パケットトレーサで学ぶNW構築（基礎編）

⑤　　総合実習

お　品　書　き

１　構成図

２　構成条件

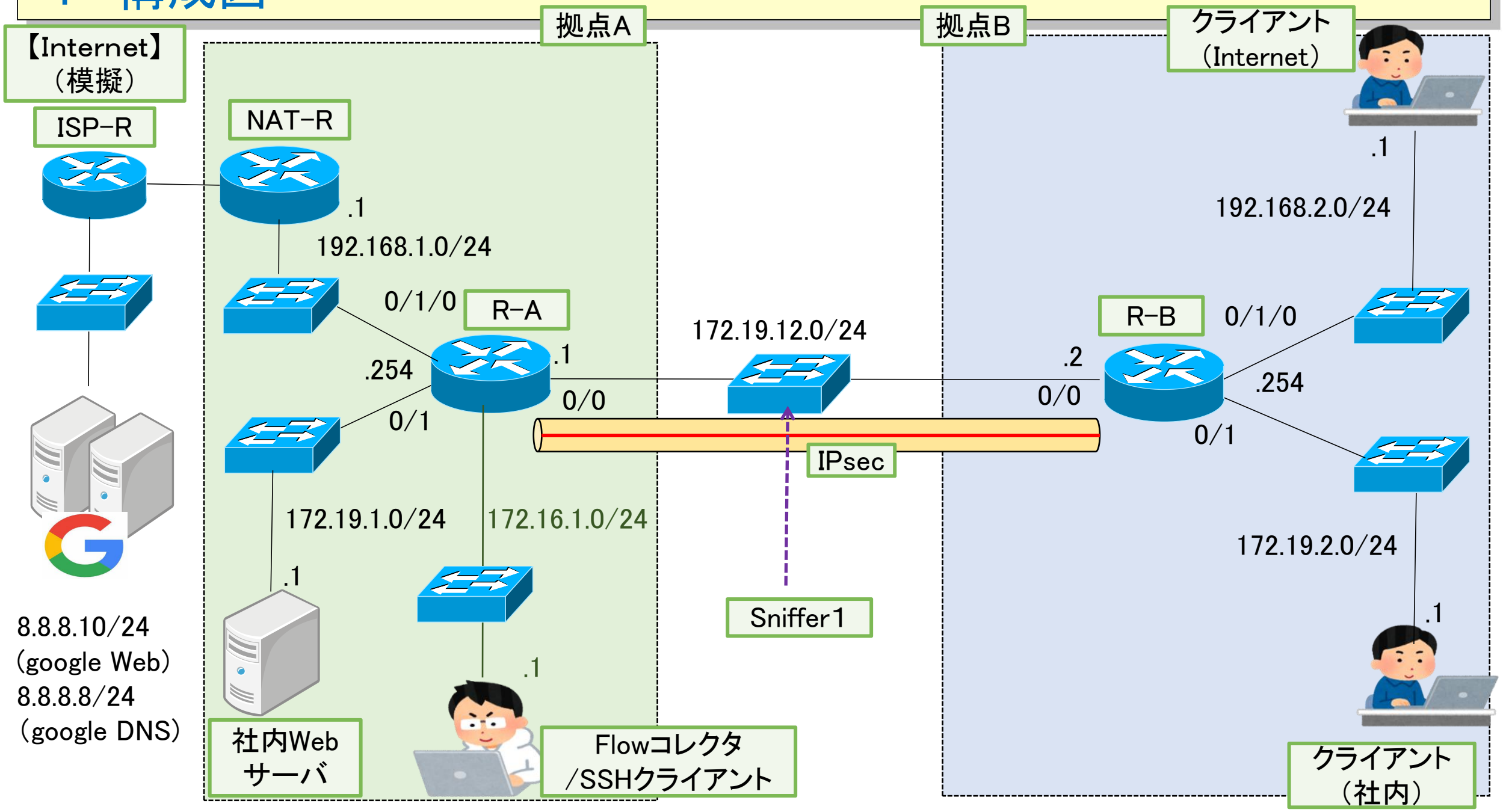
３　構成後の機能確認

４　参考資料
（1）インタフェースモジュールの追加例
（2）Netflowによるトラヒックの確認
（3）ルータへのSSH設定及び確認

一応、今回の構成例　sougou-1-mihon.pkt を用意しました！
（ですが。。今回は構成図及び構成条件を元に最初から作成してみてください！）

1 構成図

1　構成図


【Internet】
（模擬）
ISP-R
NAT-R
拠点A
拠点B
クライアント
（Internet）
.1
192.168.2.0/24
192.168.1.0/24
0/1/0
R-A
R-B
0/1/0
.254
.1
.2
0/0
0/0
0/1
0/1
172.19.12.0/24
IPsec
Sniffer1
172.19.1.0/24
172.16.1.0/24
172.19.2.0/24
.1
.1
.1
8.8.8.10/24
(google Web)
8.8.8.8/24
（google DNS）
社内Web
サーバ
Flowコレクタ
/SSHクライアント
クライアント
（社内）

2　構成条件

２　構成条件

（提供サービス）
拠点A～拠点B間において以下のさーびす
　①　拠点Bクライアント→拠点Aサーバに対するWebアクセス
　②　拠点Bクライアント→拠点AのNAT-R経由によるインターネットアクセス

（監視条件）
　拠点Aの保守端末は以下の機能を具備します。
　　各NW機器に対するSSHアクセス
　　Netflowによるトラヒック確認

（回線条件）
　拠点A～拠点BにおいてはVPNルータにより秘匿（IPSEC）を実施
＜秘匿対象は全サービスとする＞

（構成及び使用アドレス）
　１　構成図のとおり

３　　構成後の確認

３　構成後の機能確認

（提供サービスの機能確認）
拠点A～拠点B間において以下のサービスが提供できるかを確認してください
　①　拠点Bクライアント→拠点Aサーバに対するWebアクセス
　②　拠点Bクライアント→拠点AのNAT-R経由によるインターネットアクセス

（監視条件の機能確認）
　拠点Aの保守端末から以下の動作が可能かを確認してください。
　　各NW機器に対するSSHアクセス
　　Netflowによるトラヒック確認

（回線条件の機能確認）
　拠点間VPNルータにより秘匿（IPSEC）できているかを以下の方法で確認してください
　　・ルータのIPSEC関連コマンドおょびアクセスリスト（カウンタ）での確認
　　・Snifer0による各提供サービスのトラヒックが秘匿（ESP）されているか？

4　参　考

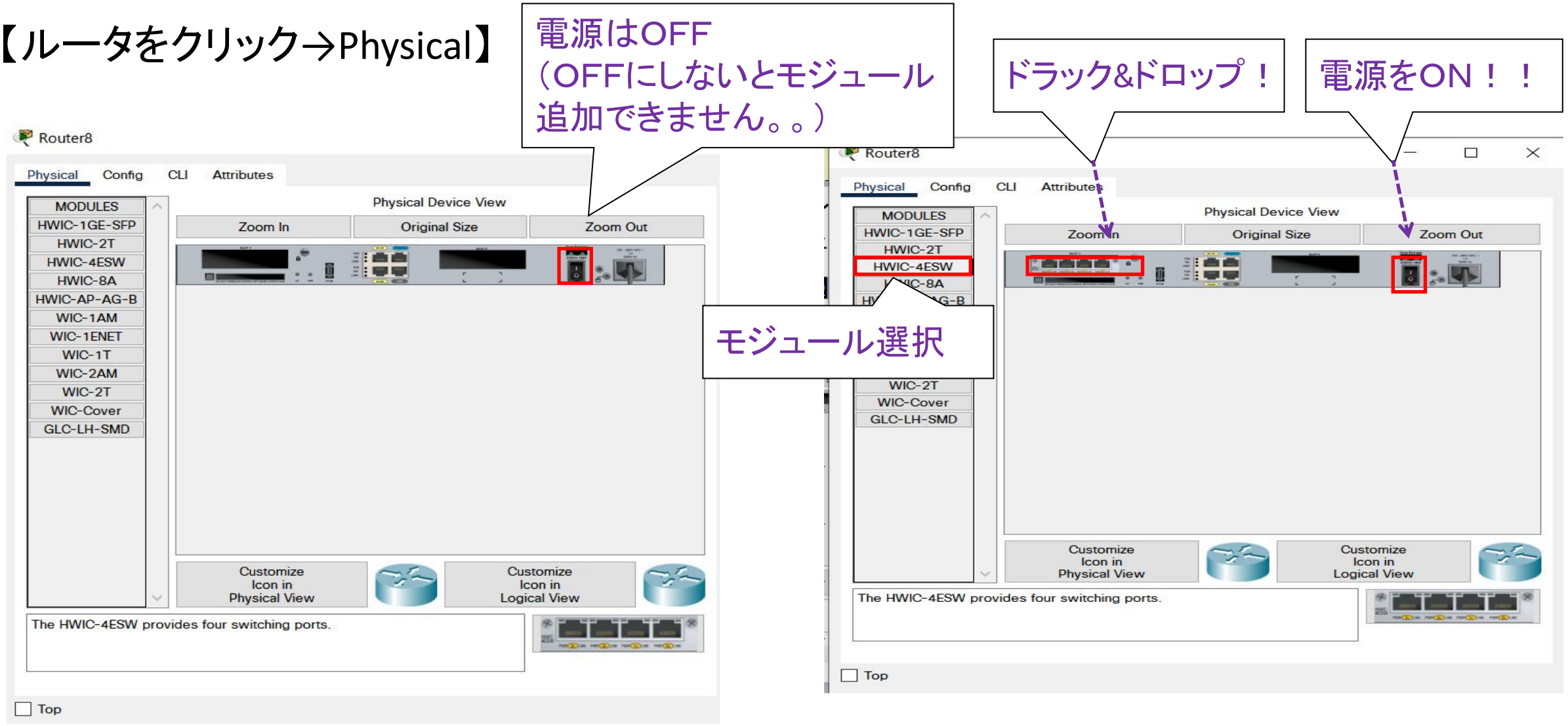
（1） インタフェースモジュールの追加例

4　参考資料

（1）　インタフェースモジュールの追加例

今回のルータはインターフェースが足らない。。ので以下の要領で追加しました！

【ルータをクリック→Physical】



4　参考資料

（1） インタフェースモジュールの追加例

モジュール追加後、インタフェースが認識しているかを確認！

（追加前）

```
Router#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

（追加後）

```
Router#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        unassigned      YES unset  administratively down down
FastEthernet0/1/0      unassigned      YES unset  up                    down
FastEthernet0/1/1      unassigned      YES unset  up                    down
FastEthernet0/1/2      unassigned      YES unset  up                    down
FastEthernet0/1/3      unassigned      YES unset  up                    down
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

４　　参　　考

（２） Netfowの設定および確認

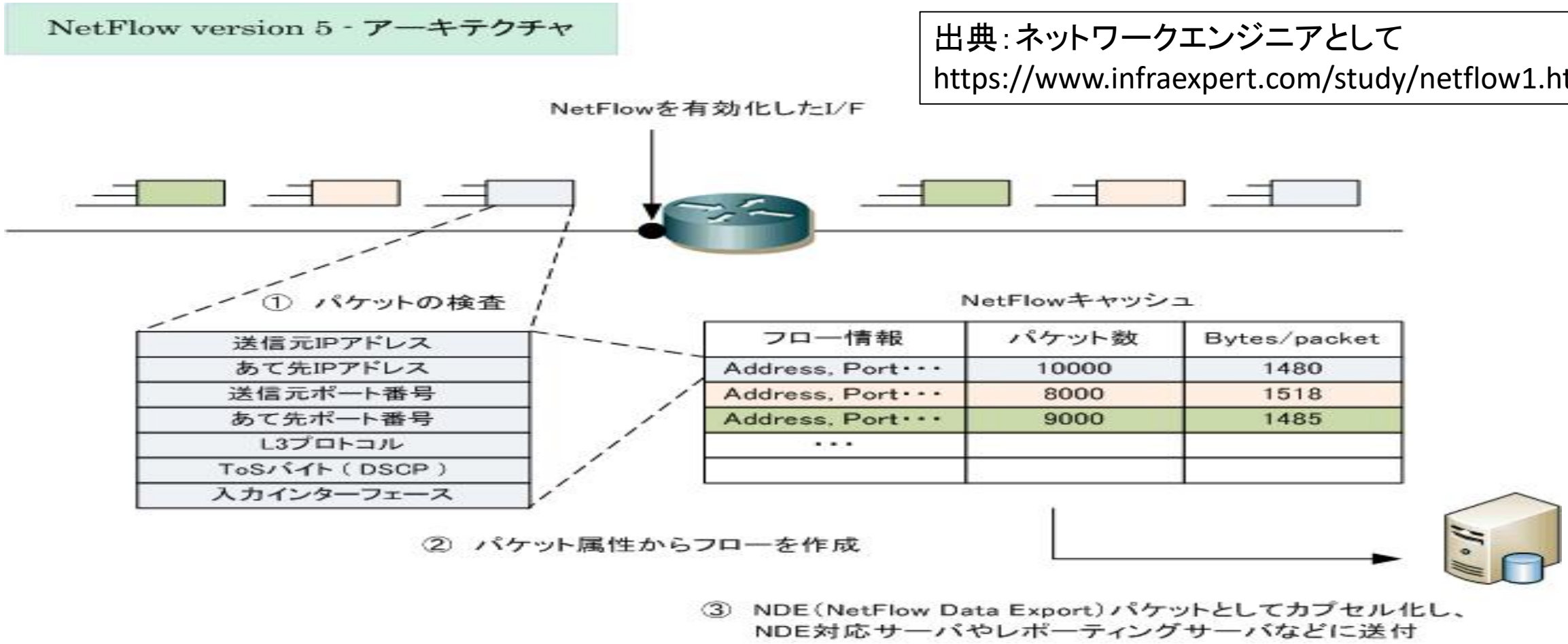
4　参考資料

（2） Netfowの設定および確認

○　Netflowとは？？

ネットワーク上で流れるトラフィックフローを受動的にモニタできる機能のことです。
NetFlowはIOSの機能の1つであり、1996年にCiscoが開発しました。

出典：ネットワークエンジニアとして
https://www.infraexpert.com/study/netflow1.html



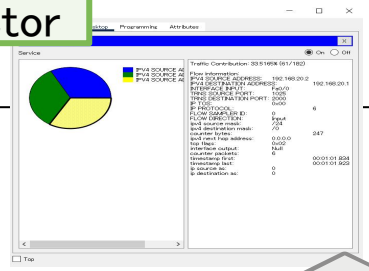
4　参考資料

（2）　Netfowの設定および確認

○　Netflow設定及び確認イメージ

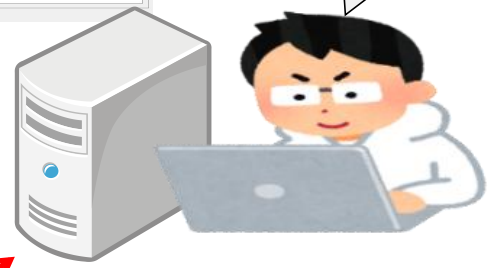
① エクスポータ（NW機器）に設定を投入

```
ip flow-export destination 192.168.110.1 9996
ip flow-export version 9
int fa0/0
ip flow ingress      /受信トラヒックを対象
ip flow egress       /送信トラヒックを対象
```



Netflow
Collector

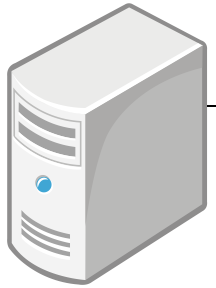
④ コレクター
により確認



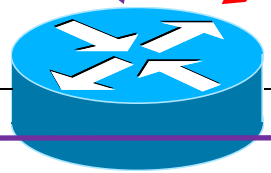
IP　：192．168．110．1

③ コレクター
にFlowを送信

サーバ



fa0/1



fa0/0

クライアント

Netflow
エクスポータ

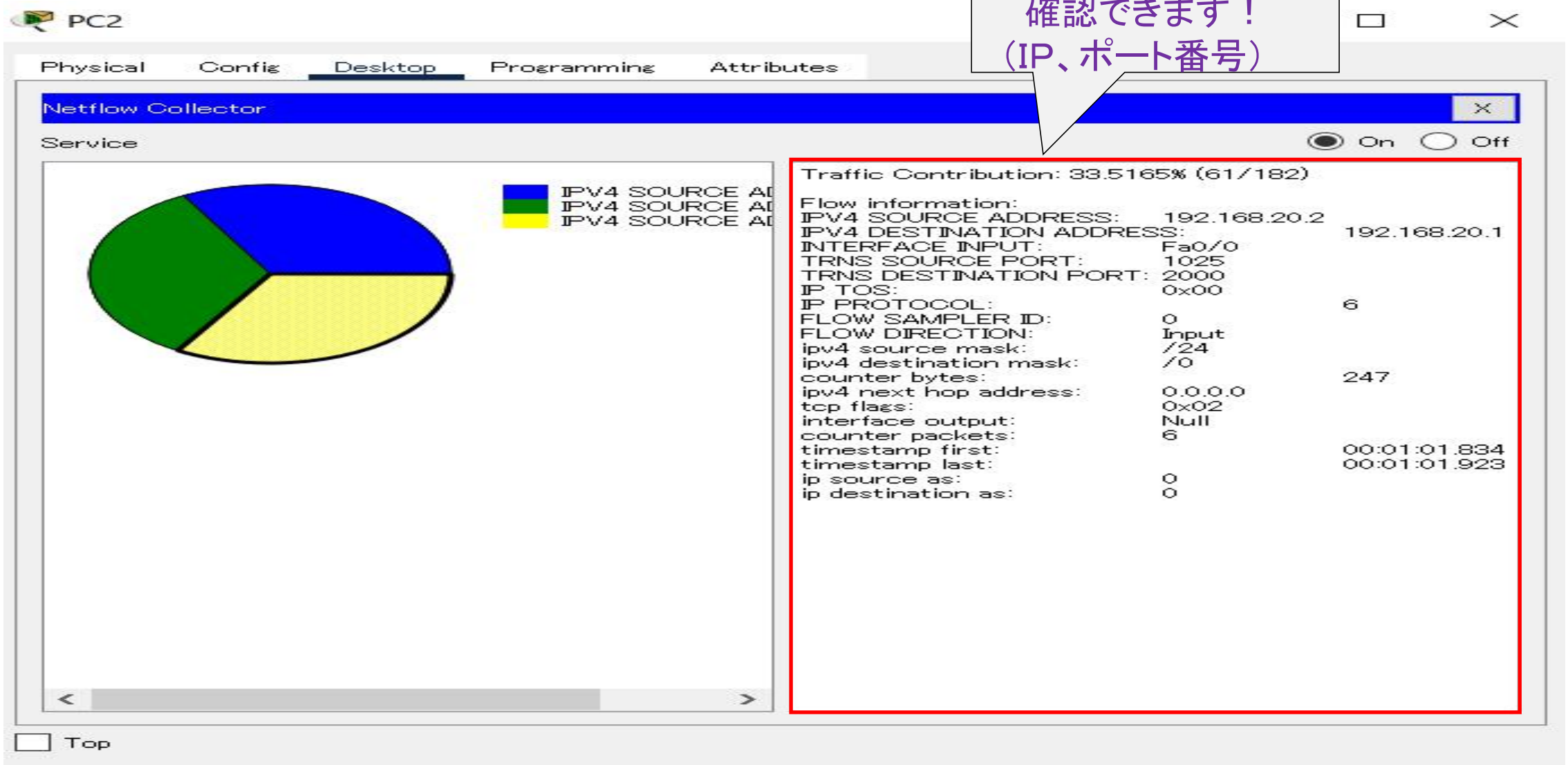
② トラヒックが通過

4　参考資料

（2） Netfowの設定および確認

○　Netflowコレクターの出力例

フロー結果が
確認できます！
（IP、ポート番号）



4　参考資料

（2） Netfowの設定および確認

○　Netflowエクスポータでの確認（例）

#show ip cache flow　コマンドで確認できます！

```
R-2#show ip cache flow
IP packet size distribution (261 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .939 .023 .038 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 118 added
  1 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol          Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------          Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-H323              1      0.0         6    41      0.0       3.0      15.0
UDP-DHCP              2      0.0         5    77      0.0       0.5      15.0
UDP-other           113      0.0         2    28      0.011250534.9      15.0
Total:              116      0.0         2    30      0.010959572.9      15.0

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa            192.168.20.1    Local         192.168.110.1   11 0000 270c     2
Fa            192.168.20.1    Local         192.168.120.1   11 0401 0401     1
R-2#
```

この例では
H323：VOIPの呼制御プロトコル
その他プロトコルが確認できる！！

４　　参　　考

（３） ルータのSSH設定及び確認

４　参考資料

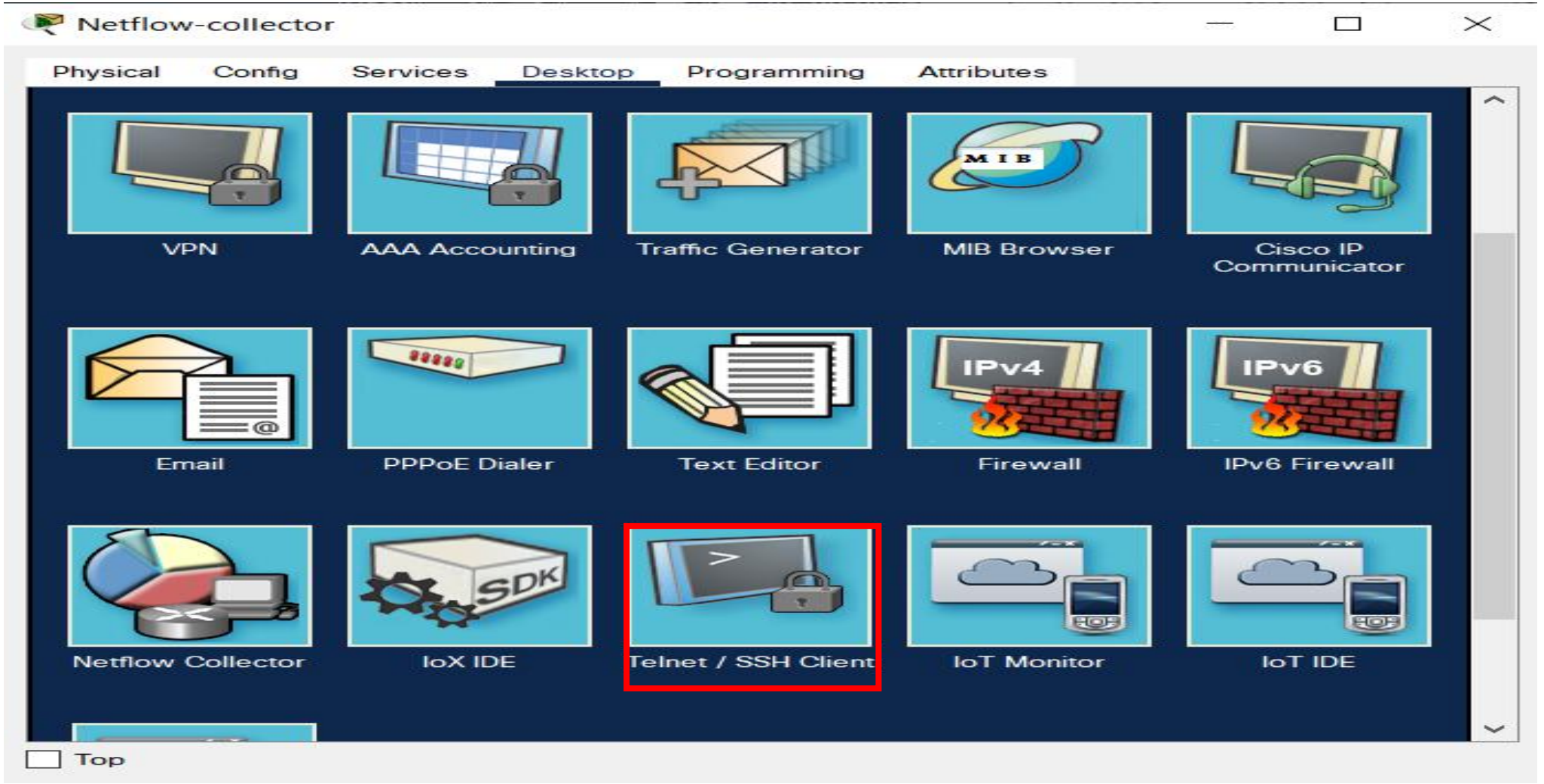
（３） ルータのSSH設定及び確認

```
R-B(config)#username admin password cisco                    /SSHログイン時のユーザ名/パスワード）
R-B(config)#ip domain-name cisco
R-B(config)#crypto key generate rsa
The name for the keys will be: R-B.cisco
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024                      /  RSAキーは1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*Mar 1 2:19:31.282: %SSH-5-ENABLED: SSH 1.99 has been enabled
R-B(config)#ip ssh version 2
R-B(config)#line vty 0 4                                     /ルータへのリモート接続
R-B(config-line)#login local                                 /ローカルユーザを使用
R-B(config-line)#transport input ssh                          /SSH接続を許可
R-B(config-line)#exit
R-B(config)#
R-B(config)#enable secret cisco                               /enable   Secret設定（Cisco）
R-B(config)#
```

4　参考資料

（3） ルータのSSH設定及び確認

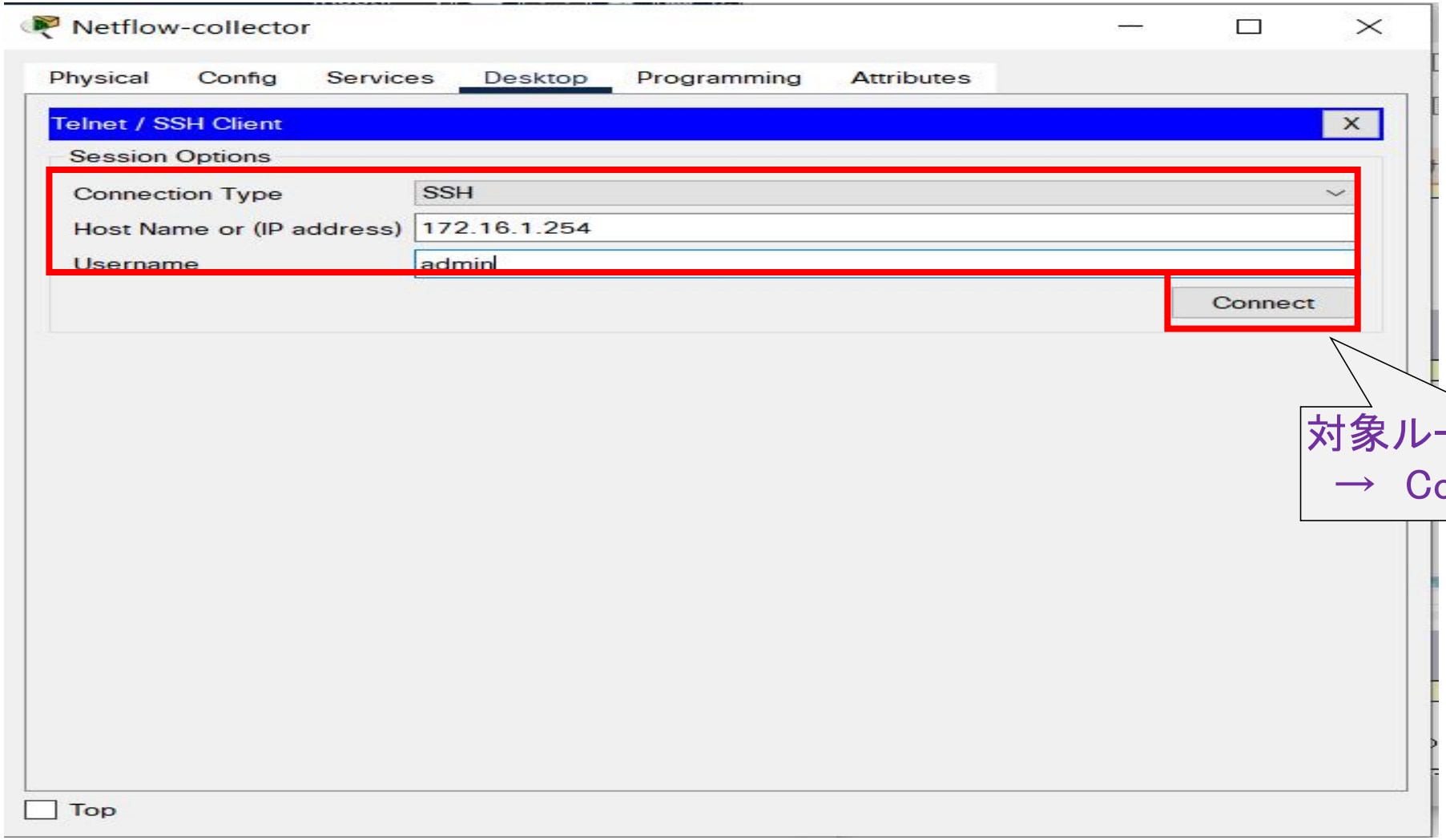
SSHクライアント使用方法



4　参考資料

（3） ルータのSSH設定及び確認

SSHクライアント使用方法



対象ルータを指定
→　Connect

4　参考資料

（3） ルータのSSH設定及び確認

SSHクライアント使用方法