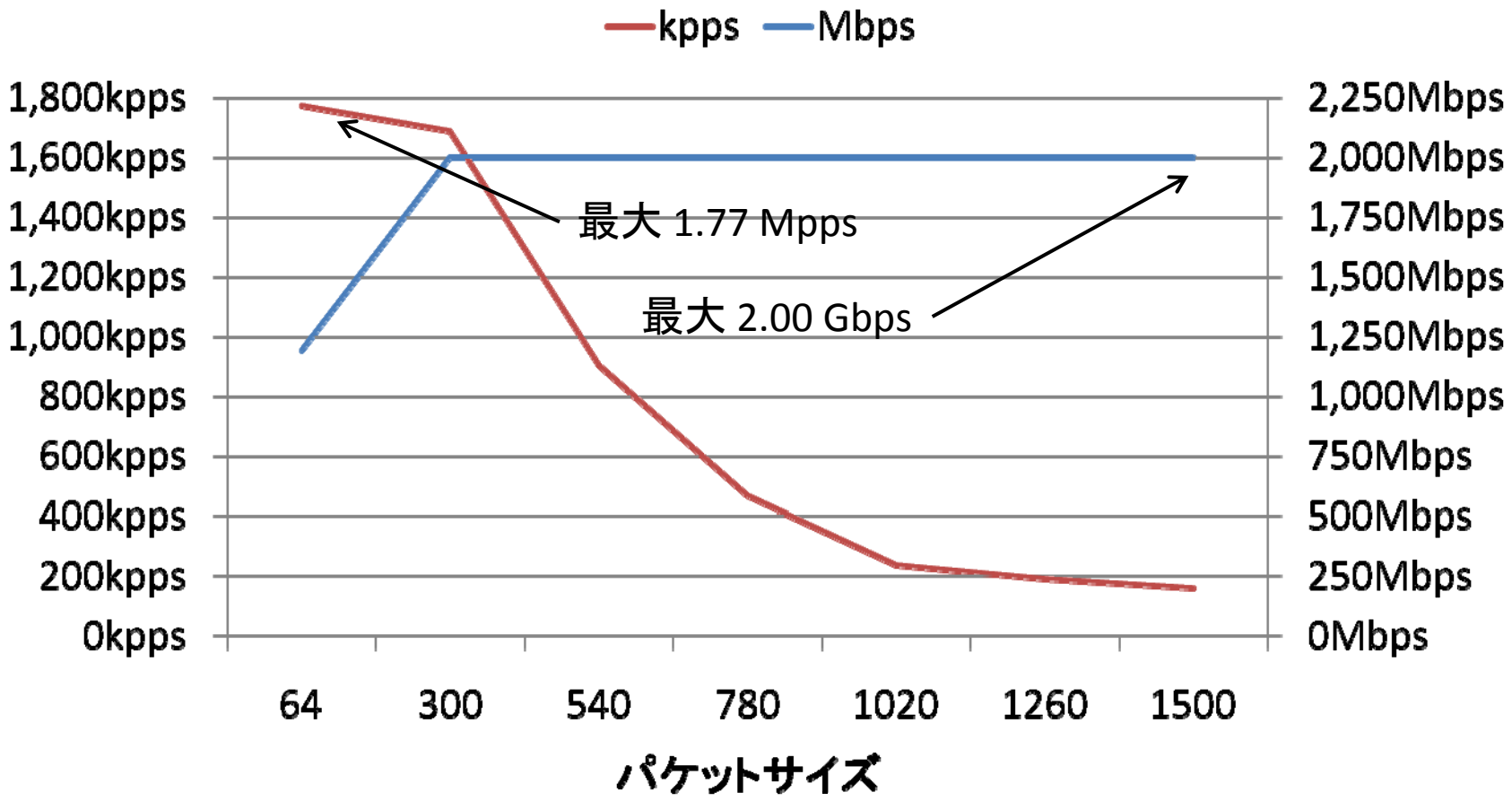


Vyatta Core の H/W 構成

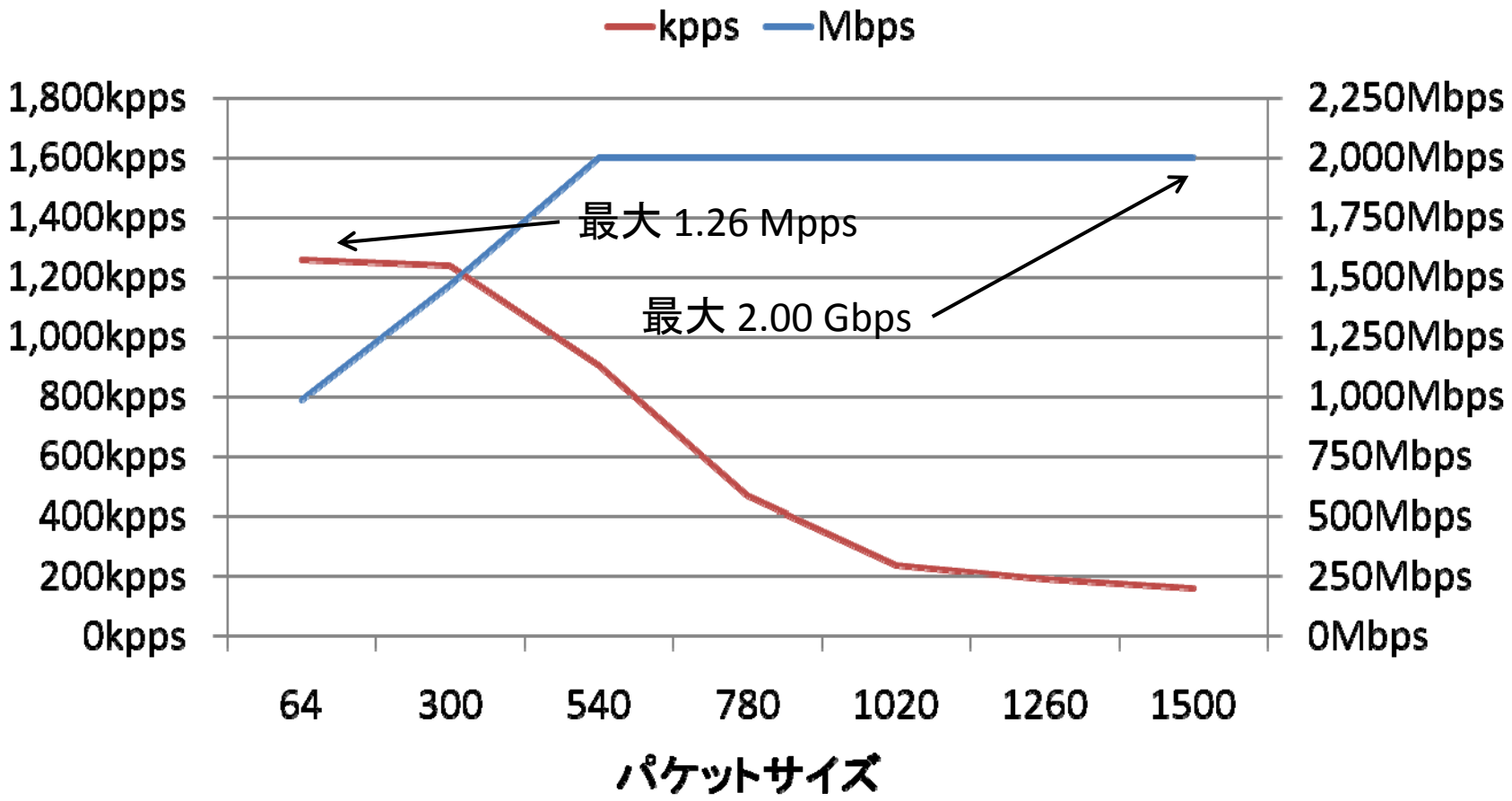
Model	HP DL160 G6
CPU	Xeon E5620 2.40GHz
Memory	DDR3 SDRAM 1333MHz 6GB
NIC	Intel 82576EB Dual Port

宛先アドレス(IPv4)
Ge0→Ge1: 11.0.0.0～11.0.0.255
Ge1→Ge0: 12.0.0.0～12.0.0.255
宛先アドレス(IPv6)
Ge0→Ge1: 2400::～2400::ff
Ge1→Ge0: 2400:1::～2400:1::ff

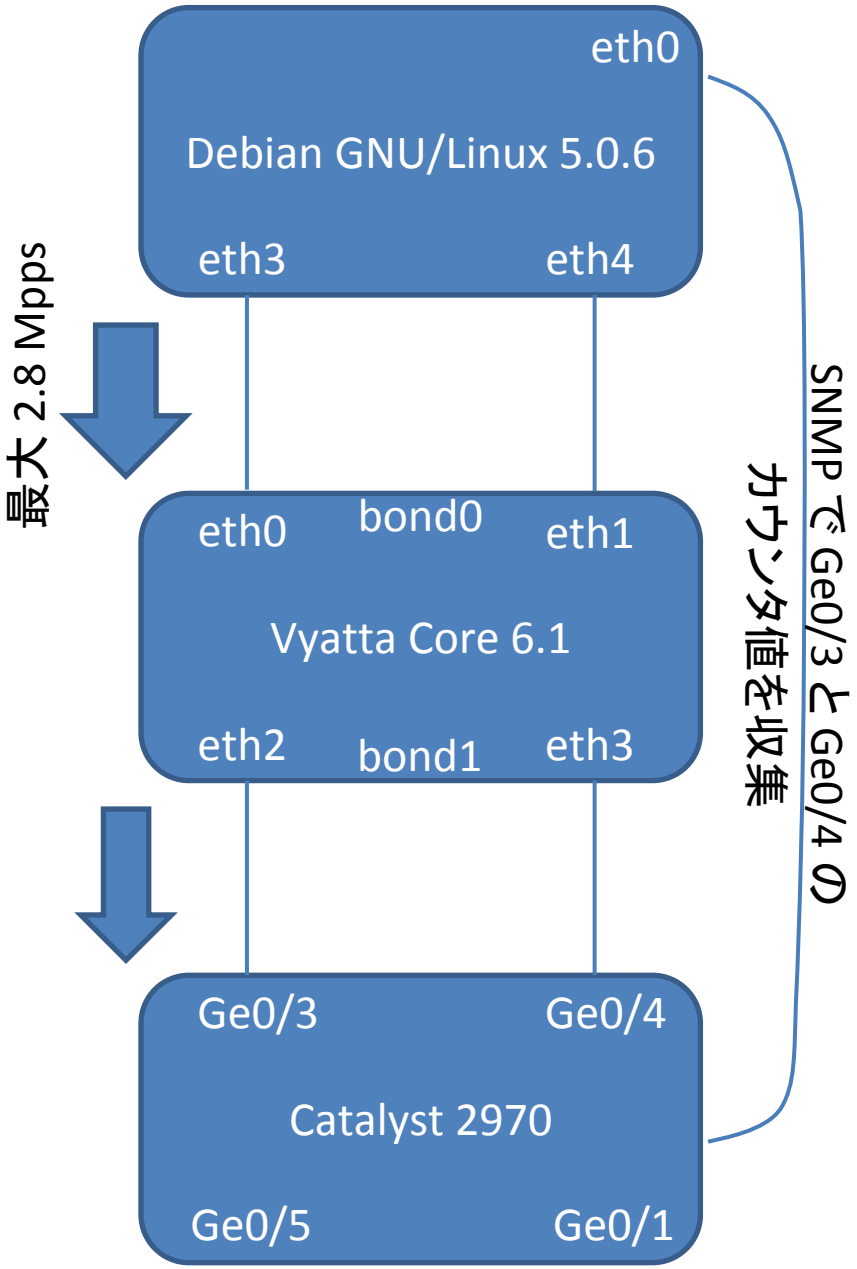
パケットサイズと転送性能(IPv4)



パケットサイズと転送性能(IPv6)



アタック耐性



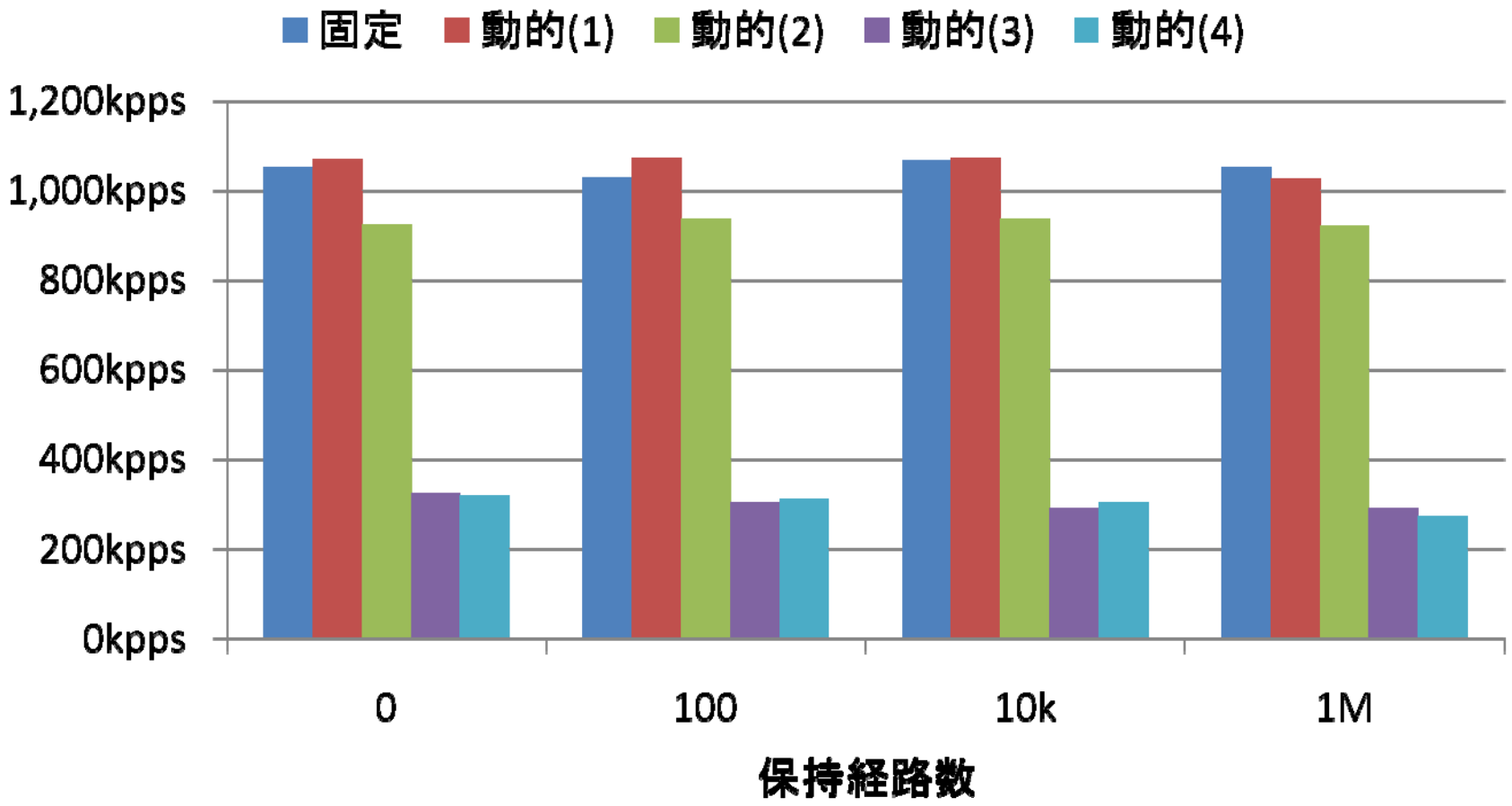
IPv4 宛先アドレス

固定	11.123.123.123
動的(1)	11.123.123.0～11.123.123.255
動的(2)	11.123.0.0～11.123.255.255
動的(3)	11.0.0.0～11.255.255.255
動的(4)	11.0.0.0～138.255.255.255

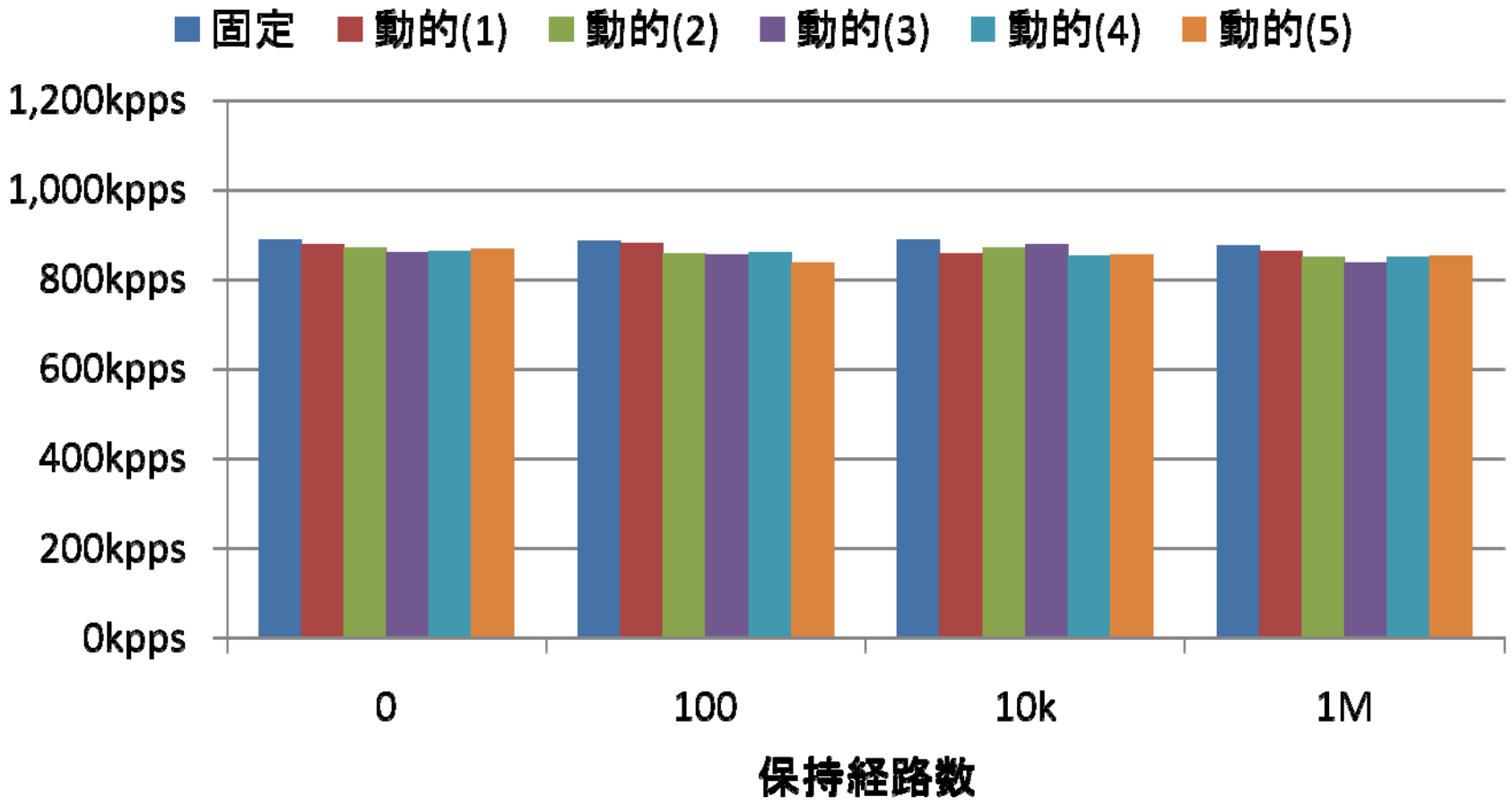
IPv6 宛先アドレス

固定	2400:123:123:123::123
動的(1)	2400:123:123:123::～ 2400:123:123:123:ffff:ffff:ffff:ffff
動的(2)	2400:123:123::～ 2400:123:123:ffff:ffff:ffff:ffff:ffff
動的(3)	2400:123::～ 2400:123:ffff:ffff:ffff:ffff:ffff:ffff
動的(4)	2400::～ 2400:ffff:ffff:ffff:ffff:ffff:ffff:ffff
動的(5)	2400::～ 24ff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

経路・宛先と転送性能(IPv4)



経路･宛先と転送性能(IPv6)



保守性と運用性

保守性と運用性

- セットアップ手順が簡単
  - 数ステップでインストールできます
- バックアップ＆リストアが簡単
  - すべての設定がひとつのファイルで管理されるのでバックアップはそのファイルだけで OK
- 安定性は…
  - 有限会社銀座堂では 1 年半ほど Vyatta を BGP AS 境界ルータとして運用していますが過去 2 回障害を経験しました

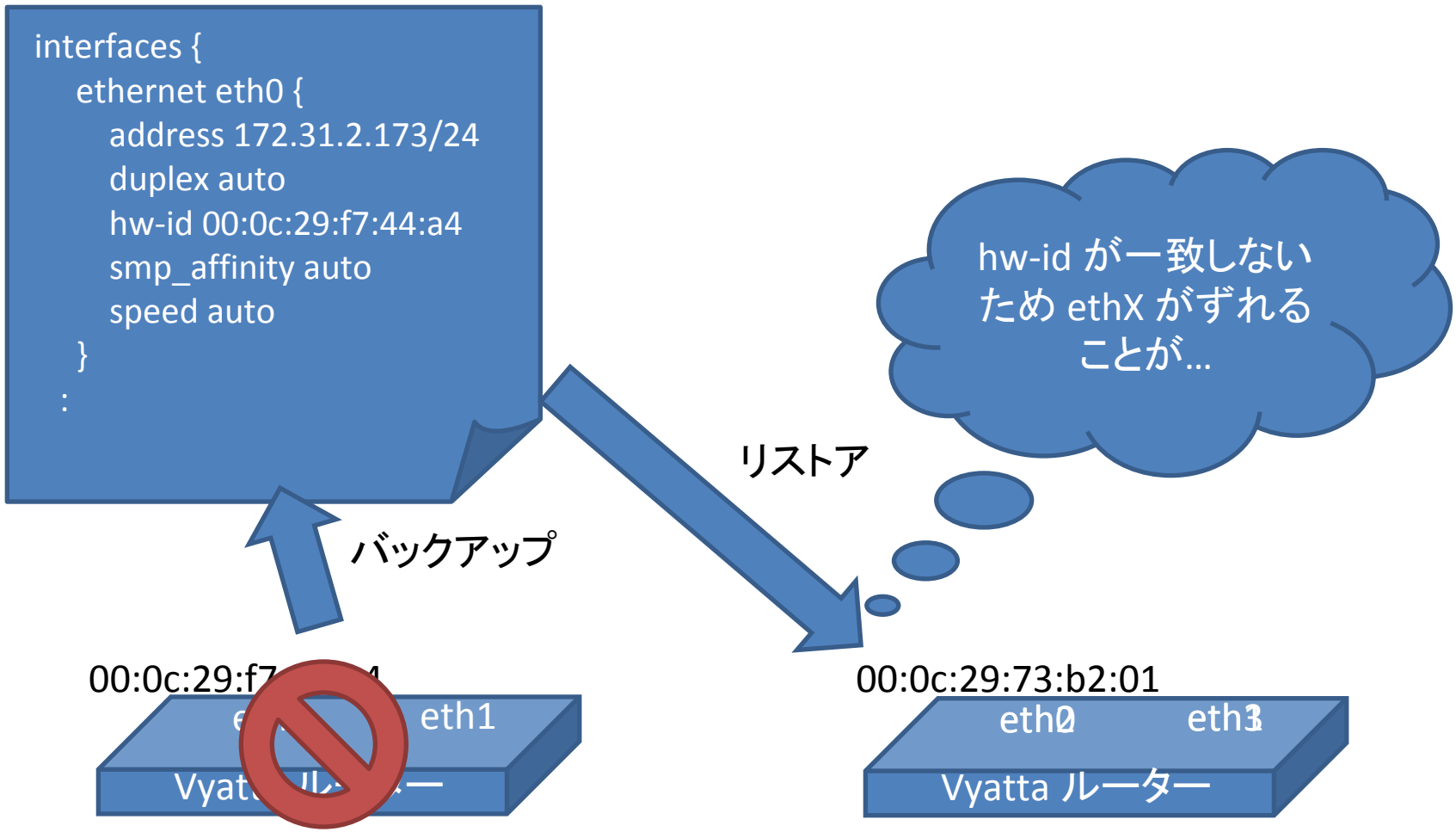
実際に経験した障害

- 2009 年 5 月 3 日
  - BGP プロセスが突然死
  - 長い AS-octets AS 番号が aspath に含まれていた際に起こる Quagga(Vyatta が利用しているルーティングソフトウェア) のバグが原因
- 2010 年 9 月 18 日
  - OSPF プロセスが突然死
  - 原因不明
  - ログになにも残っておらず調査断念

BGPd crash on long asn32 aspath

- 2009 年 5 月 3 日 21:00
  - 片方の Vyatta の BGP プロセスがエラーを吐き死亡
- 2009 年 5 月 4 日 13:32
  - 調べたところ quagga-users ML で 2009 年 2 月 3 日にバグ報告と修正パッチがやり取りされていることが判る
- 2009 年 5 月 4 日 22:34
  - Vyatta 用の修正済みパッケージを Blog で公開している人がいたのでそれをインストール
- 2009 年 5 月 6 日 16:54
  - 本家のリポジトリに取り込まれる(VC 5.0.2 で対応)

hw-id 問題


interfaces {
ethernet eth0 {
address 172.31.2.173/24
duplex auto
hw-id 00:0c:29:f7:44:a4
smp_affinity auto
speed auto
}
:
hw-id が一致しない
ため ethX がずれる
ことが…
リストア
バックアップ
00:0c:29:73:b2:01
eth0
eth1
Vyatta ルーター

まとめ

- 適切な NIC を選択すれば ¥200,000 程度の PC でも 1Mpps 程度のトラヒックを捌ける
  - ☞ 高いコストパフォーマンス
- それなりの知識が無いと保守性や運用性で躓く可能性がある
  - ☞ 機器故障時の対応手順を事前に確認

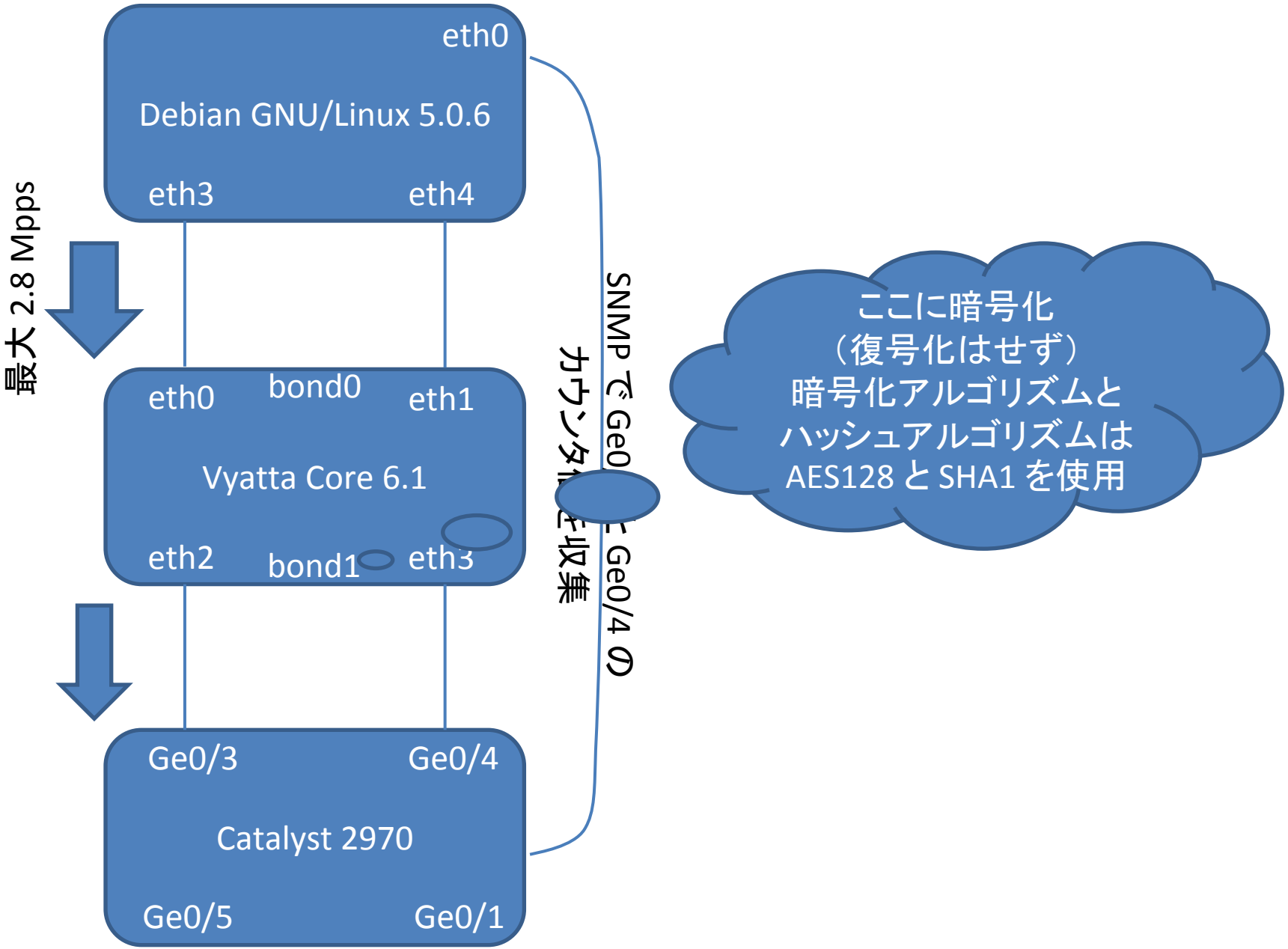
日本 Vyatta ユーザ会のようなコミュニティや有償でサポートしてくれるところを活用しましょう！

謝辞

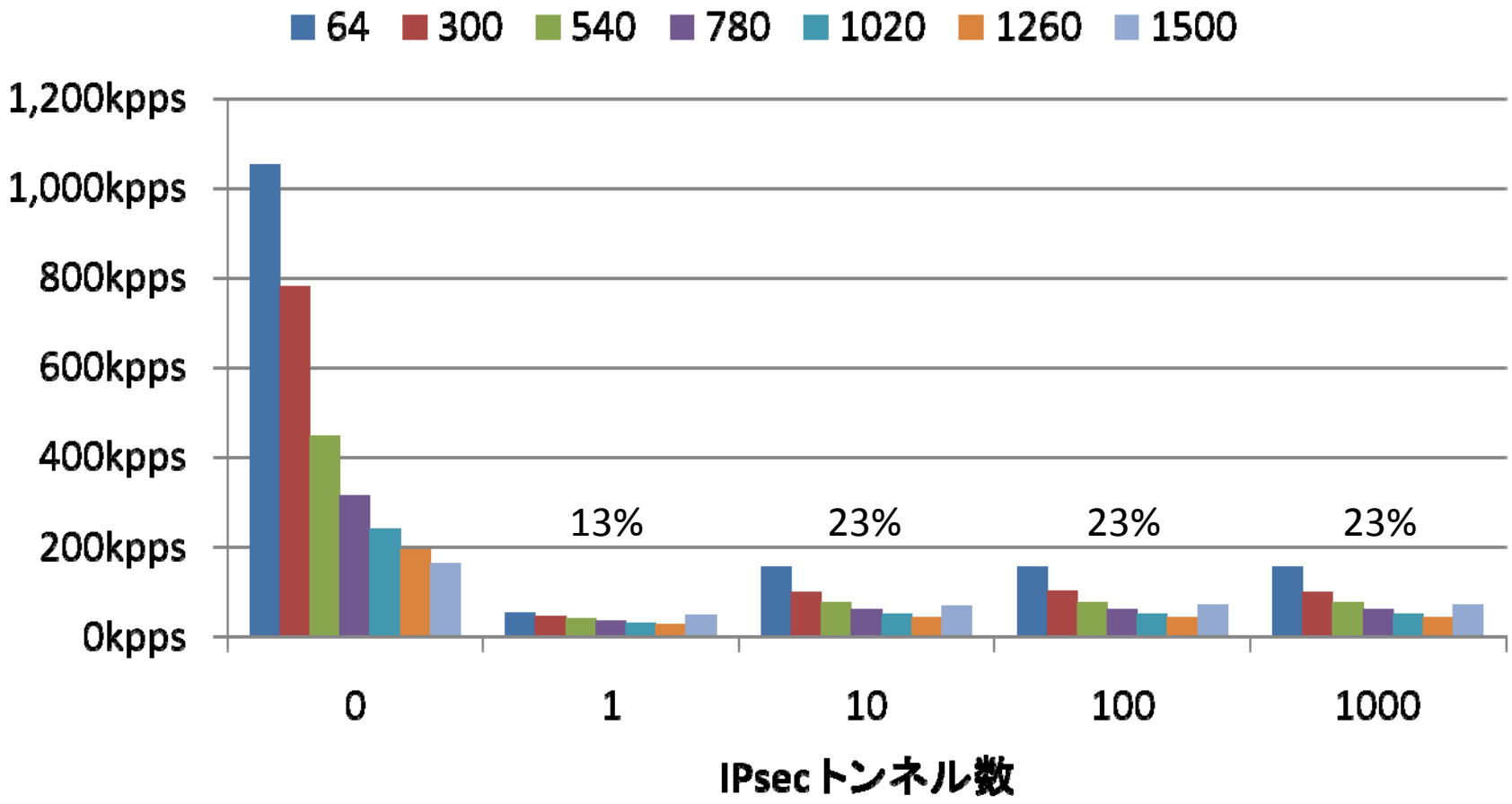
- ネットワンシステムズ株式会社様
  - 性能測定の測定機器と場所をご提供頂きました

もうちょっと深いところの話

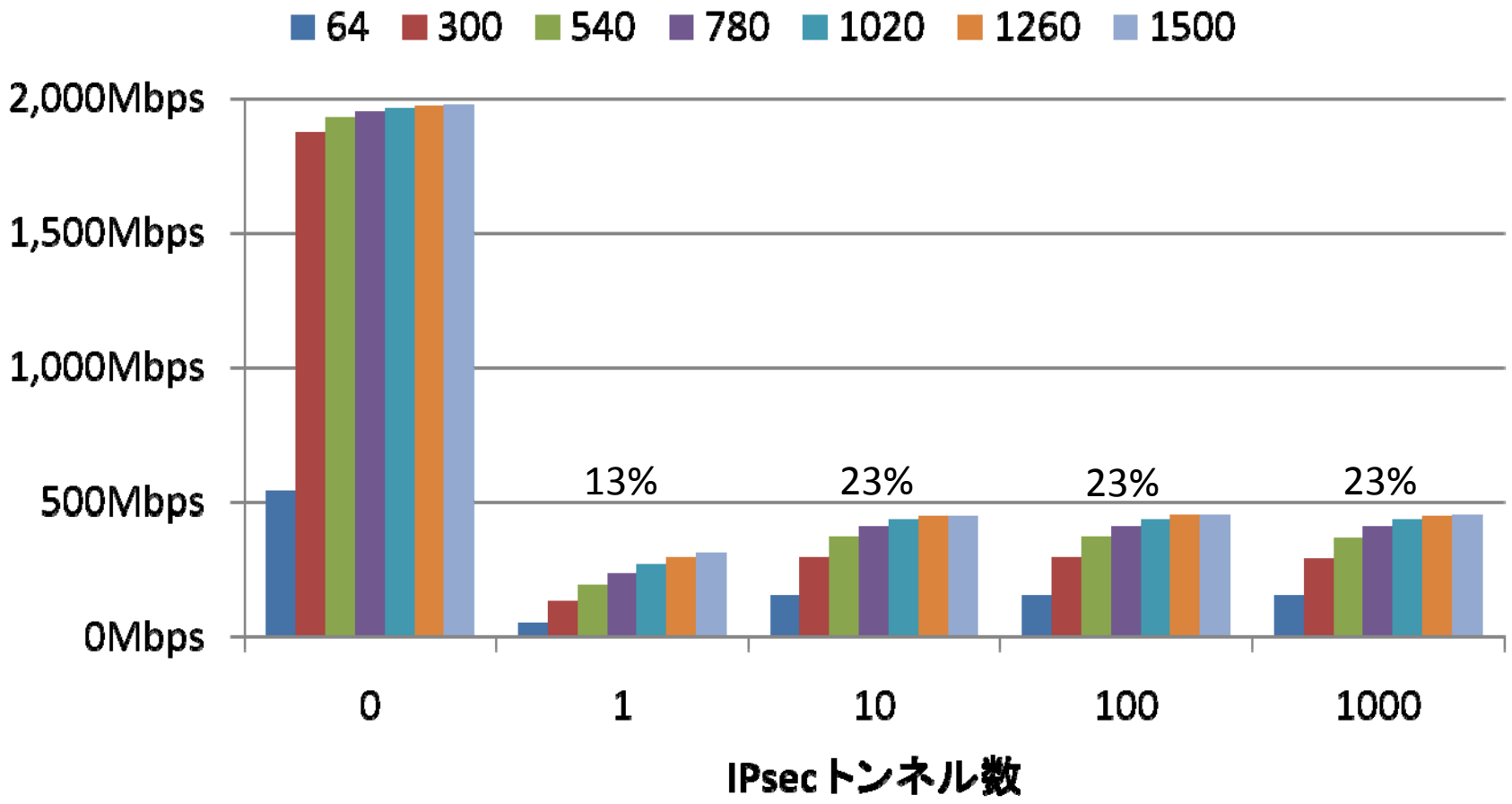
IPSEC で暗号化したとき


eth0
Debian GNU/Linux 5.0.6
eth3
eth4
最大 2.8 Mpps
eth0
bond0
eth1
Vyatta Core 6.1
eth2
bond1
eth3
Ge0/3
Ge0/4
Catalyst 2970
Ge0/5
Ge0/1
SNMP で Ge0
カウンタ
Ge0/4 の
を収集
ここに暗号化
（復号化はせず）
暗号化アルゴリズムと
ハッシュアルゴリズムは
AES128 と SHA1 を使用

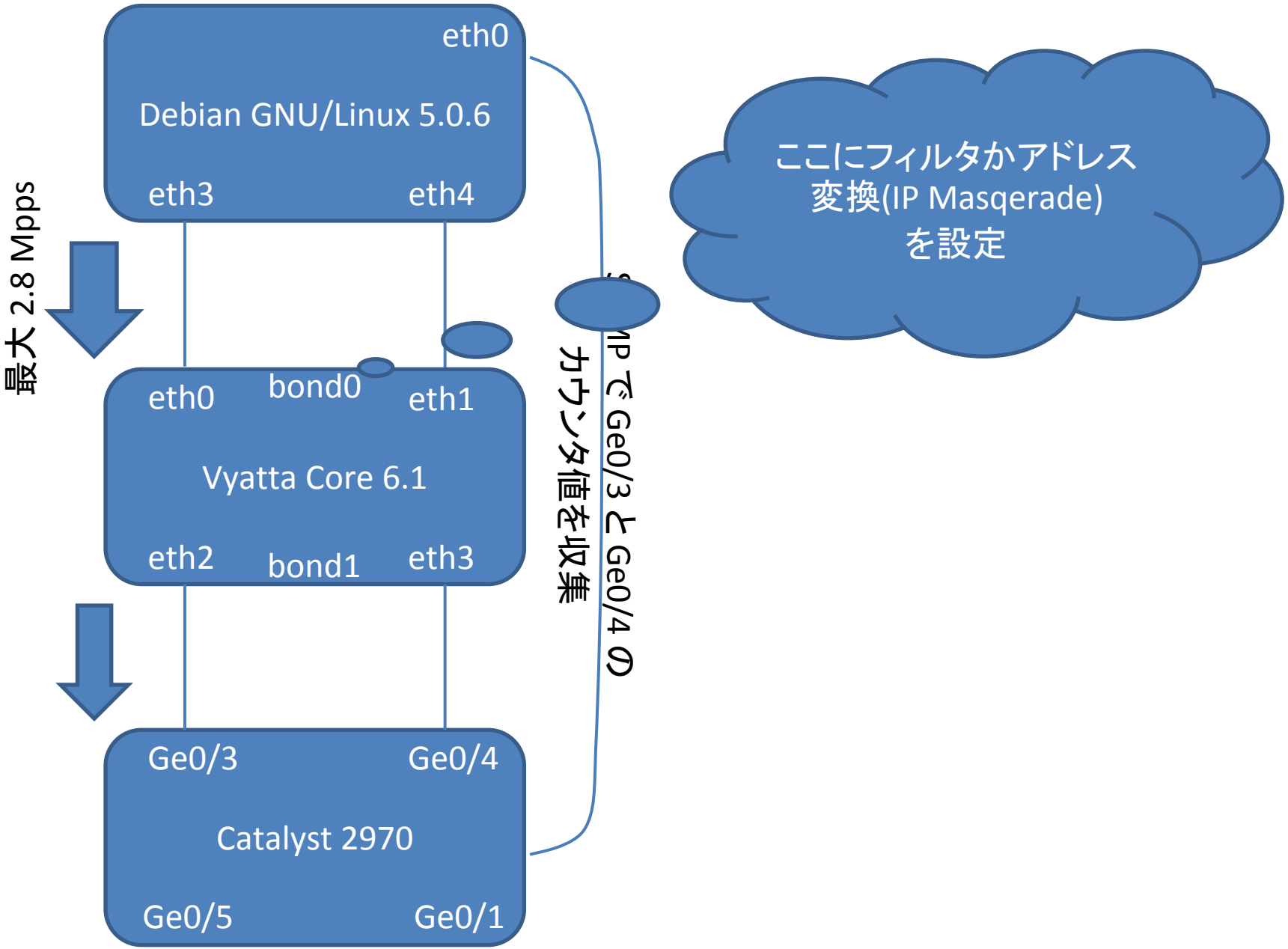
IPsecトンネル数と転送性能(IPv4)



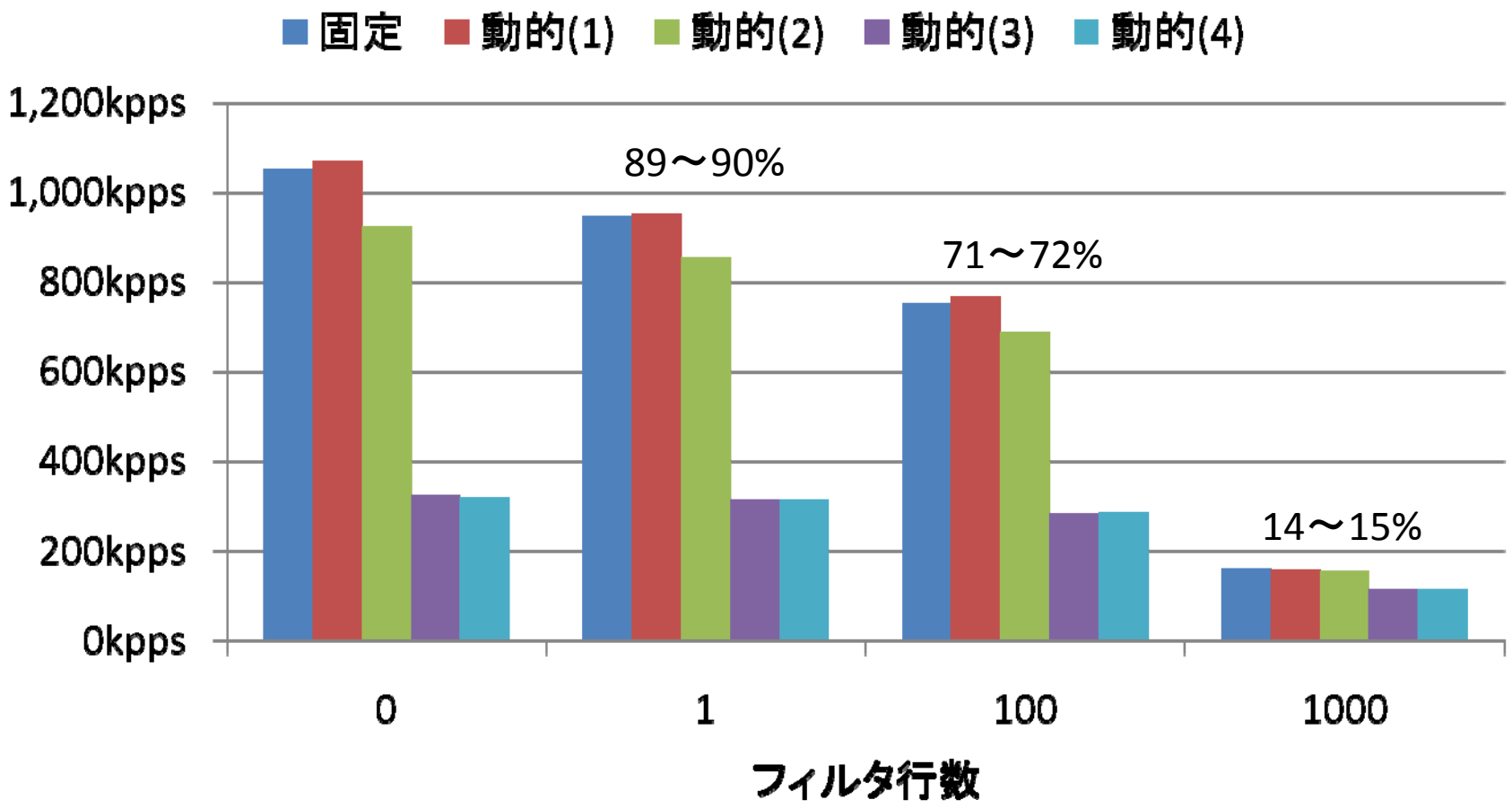
IPsecトンネル数と転送性能(IPv4)



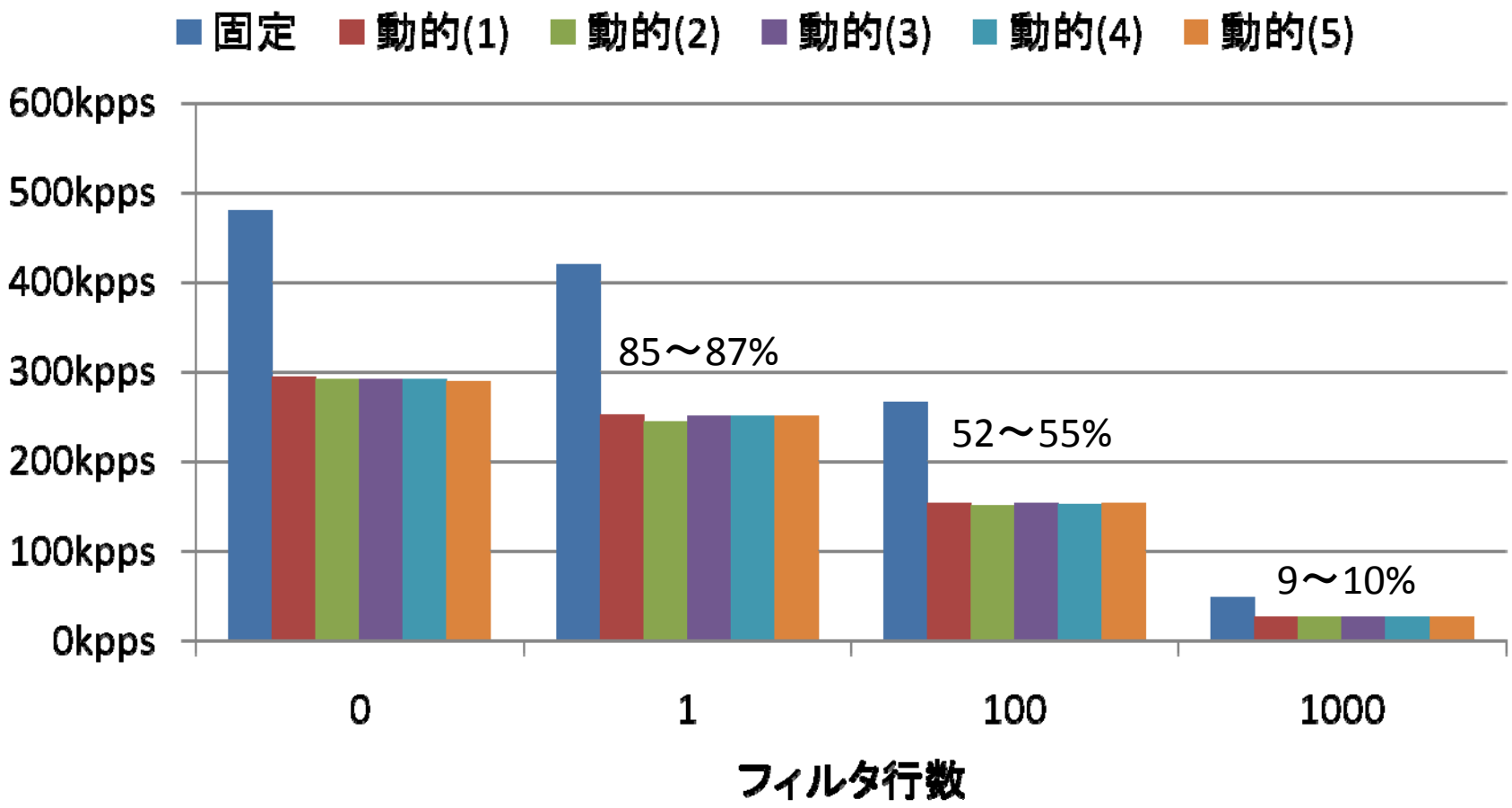
フィルタやアドレス変換を利用したとき


eth0
Debian GNU/Linux 5.0.6
eth3
eth4
最大 2.8 Mpps
eth0
bond0
eth1
Vyatta Core 6.1
eth2
bond1
eth3
Ge0/3
Ge0/4
Catalyst 2970
Ge0/5
Ge0/1
IP で Ge0/3 と Ge0/4 の
カウンタ値を収集
ここにフィルタかアドレス
変換(IP Masqerade)
を設定

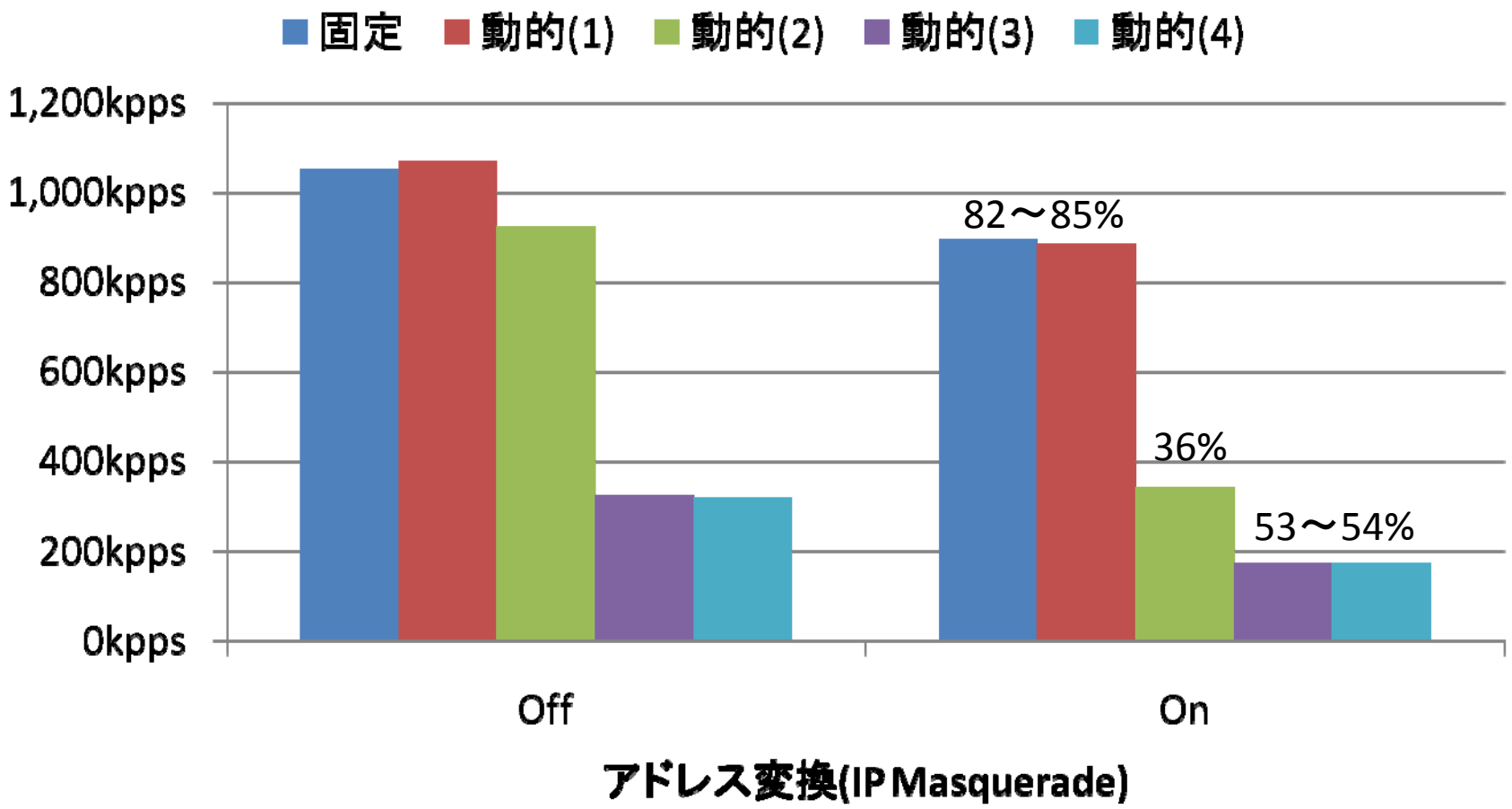
フィルタ行数と転送性能(IPv4)



フィルタ行数と転送性能(IPv6)



アドレス変換と転送性能(IPv4)



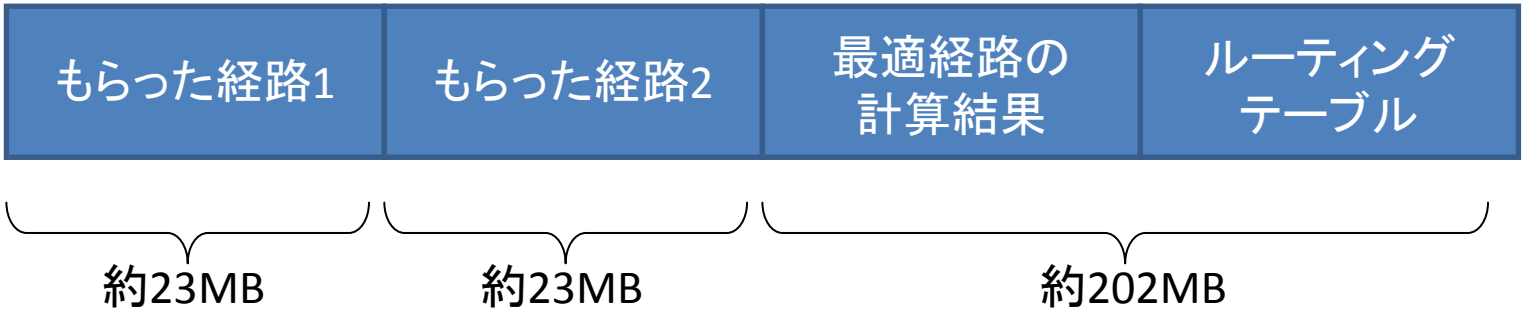
経路数

- 経路数とスループットの関係
  - 経路数がスループットに与える影響はほぼ無視できる程度
  - (詳細は次のページにて)

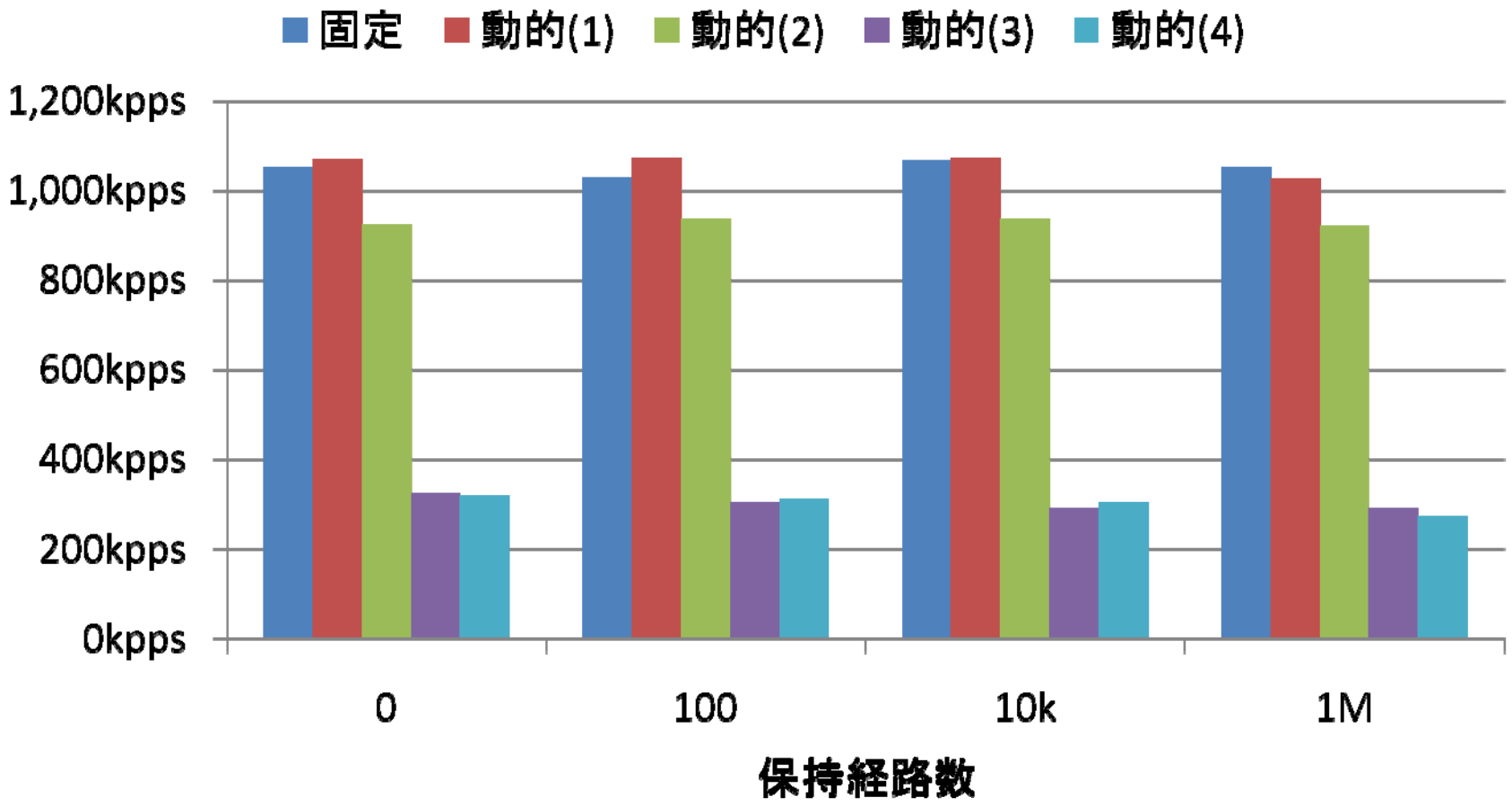
- 経路数とメモリ使用量
  - 例です:
    - 起動直後、保持経路0のときは、used 約70MB
    - すぐに30万経路保持させたら、used 約295MB
    - さらに同じ経路(30万)を追加で保持させたら、used 約318MB

    → 最初に30万経路保持するとき、約225MB消費。

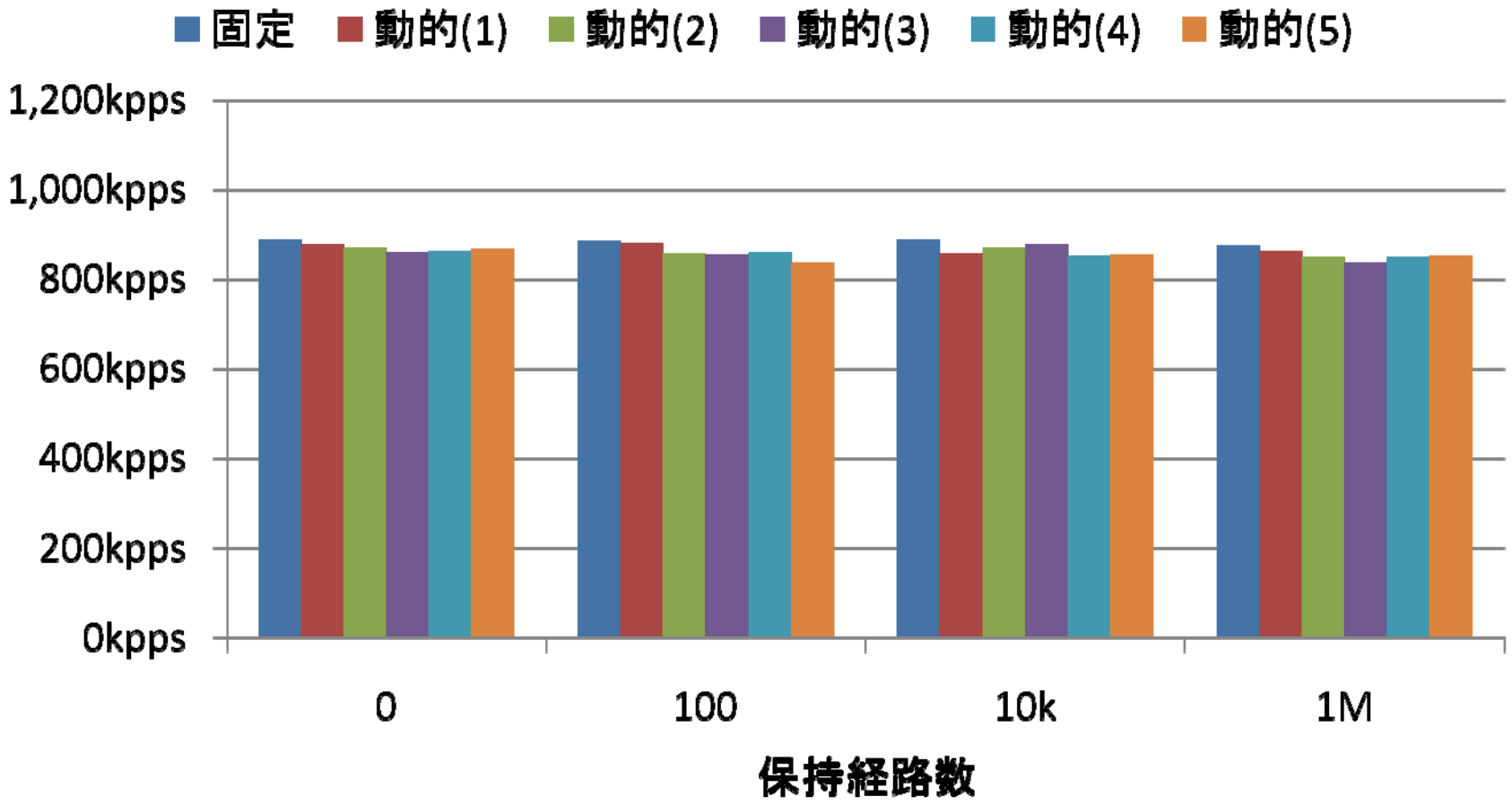
    → 同じ経路情報をさらに30万保持するとき、追加で約23MB消費。



経路・宛先と転送性能(IPv4)

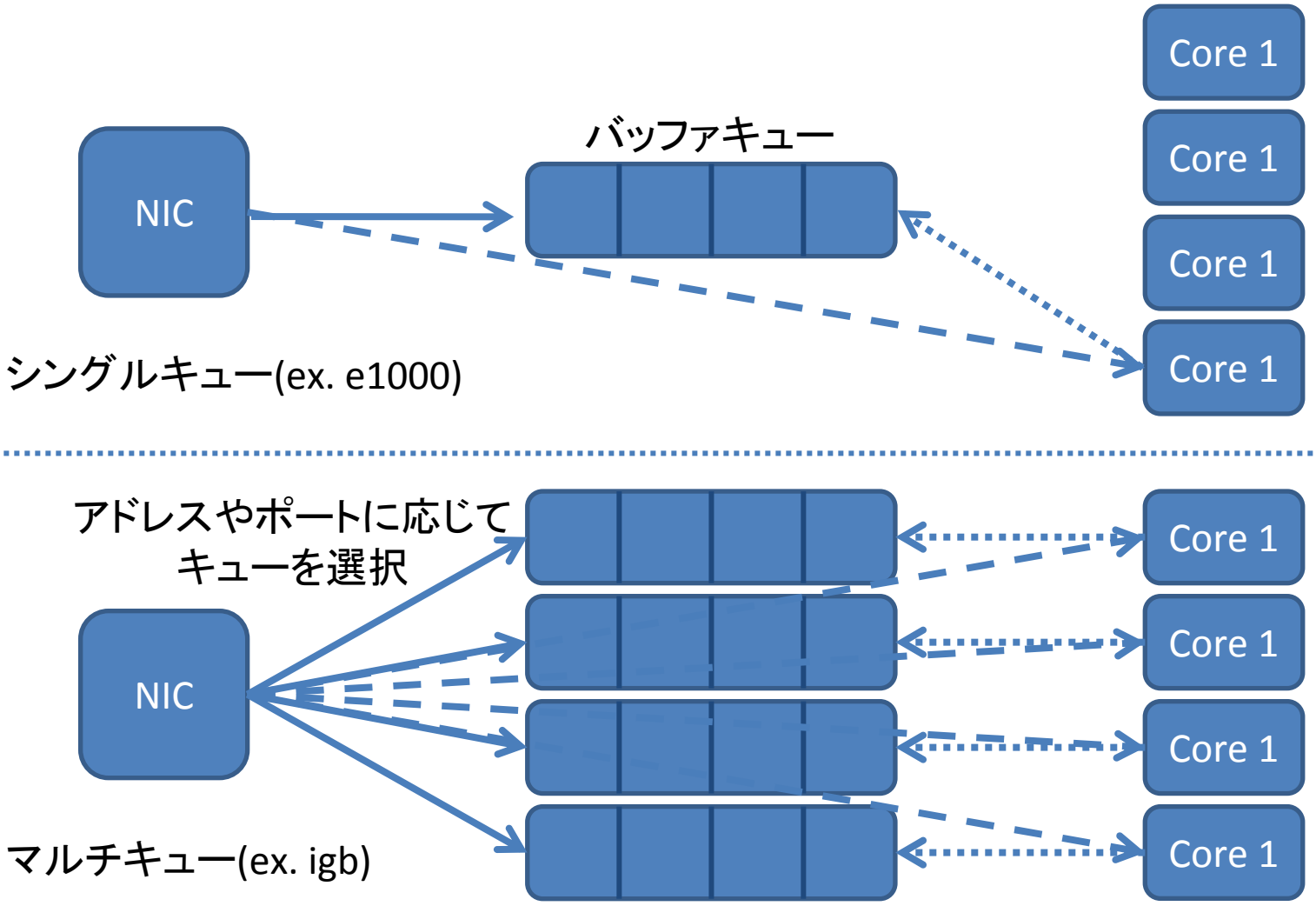


経路･宛先と転送性能(IPv6)

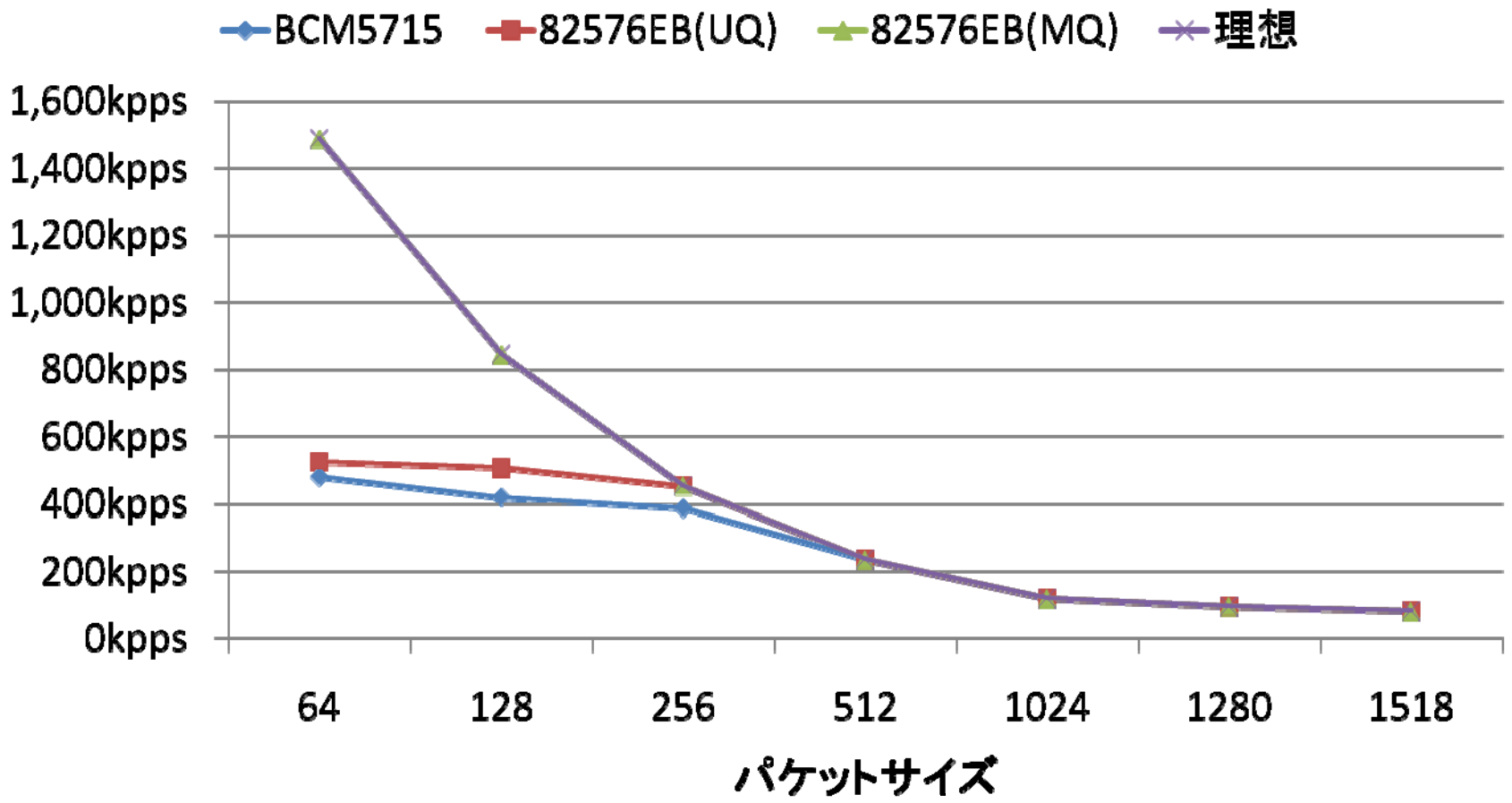


搭載 NIC の違いによる性能差とマルチキューのメリット

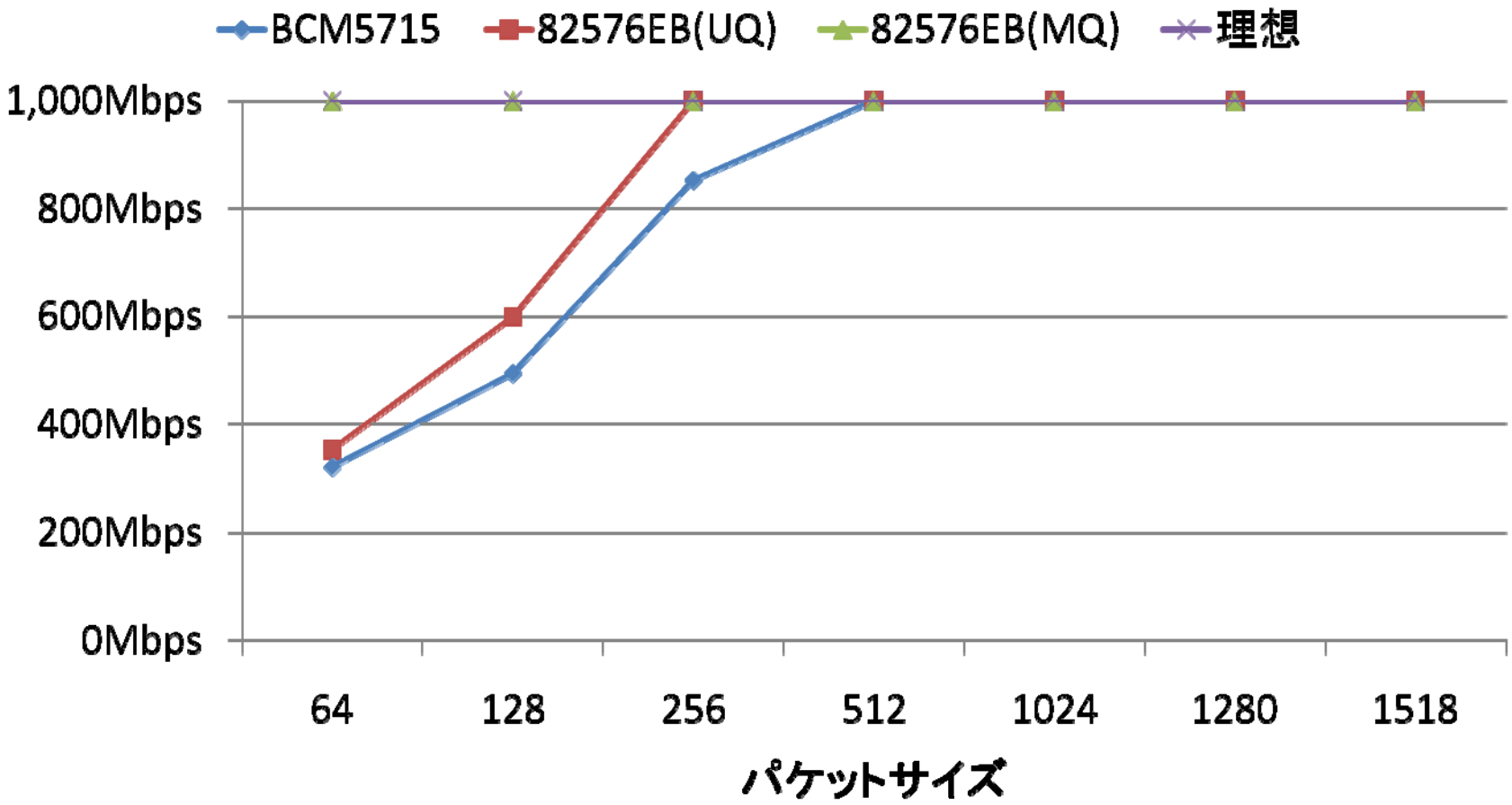
マルチキュー(Receive Side Scaling)



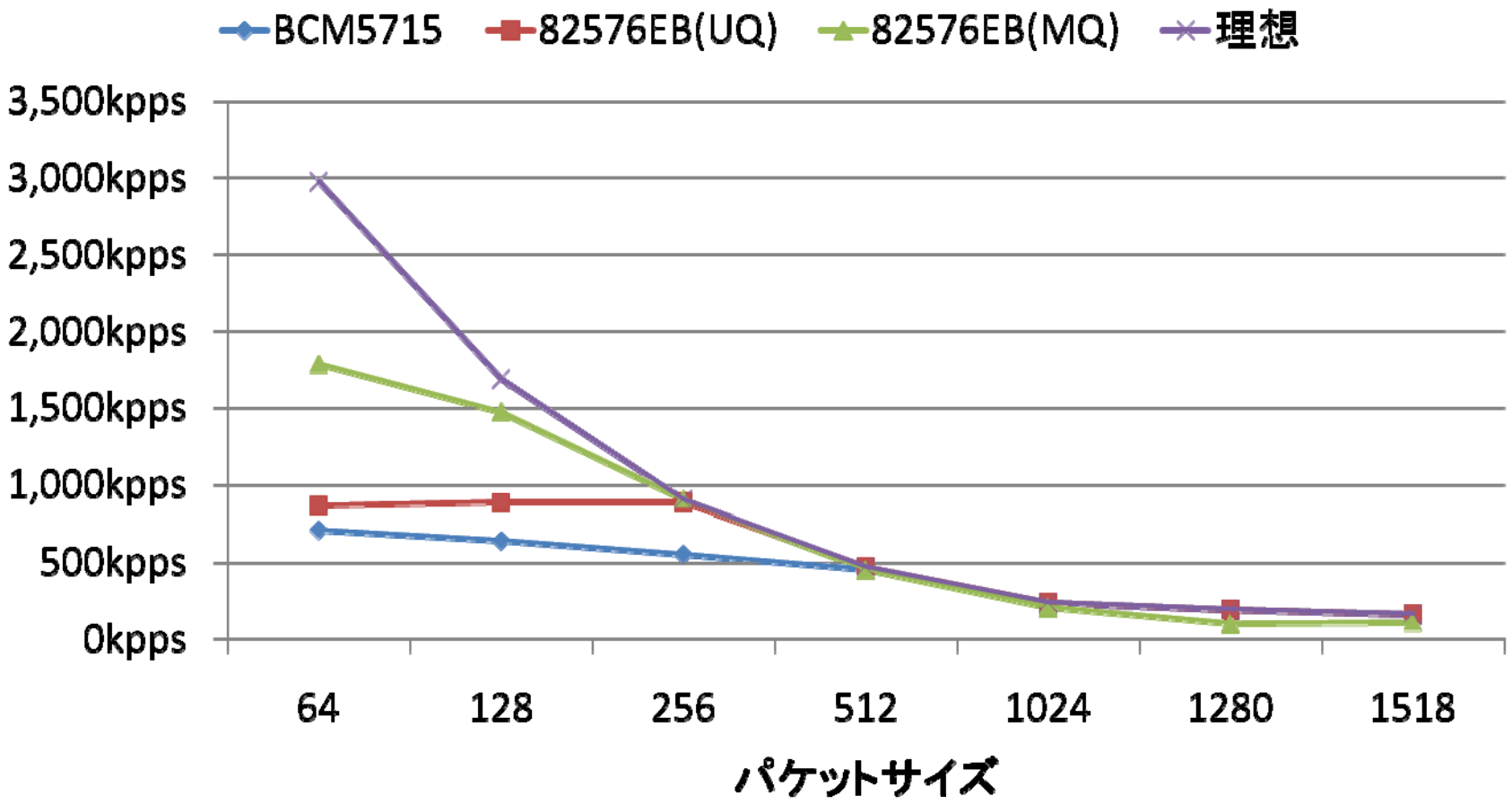
IPv4 片方向の転送性能



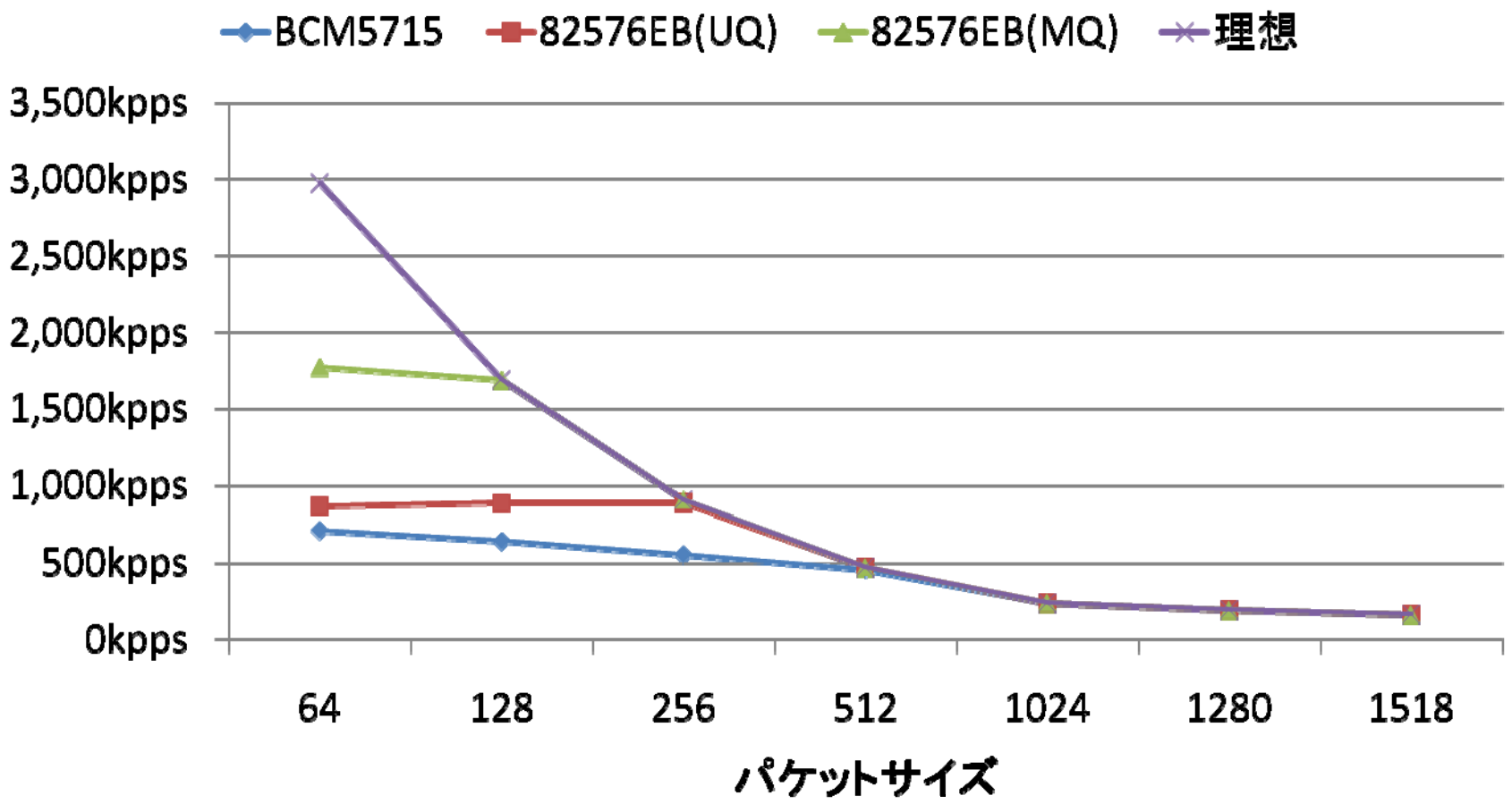
IPv4 片方向の転送性能



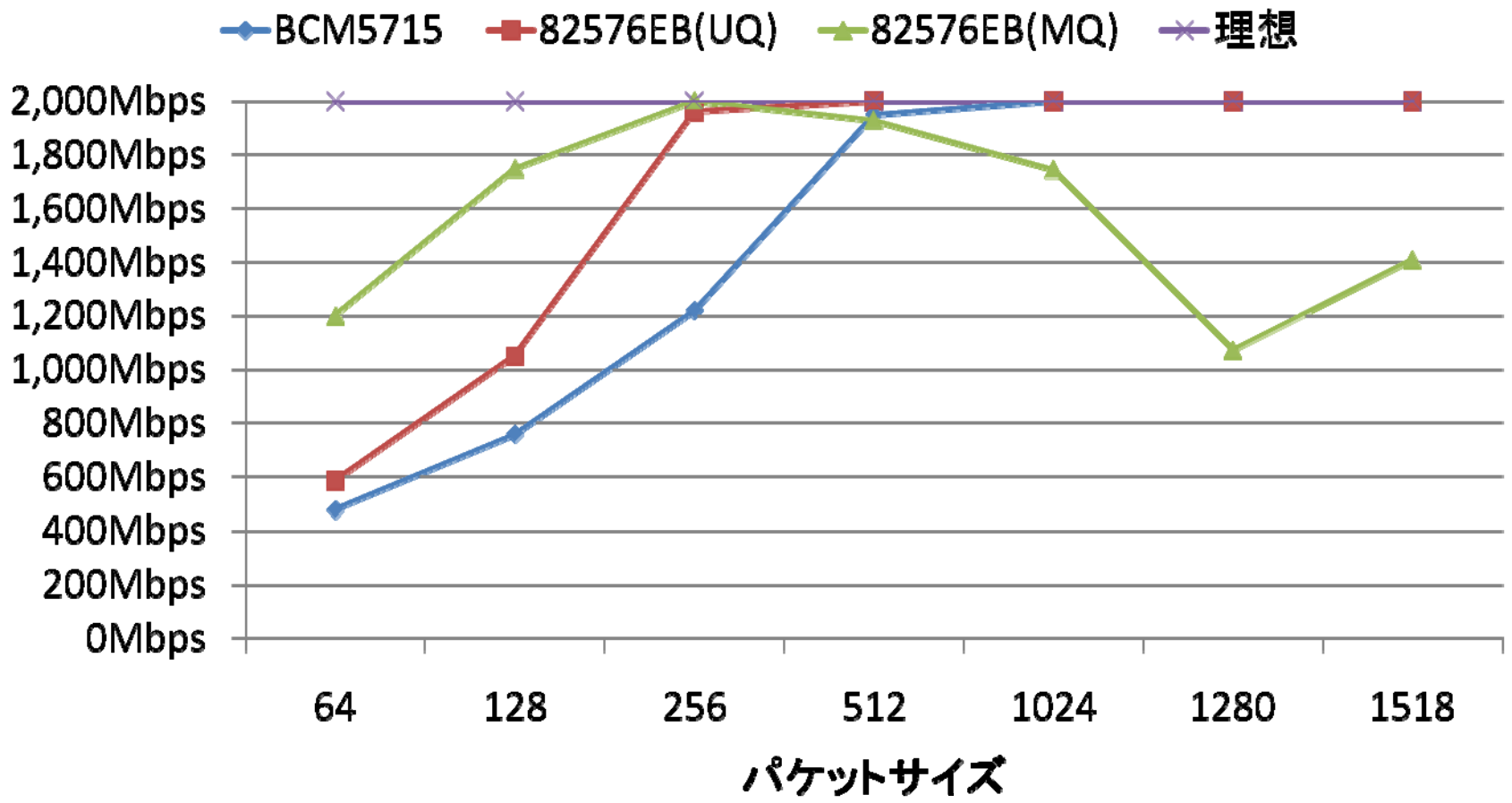
IPv4 両方向の転送性能



IPv4 両方向 (0.1% ロス許容)



IPv4 両方向の転送性能



IPv4 両方向 (0.1% ロス許容)