トラフィックグラフはどう作られる？
～sFlow/NetFlowを使ってみる～

BBSakura Networks 株式会社　外山 結月

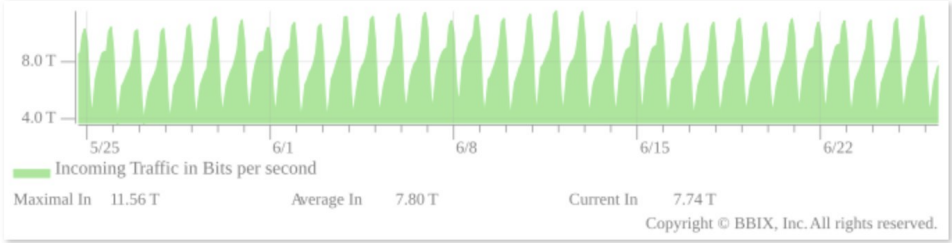
BBSakura Networks

Daily Graph (5 Minute Average)

Weekly Graph (5 Minute Average)

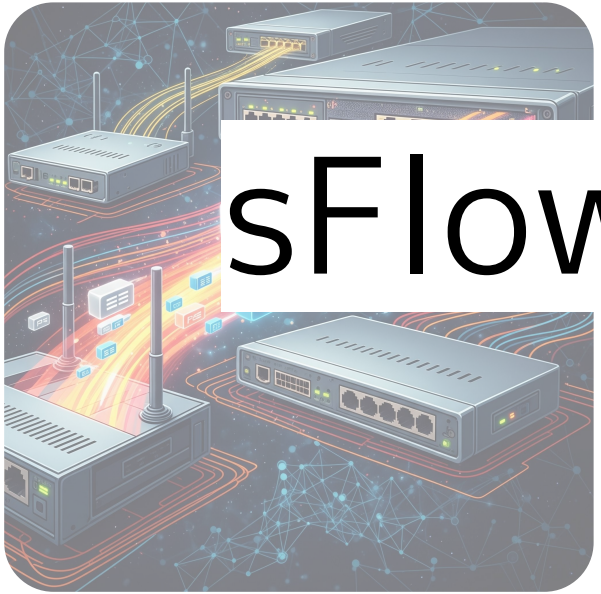
トラフィックグラフ

Monthly Graph (5 Minute Average)



https://www.bbix.net/service/ix/traffic-graph/

トラフィックグラフとは



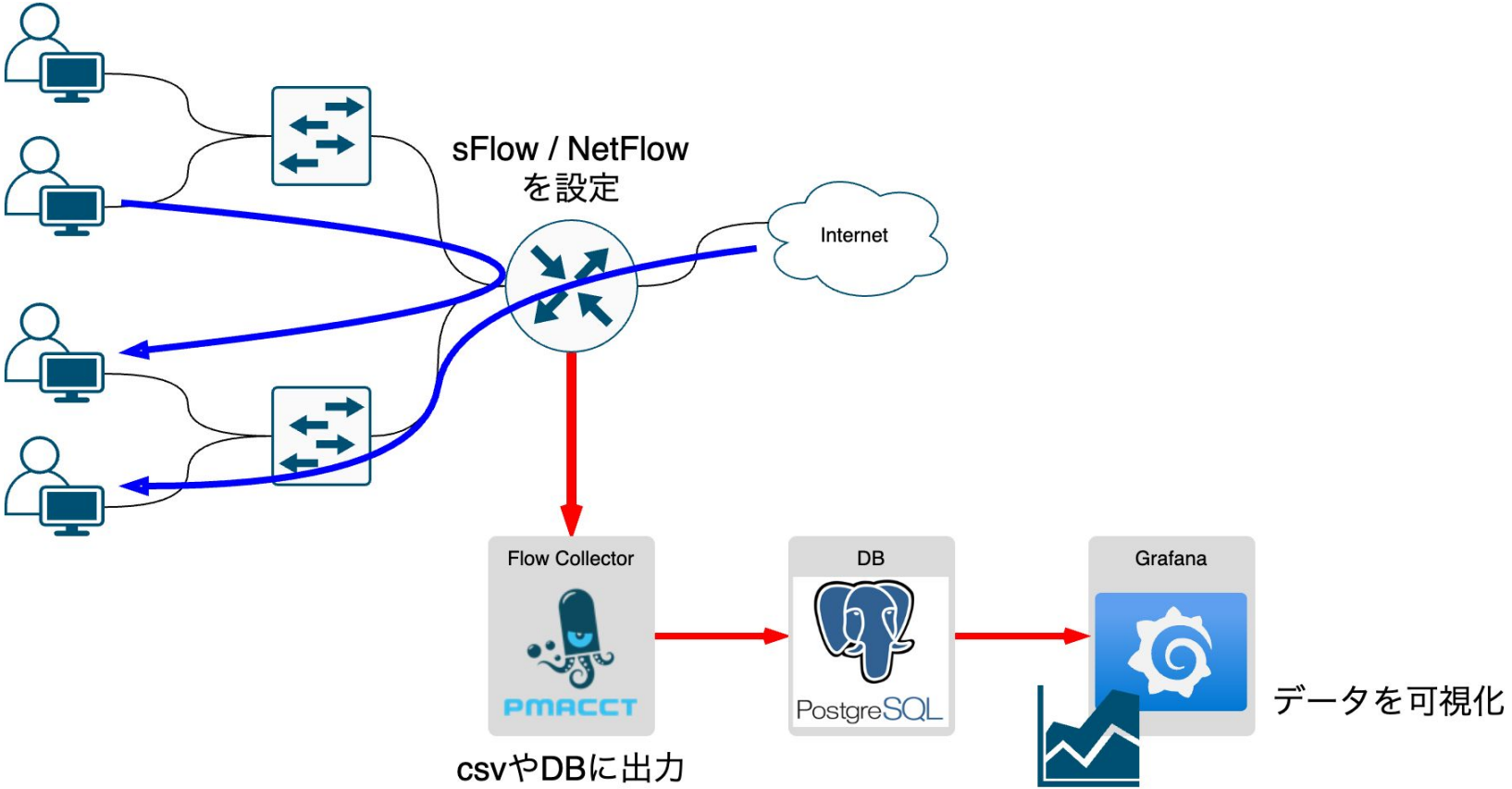
sFlow / NetFlow

- 通信量
- 発信元・受信先IPアドレス
- 利用プロトコル・ポート　etc.

sFlow / NetFlowってなに？

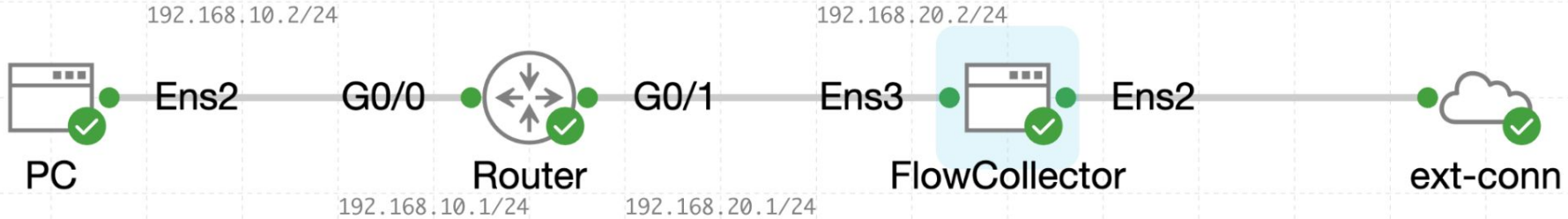
- **sFlow：可視化に強い**
  - パケットを**サンプリング**
  - 軽量&リアルタイムにネットワーク全体の傾向を把握
- **NetFlow: ログ、課金に強い**
  - **全ての通信**を取得
  - 通信ごとの詳細なトラフィック情報を取得
- SNMP: 死活監視、運用
  - 定期的に監視システムから状態を問い合わせる、ポーリング型
  - 機器の状態（CPU / メモリ / インターフェース使用率）を監視

トラフィックグラフができるまで



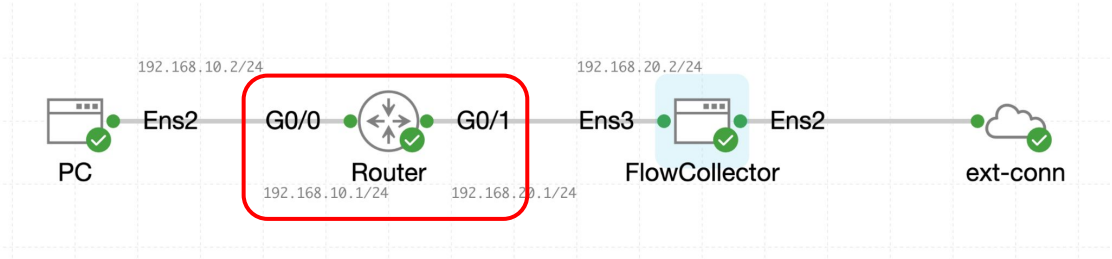
NetFlowのシミュレーション (Cisco Modeling Labs)

BBSakura Networks



Routerの設定

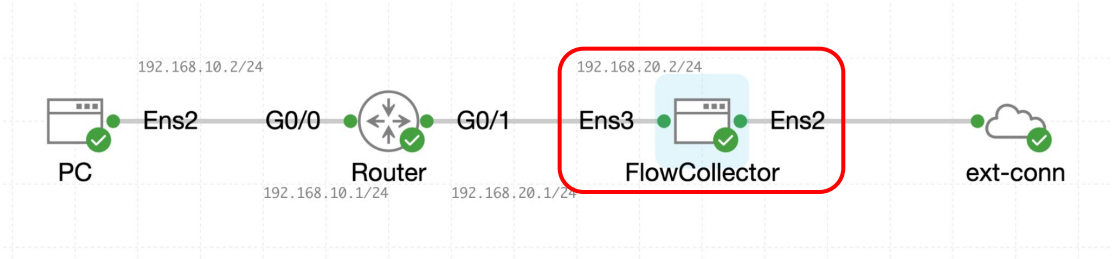
```
configure terminal
!
ip flow-export version 5
ip flow-export destination 192.168.20.2 2055
!
interface GigabitEthernet0/0
 ip flow ingress
 ip flow egress
!
interface GigabitEthernet0/1
 ip flow ingress
 ip flow egress
!
end
```



Flow Collectorの設定

```
sudo apt update
sudo apt install pmacct
sudo vim /etc/pmacct/nfacctd.conf
sudo systemctl start nfacctd
sudo systemctl enable nfacctd
```

```
# /etc/pmacct/nfacctd.conf
daemonize: true
pidfile: /var/run/nfacctd.pid
syslog: daemon
!
aggregate: src_host,dst_host,src_port,dst_port,proto
!
interface: ens3
!
plugins: print
print_output_file: /var/log/pmacct/flow_data.log
```



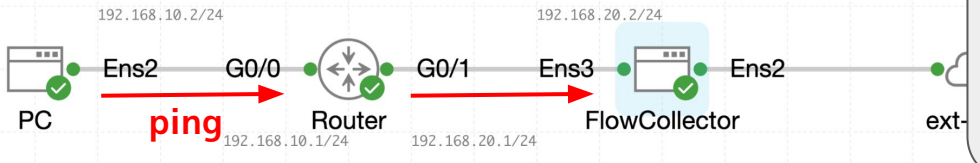
データの取得

```
cisco@PC:~$ ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=255 time=2.44 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=255 time=2.57 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=255 time=2.53 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=255 time=2.61 ms
64 bytes from 192.168.10.1: icmp_seq=5 ttl=255 time=2.60 ms
64 bytes from 192.168.10.1: icmp_seq=6 ttl=255 time=2.62 ms
64 bytes from 192.168.10.1: icmp_seq=7 ttl=255 t
64 bytes from 192.168.10.1: icmp_seq=8 ttl=255 t
64 bytes from 192.168.10.1: icmp_seq=9 ttl=255 t
```

```
user@FlowCollector:/var/log/pmacct$ sudo tcpdump -nni ens3 udp port 2500
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
02:21:44.712646 IP 192.168.20.1.65035 > 192.168.20.2.2100: UDP, length 600
02:21:56.712146 IP 192.168.20.1.65035 > 192.168.20.2.2100: UDP, length 360
02:22:10.719496 IP 192.168.20.1.65035 > 192.168.20.2.2100: UDP, length 264
02:22:24.723884 IP 192.168.20.1.65035 > 192.168.20.2.2100: UDP, length 648
```

```
tail: flow_data.log: file truncated
```

SRC_IP	DST_IP	SRC_PORT	DST_PORT	PROTOCOL	PACKETS	BYTES
192.168.10.2	8.8.8.8	58800	53	udp	1	60
192.168.10.2	8.8.8.8	52999	53	udp	1	62
192.168.10.2	8.8.4.4	35502	53	tcp	4	244
192.168.10.2	192.168.10.1	0	0	icmp	5	500
192.168.10.2	8.8.8.8	59938	53	tcp	4	244
192.168.10.2	8.8.4.4	53979	53	udp	1	62
192.168.10.2	8.8.4.4	47255	53	udp	1	60
192.168.10.2	8.8.4.4	55623	53	udp	1	60
192.168.10.2	8.8.4.4	54021	53	udp	1	62



このlog（csv, DBとして出力も可）を
良い感じに加工すると、
トラフィックグラフができる！

まとめ

sFlow, NetFlowの設定を入れれば

簡単にトラフィックデータをとれる！

Enabling a Connected Future.

BBSakuraNetworks