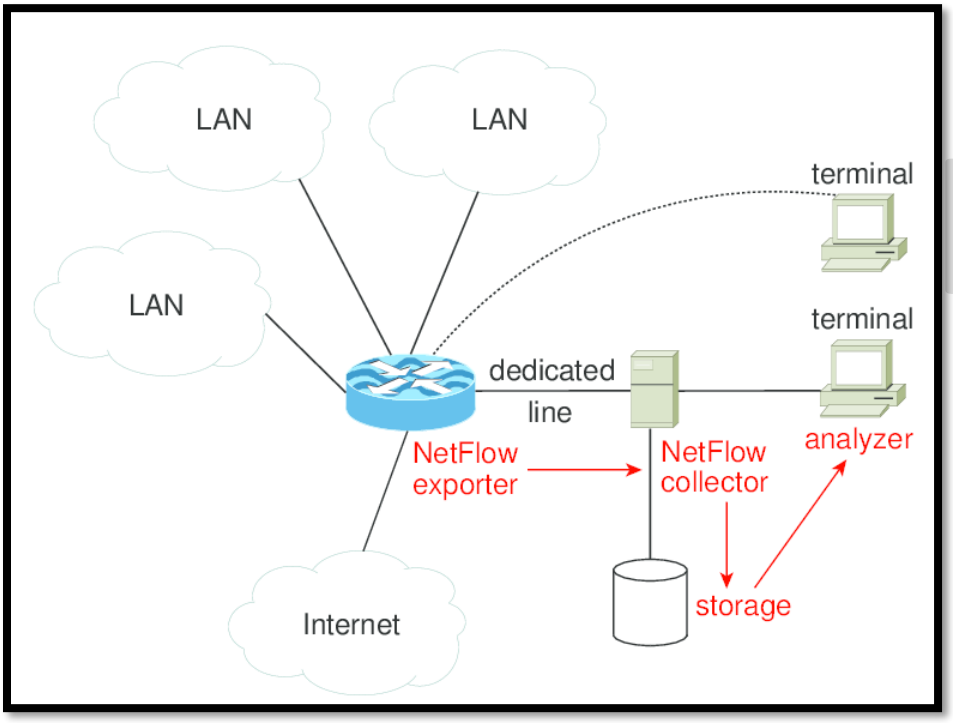

Networkforyou
Welcome
To
Network for you
CISCO NetFlow
Networkforyou

CISCO NetFlow:

- **Network management protocols like SNMP allow us to monitor our network**.
- We can check things like **cpu load, memory usage, interface status and even the load of an interface**
- One of the things we can't do with those tools (SNMP) is **tracking all flows in our network**.
- A flow is a stream of packets that share the same characteristics like source/destination port, source/destination address, protocol, type, service marking, etc.
- **NetFlow allows us to track these flows on our network.**
- We can use this information to solve problems like bottlenecks, **identify what applications** are used, how much bandwidth they use etc.
- For each of the flows, NetFlow will track the number of packets sent, bytes sent, packet sizes and more.
- We can configure your router to keep track of all flows and then export them to a central server where we analyze our traffic.
- NetFlow is an application for collecting IP traffic information.
- NetFlow is a protocol developed by Cisco Systems to record all IP traffic flows.
- Flow characteristics are like source, destination port, address, protocol, type etc.
- NetFlow allows tracking these flows on in the network.
- NetFlow track the number of packets sent, bytes sent, packet sizes and more.
- Configure router to keep track of all flows and then export them to central server.
- NetFlow is a great protocol to get an insight in the network traffic.
- NetFlow allows seeing real time data on who/what is eating the bandwidth.
- NetFlow is used to collect data flows from routers & switches interfaces.
- NetFlow is an application that provides statistics on packets flowing through routers.
- NetFlow captures statistics on IP flows through a device.
- NetFlow allows collecting traffic and analyzing it through a program.
- NetFlow is configured in the interface configuration mode on a router.
- NetFlow monitor of ingress traffic, egress traffic, or both ingress or egress traffic.
- Specify the IP address of the NetFlow collector & UDP port of collector is listening.
- Provides statistics on packets flowing through a router or a switch.
- NetFlow collect and export the data to enable network & security monitoring.
- NetFlow collect & export data for network planning, traffic analysis & IP accounting.
- NetFlow records are exported to a NetFlow collector using UDP.
- The standard value is UDP port 2055, but other values can be set 9555 or 9995.
- NetFlow can be used for network accounting and security auditing.
- NetFlow consumes additional memory of devices to process.

Or in Simple words we can say

- One of the most important tasks of a network administrator is to monitor the health of our networks, learn how our bandwidth is being used, what applications are consuming it, when it needs upgrade…
- Although monitoring protocols like SNMP and SPAN (port mirroring) can help us answer some questions but they are not enough to give us an insightful view of our networks.
- Luckily we have another amazing tool: NetFlow!
- NetFlow is a networking analysis protocol that gives the ability to collect detailed information about network traffic as it flows through a router interface.
- NetFlow helps network administrators answers the questions of who (users), what (application), when (time of day), where (source and destination IP addresses) and how network traffic is flowing.



NetFlow Versions:

Version 1:

- First implementation, now obsolete, and restricted to IPV4 only.

Versions 2:

- Cisco internal version never released.

Version 3:

- Cisco internal version never released.

Version 4:

- Cisco internal version never released.

Version 6:

No longer supported by Cisco Encapsulation information.

Version 6 is not compatible with Cisco routers.

Version 7:

- Cisco-specific version for Catalyst 5000 series switches.
- Version 7 is not compatible with Cisco routers.

Version 8:

- Choice of aggregation schemes in order to reduce resource usage.

Version 5:

- Fixed format that cannot be added or extended.
- NetFlow version 5 only support IPv4.
- NetFlow version 5 added BGP support.
- Export data from main cache only.
- No real concept of ingress & egress flows.
- NetFlow added flow sequence numbers & additional fields.
- NetFlow Version 5 is standard & most common NetFlow version.

Version 9:

- NetFlow Version 9 support IPV4 and IPv6.

- Not backwards compatible with any previous version.
- Added additional information to flows & template based.
- Exports data from main & aggregation cache.
- NetFlow Version 9 support for MPLS.
- Support flow-record format known as Flexible NetFlow technology.
- NetFlow Version 9 is most important NetFlow version.

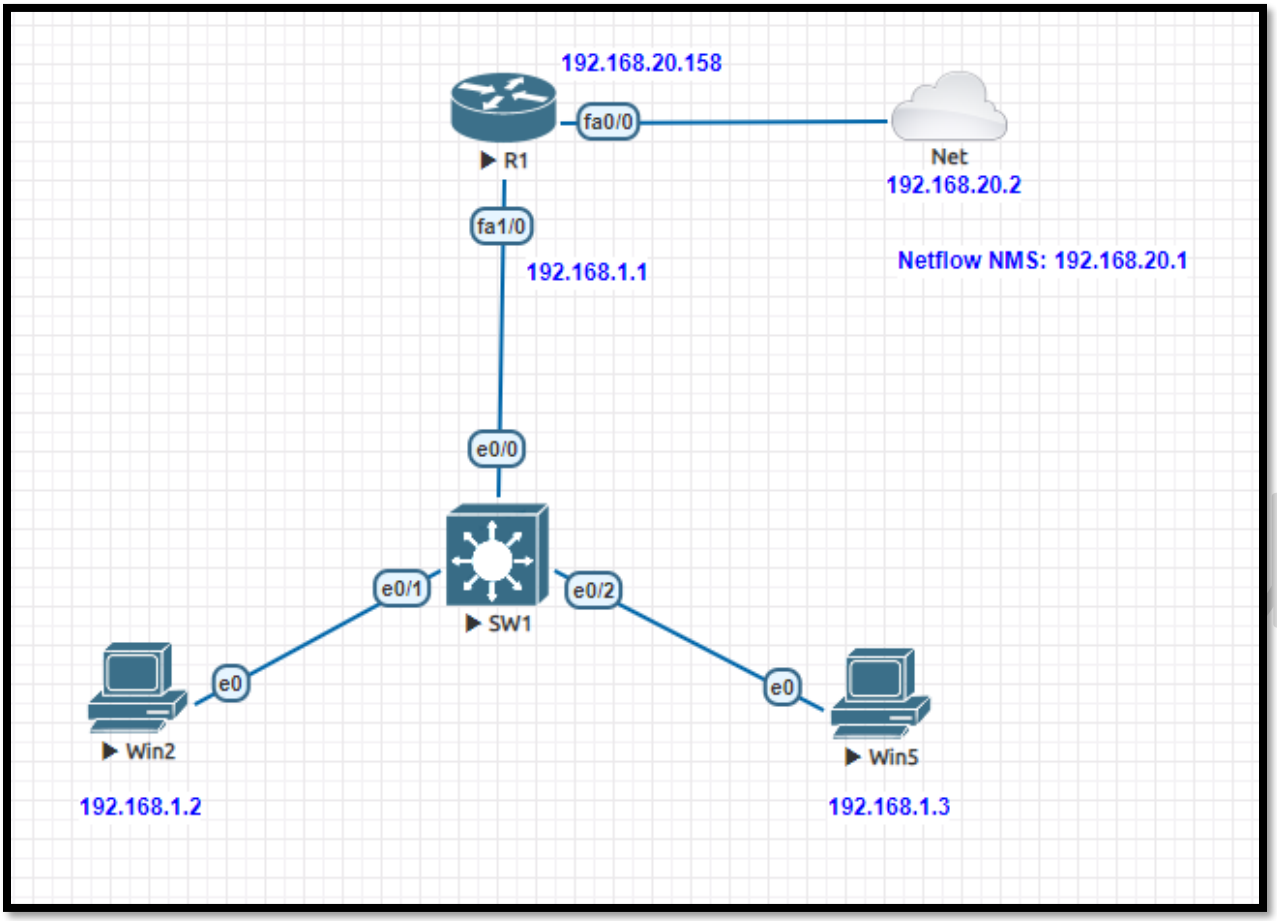
NetFlow uses the following fields to identify a unique flow:

- Source IP address
- Source port number
- Destination IP address
- Destination port number
- Layer 3 Protocol Type
- Type of service
- Logical input interface

Basic configuration:

Netflow Configuration Command	Description
R1(config)#ip flow-export source f0/0	We have to do is tell the router on what interfaces to track the flows
R1(config)#int f0/0 R1(config-if)#ip flow ingress R1(config-if)#ip route-cache flow R1(config-if)# ip flow egress R1(config-if)# exit	We will use the ip route-cache flow command. When you use this command, it will track all flows on the physical and all sub-interfaces. You can also use the ip flow egress or ip flow ingress commands
R1(config)#ip flow-export destination 192.168.20.1 2055	The router will export all flows to 192.168.20.1 with destination UDP port 2055
R1(config)#ip flow-export version 5	I will configure the router to use version 5
R1(config)#ip flow-cache timeout active 1	Export flow records every minute.
R1(config)#ip flow-cache timeout inactive 10	
Show Commands	Sh ip flow export
	Sh ip cache flow

Lab time:



R1 Configuration:
en config t hostname R1 int f0/0 ip add dhcp

no sh

int f1/0
ip add 192.168.1.1 255.255.255.0
no sh

ip domain-lookup
ip name-server 8.8.8.8

Netflow Configuration:

R1(config)#int f0/0
R1(config-if)#ip flow ingress
R1(config-if)#ip route-cache flow //I will use the ip route-cache flow command. When you use this command, it will track all flows
on the physical and all sub-interfaces. You can also use the ip flow egress or ip flow ingress commands
R1(config-if)#exit
R1(config)#ip flow-export destination 192.168.20.1 2055 //The router will export all flows to 192.168.20.1 with destination UDP port 2055
R1(config)#ip flow-export source f0/0 // we have to do is tell the router on what interfaces to track the flows
R1(config)#ip flow-export version 5 //I will configure the router to use version 9
R1(config)#ip flow-cache timeout active 1 //export flow records every minute.
R1(config)#ip flow-cache timeout inactive 10

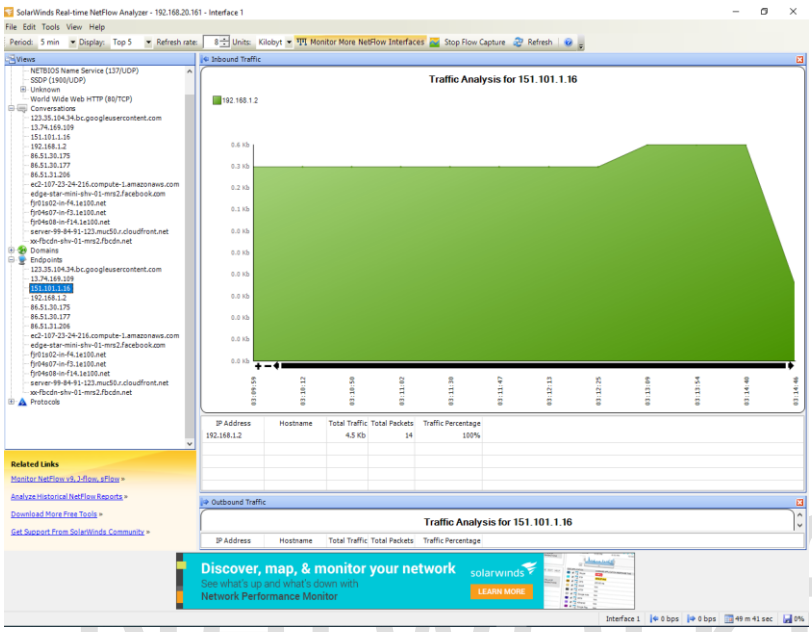
Show Command

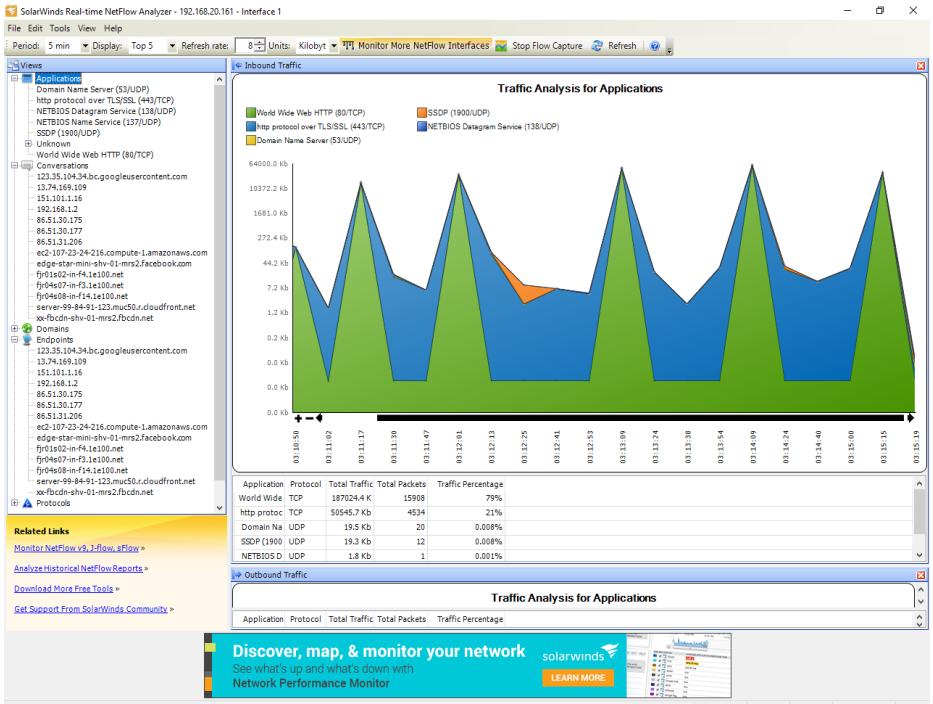
R1#show ip flow export
R1# show ip cache flow

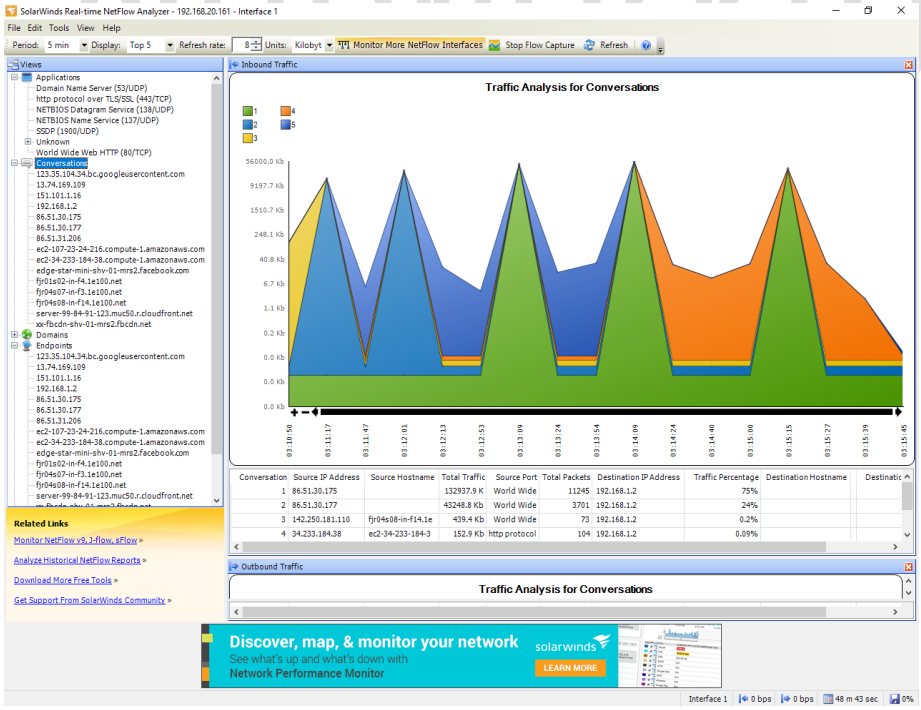
```
R1#sh ip flow export
Flow export v5 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Destination(1)  192.168.20.1 (2055)
  Version 5 flow records
  56 flows exported in 15 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
R1#sh ip cas
```

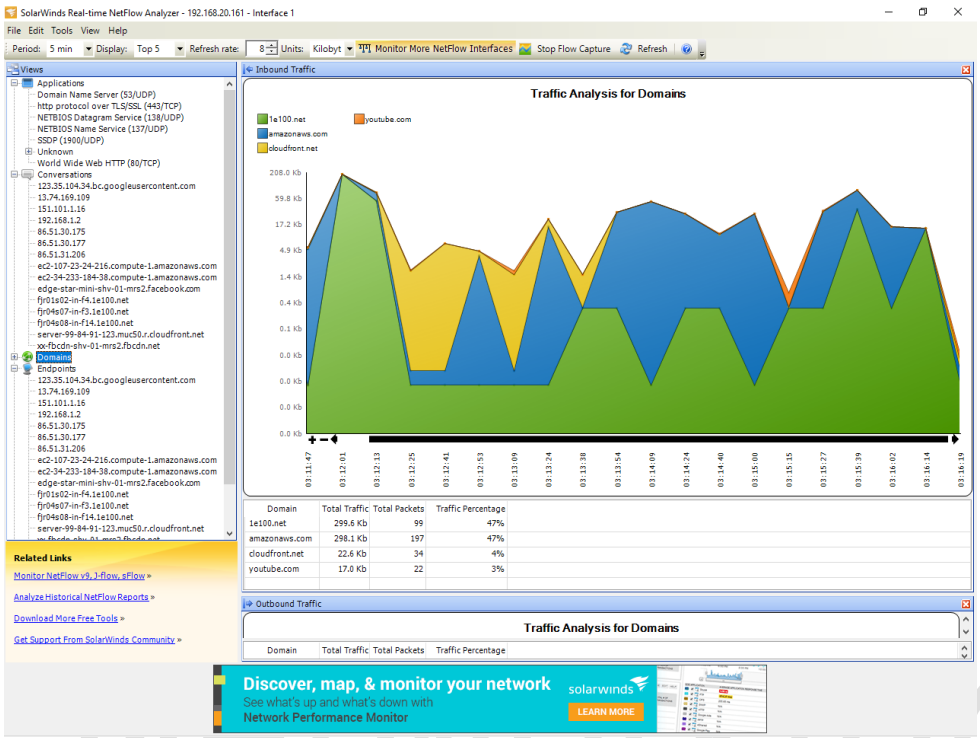
```
R1#sh ip cache flow
IP packet size distribution (29492 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .223 .000 .000 .000 .000 .000 .000 .000 .000 .000 .002 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .003 .001 .008 .753 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  2 active, 65534 inactive, 102 added
  2819 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 10 seconds
IP Sub Flow Cache, 533256 bytes
  2 active, 16382 inactive, 57 added, 57 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-WWW             48      0.0       550  1137     22.2      29.5      11.0
TCP-other           30      0.0         3   274      0.0       2.0      11.3
UDP-DNS              6      0.0         1    68      0.0       0.5      14.7
UDP-other           15      0.0         2   164      0.0       1.1      14.8
IGMP                 1      0.0         5    40      0.0       0.2      15.1
Total:             100      0.0       265  1131     22.3      15.0      11.9

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0         34.104.35.123   Fa1/0         192.168.1.2     06 0050 C041     1
Fa1/0         192.168.1.2     Fa0/0*        34.104.35.123   06 C041 0050     1
Fa1/0         192.168.1.2     Fa0/0*        86.51.30.175    06 C04B 0050   744
Fa0/0         86.51.30.175    Fa1/0         192.168.1.2     06 0050 C04B  3163
```

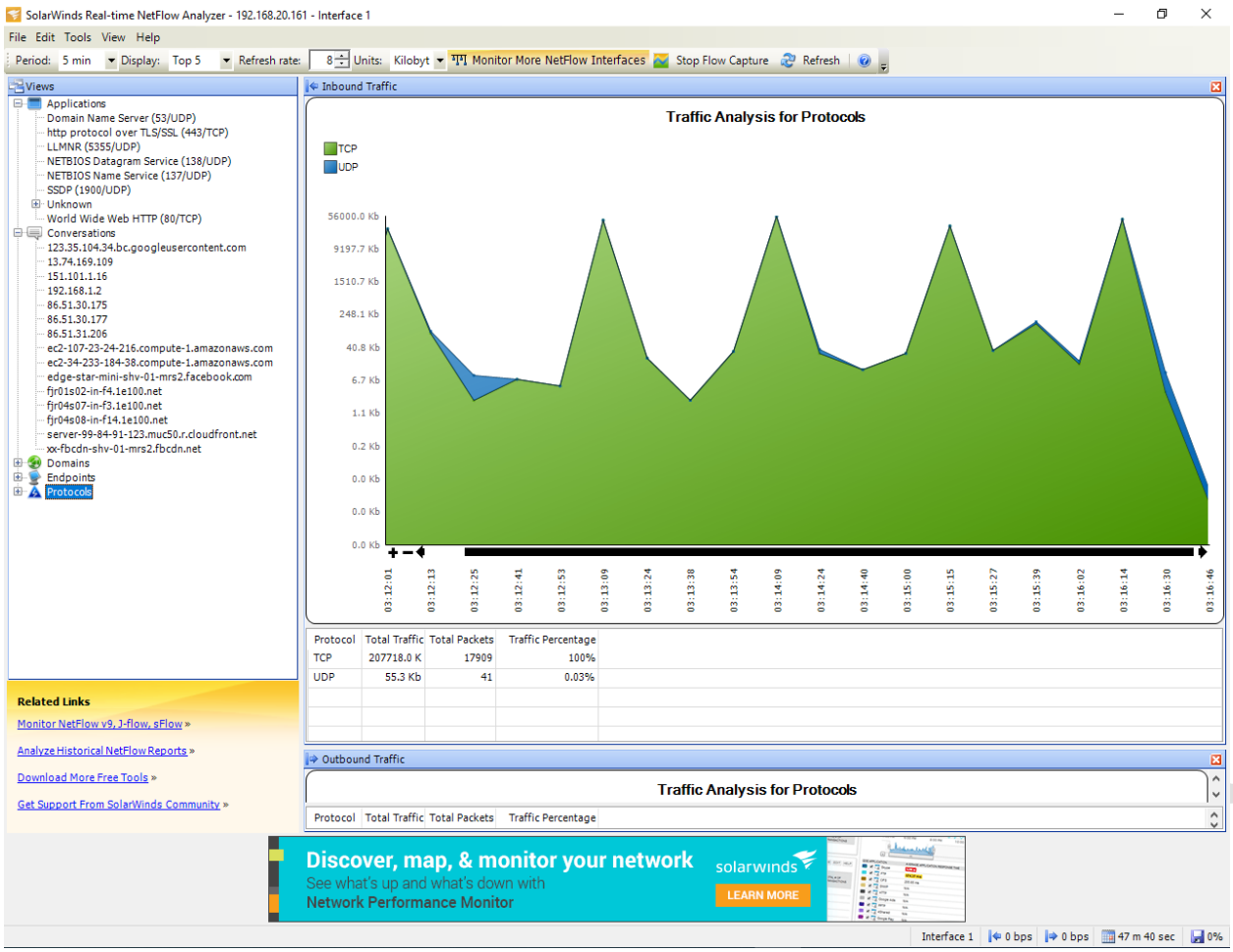
For Lab Purpose we will use SolarWinds Real Time Netflow Analyzer you can download from Net free.











Top Talker
R1(config)# ip flow-top-talkers R1(config-flow-top-talkers)# top 10 R1(config-flow-top-talkers)# sort-by packets
Sh Command
R1#sh ip flow top-talkers

```
R1#sh ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0         86.51.30.175    Fa1/0         192.168.1.2     06 0050 C0BE  1514
Fa0/0         216.58.208.225  Fa1/0         192.168.1.3     06 01BB C02A  1493
Fa0/0         172.217.21.36   Fa1/0         192.168.1.3     06 01BB C028   627
Fa1/0         192.168.1.3     Fa0/0*        216.58.208.225  06 C02A 01BB   514
Fa1/0         192.168.1.2     Fa0/0*        86.51.30.175    06 C0BE 0050   366
Fa0/0         157.240.195.35  Fa1/0         192.168.1.3     06 01BB C023   167
Fa1/0         192.168.1.3     Fa0/0*        172.217.21.36   06 C028 01BB   165
Fa0/0         86.51.94.58     Fa1/0         192.168.1.3     06 0050 C024    86
Fa0/0         157.240.195.35  Fa1/0         192.168.1.3     06 01BB C032    11
Fa0/0         52.205.139.193  Fa1/0         192.168.1.2     06 01BB C16E    11
10 of 10 top talkers shown. 28 flows processed.

R1#sh ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0         172.217.21.36   Fa1/0         192.168.1.3     06 01BB C028  1870
Fa1/0         192.168.1.3     Fa0/0*        172.217.21.36   06 C028 01BB   525
Fa0/0         157.240.195.35  Fa1/0         192.168.1.3     06 01BB C023   457
Fa0/0         172.217.19.3    Fa1/0         192.168.1.3     06 01BB C02C   219
Fa0/0         86.51.30.175    Fa1/0         192.168.1.2     06 0050 C0BE    42
Fa1/0         192.168.1.3     Fa0/0*        157.240.195.35  06 C023 01BB    32
Fa1/0         192.168.1.3     Fa0/0*        172.217.19.3    06 C02C 01BB    31
Fa0/0         142.250.181.78  Fa1/0         192.168.1.3     06 01BB C041    25
Fa1/0         192.168.1.3     Fa0/0*        142.250.181.78  06 C041 01BB    14
Fa0/0         52.205.139.193  Fa1/0         192.168.1.2     06 01BB C16E    14
10 of 10 top talkers shown. 43 flows processed.
```