ネットワークＩ／Ｏ帯域の隔離

Xen Sumit Tokyo 2008

宝曼 西門 <simon@valinux.co.jp>
稲越 宏弥 <inakoshi.hiroya@jp.fujitsu.com>

２００８年１１月２２日～２１日

本研究・開発の一部は、経済産業省の委託を受けた技術研究組合　超先端電子技術開発機構(ASET)のセキュア・プラットフォームプロジェクトの成果です

目次

第 1 節

帯域の隔離

目的

公平性

- 全部のドメインが公平にネットワークの資源を使えるように
  - 管理者のポリシー設定に応じて
- ウイルスがあるドメインから防衛します
- 悪意あるドメインから防衛します

ネットワークの資源

- NIC帯域
- Dom0 CPU
- Dom0 カーネル内メモリ

ネットワークの資源

- NIC帯域
  - domU送受信速度
- Dom0 CPU
  - domU送受信速度
- Dom0 カーネル内メモリ
  - Dom0 カーネルのバケット待ち時間

パケットスケジューラ

- 送受信したdomUによって、バケットを優先度付けします
- キューは満杯時にパケットを破棄します

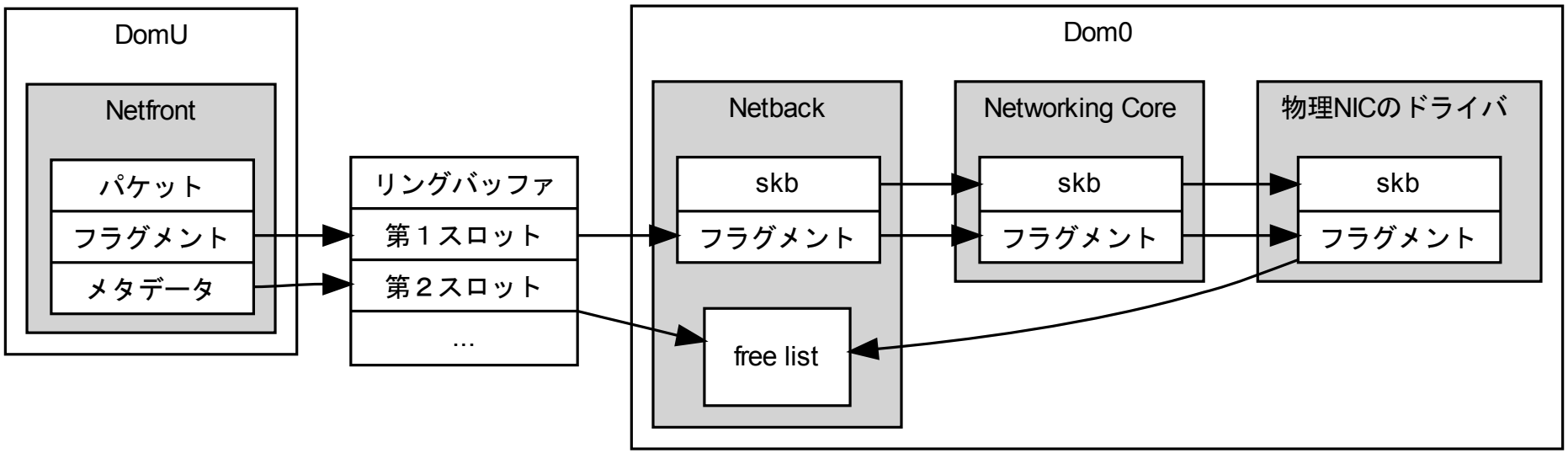
パケットスケジューラ

- 送受信したdomUによって、バケットを優先度付けします
  - NIC帯域
  - Dom0 CPU
- キューは満杯時にパケットを破棄します
  - Dom0カーネル内メモリ

Netback/Netfrontフロー制御

Netfrontから物理NICの間でルーティングが行なわれるので, パケットスケジューラはネットワーク資源を制御できます

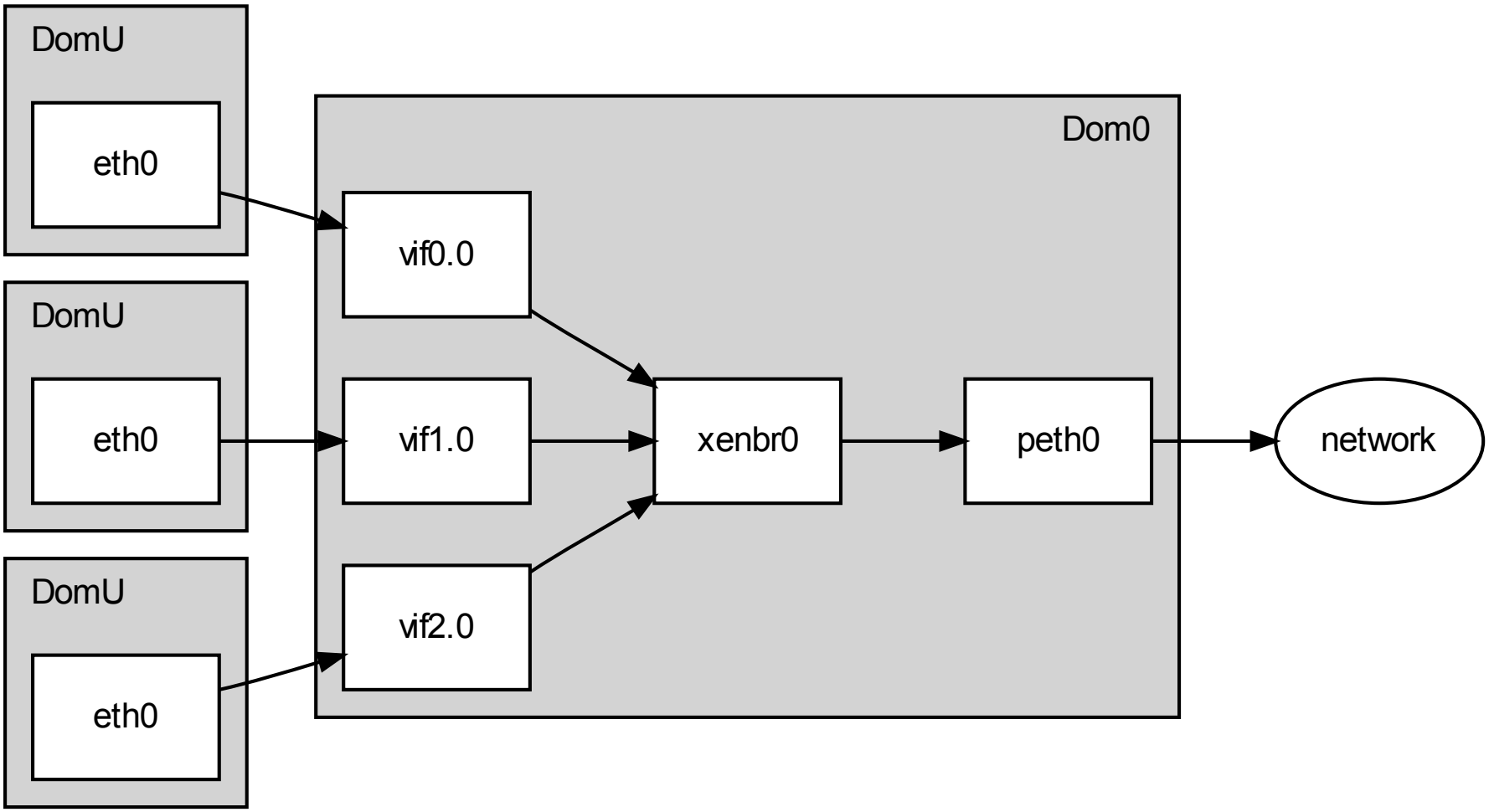
- dom0のCPU
- dom0のカーネル内のメモリ



第 2 節

パケットの識別

DomU送信: パケットを識別する



- どのインターフェースからxenbr0に転送されたか分かると送信したdomUが分かります

DomU送信: iptablesのルール

domUが使用するインターフェースによって,fwmarkを付与します

```
iptables -t mangle -A FORWARD -m physdev \
        --physdev-in vif2.0 -j MARK --set-mark 100
iptables -t mangle -A FORWARD -m physdev \
        --physdev-in vif3.0 -j MARK --set-mark 110
iptables -t mangle -A FORWARD -m physdev \
        --physdev-in vif5.0 -j MARK --set-mark 120
```

第 3 節

パケットスケジューラ

パケットスケジューラ

- フィルタリング
  - クラスに対して設定します
- 優先度付け
  - クラス識別に基づきます
  - パケットを遅延させることが出来ます
- キューイング
  - 優先付け時とフィルタリング後、送信のために
- ドロップ
  - キューが満杯の時

Netback/Netfrontのフロー制御

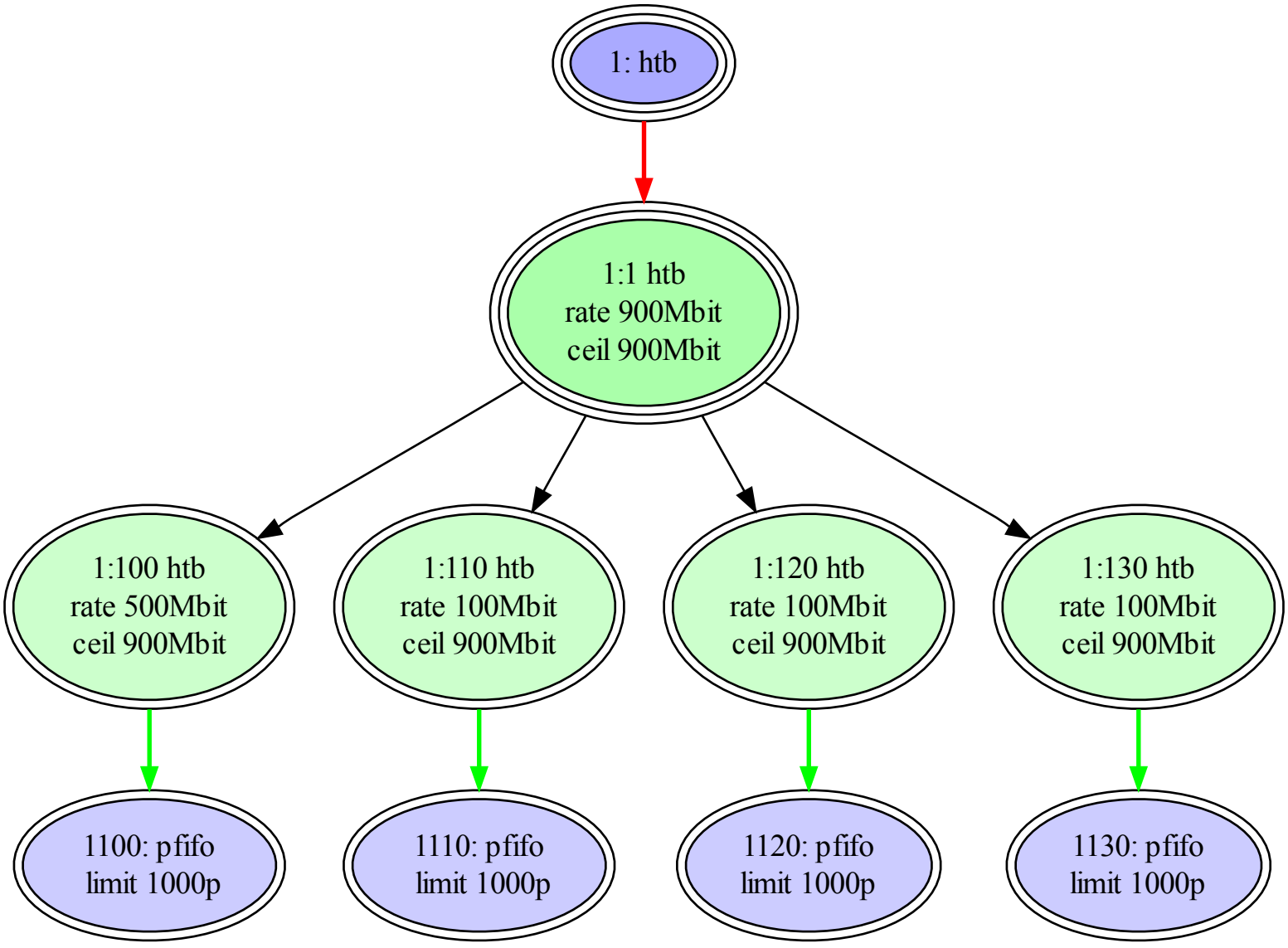
DomU送信

$$p \leq n$$

where: p: vif$N.M$から送信したdom0にキューに入れたパケット
n: netbackのリングバッファのスロット数
(デフォルト= 256)

- dom0にパケットを遅延するので十分です
- dom0内でパケットを破棄するのは悪影響があります
  - dom0内でパケットを遅延させるにしたがって、domU送信は遅くなります

DomU送信: パケット・スケジューラの階層図



DomU送信: HTBのルール: Leafクラス

Leafクラス

- ドメインを 1 個ずつ
- デフォルト

```
tc class add dev peth0 parent 1:1 classid 1:100 htb \
        rate 500Mbit ceil 900Mbit
tc class add dev peth0 parent 1:1 classid 1:110 htb \
        rate 100Mbit ceil 900Mbit
tc class add dev peth0 parent 1:1 classid 1:120 htb \
        rate 100Mbit ceil 900Mbit
tc class add dev peth0 parent 1:1 classid 1:130 htb \
        rate 100Mbit ceil 900Mbit
```

DomU送信: フィルタ

iptablesによって設定されるfwmarkによりフィルタされます

- `handle` N はfwmark のキーです
- `flowid` X:Y flowid X:Yはパケット繋ぐキューです

```
tc filter add dev peth0 protocol ip parent 1: \
        handle 100 flowid 1:100
tc filter add dev peth0 protocol ip parent 1: \
        handle 110 flowid 1:110
tc filter add dev peth0 protocol ip parent 1: \
        handle 120 flowid 1:120
```

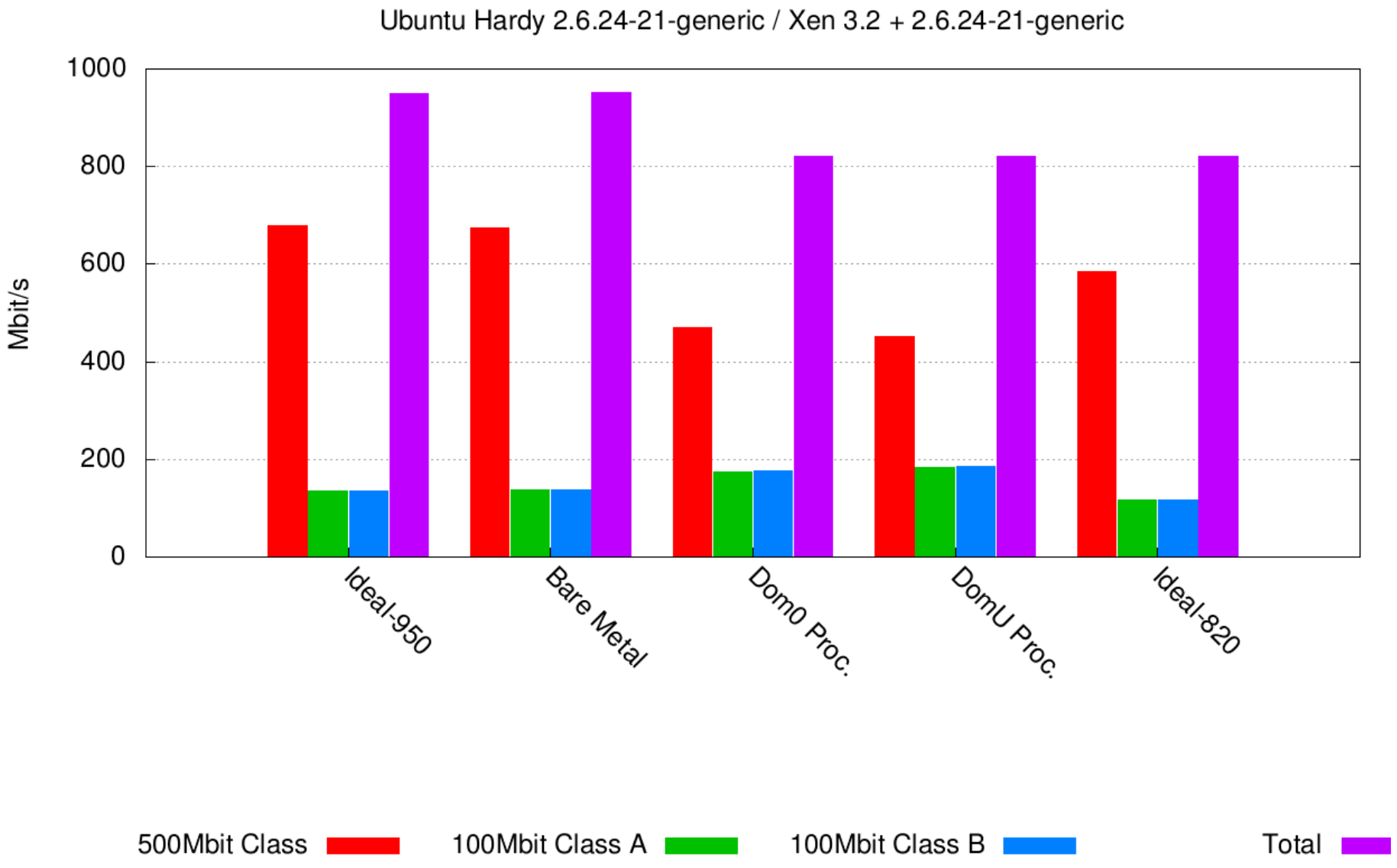
質問

質問がありますか

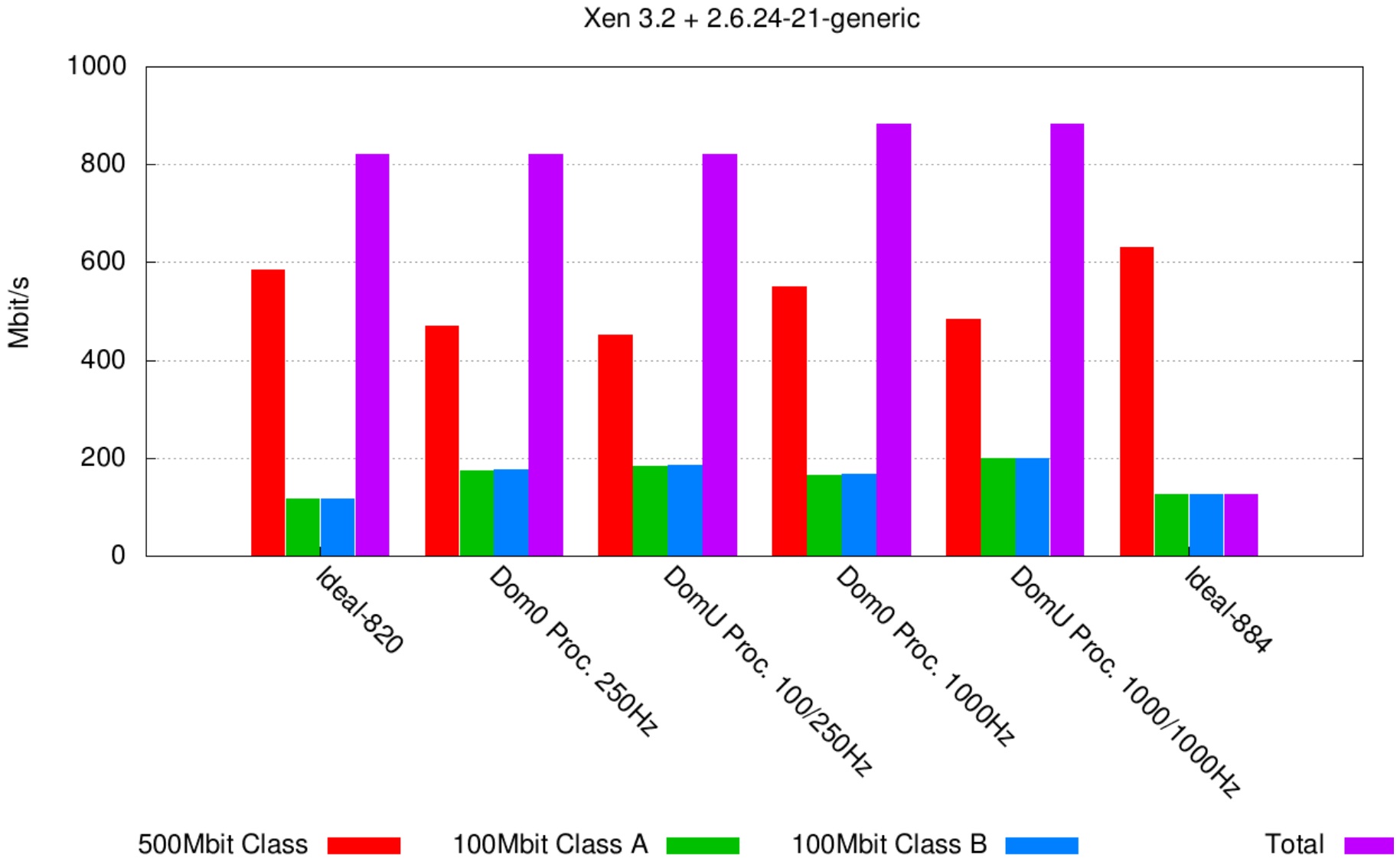
第 4 分

延長

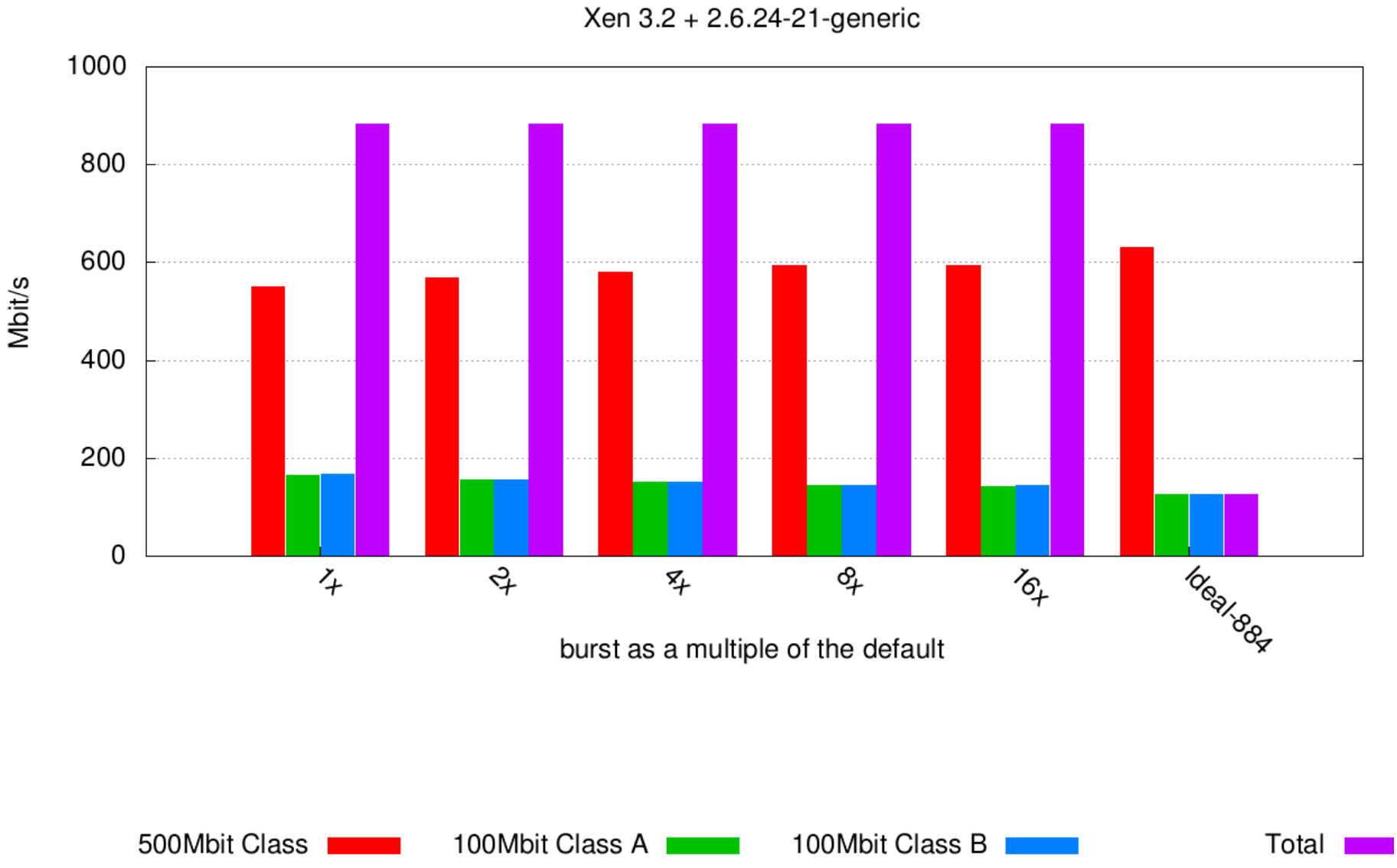
HTBのパフォーマンス



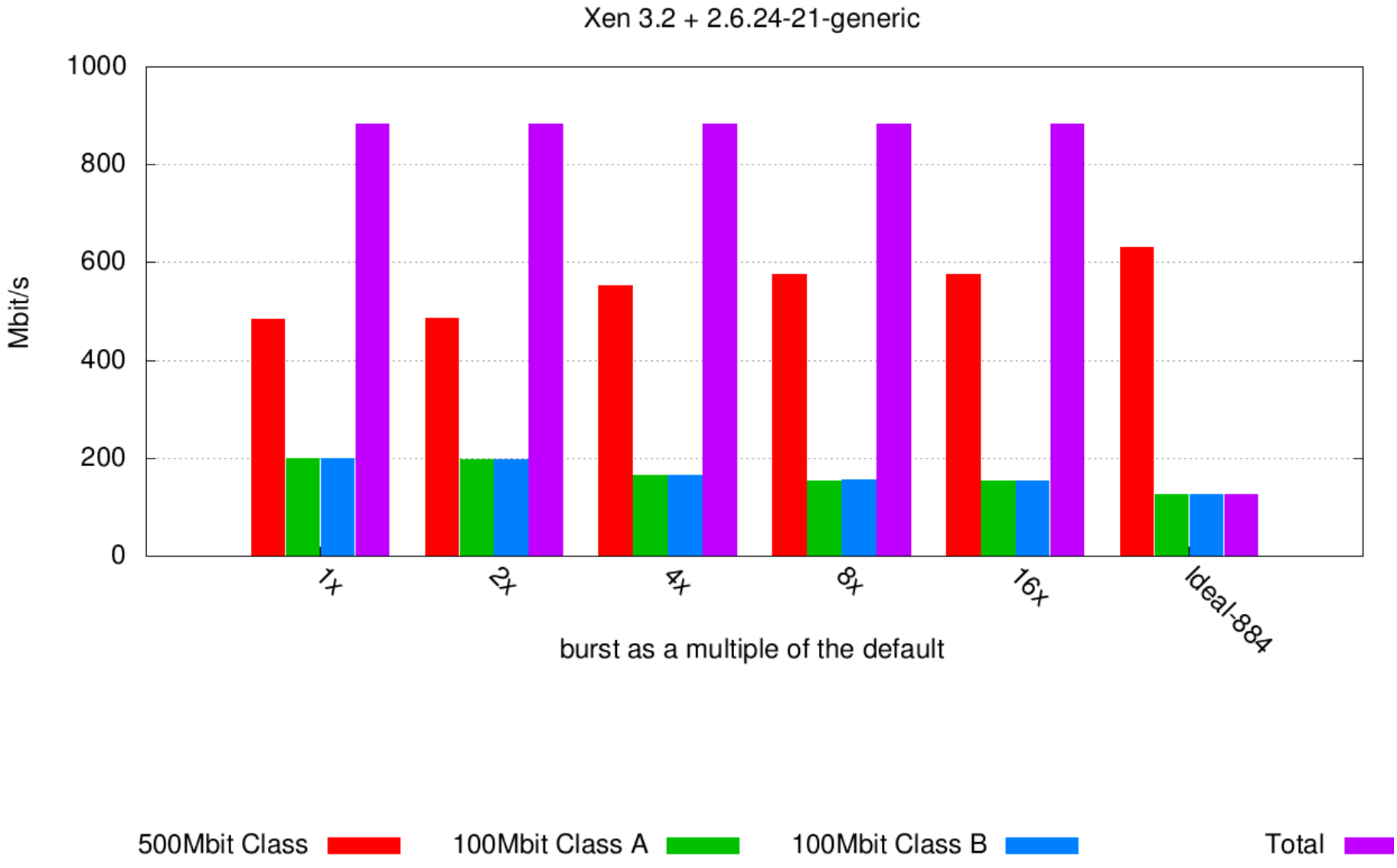
HZのチューニング


Xen 3.2 + 2.6.24-21-generic
Mbit/s
1000
800
600
400
200
0
Ideal-820
Dom0 Proc. 250Hz
DomU Proc. 100/250Hz
Dom0 Proc. 1000Hz
DomU Proc. 1000/1000Hz
Ideal-884
500Mbit Class
100Mbit Class A
100Mbit Class B
Total

バーストのチューニング: Dom0から出るパケット



バーストのチューニング: DomUから出るパケット



終了