https://dx.doi.org/10.22161/ijaers.4.12.9 ISSN: 2349-6495(P) | 2456-1908(O)

Using Netflow Protocols to Identify and Assess the Network Packet Flows in Unsecured Network Environments

Desta Dana

B.Sc. , M.Sc. in Information Technology, Lecturer of Wolaita Sodo University, Ethiopia

Abstracts— *The Network Packet Flow is analyzed and defined by the network administers in the company to assure the exact data flow in the networked systems. Currently, in the world the data flow is unreliable in the internet because of unreliability of the internet. So in My research I dully answered to identify and asses the network administrator can record the ingress and egress of the packet flow-in and flow-out in the routers respectively. Therefore the network environment is reliable, identified and assessed by using the network simulators called packet tracer and the protocol of NETFLOW protocol implementation in this research works.*

Keywords—Assess, Environments, Identify, NetFlow Protocol, Network, Packet Flow, Unsecured.

I. INTRODUCTION

In the computer network environments there is unsecured network is familiar in the world. Therefore, it's most often refers to a free temporary LAN users, Wi-Fi (wireless) network, like at a coffeehouse, retail store. It means there's no special login or screening process to get on the network, which means you and anyone else can use it. So that it means to you is that there's no guarantee of security while you use that network not secured).

So, if a hacker or false network users were nearby and felt like doing dirty deeds online on that unsecure network, there's very little that can stop him. Most of the time as we have faced in different organization we've all used free Wi-Fi by Laptop other smart phones, we all accessed our systems as temporarily and others in different environments like Cafe, Airport, Mall, city centers, public library, and even if inside rails. In these bad environments there is packet flows in and out of source and destinations i.e. the packet flow, is run through the IP process to segment the stream into a consistent packet data structure, which is easily routed through network paths. In generally the network packets is nothing but it's the data which flows from the sender to receivers.

Packets enable resilient network designs by creating uniform, stateless, independent data chunks. Packet networking has been the preferred method for networking for the last 20 years (but it's not only one). The use of packets remains a sound technical concept for abstracting the forwarding path from the payload, Focus on the network, don't be concerned about the data.

But consider common use cases for the network. The user wants to see a Web page load smoothly and quickly. The Web developer wants the Web browser to request an image, an HTML file or a script file from the Web server and load rapidly. For a sys admin, the OS opens a socket to manage a connection to a remote system and to stream data through it. These use cases are all about flows of data, but the network supports the delivery as a series of packets.

And consider the hosts at either end of the connection. In the past, servers were always located on a single port of a switch. Clients were located at a specific WAN connection or on a specific switch in the campus LAN. Packets ingressed(incoming) and egressed(outgoing)the network at known locations and the ports.

Packet assessing and identifying is based on the following basic requirements of A network flow is identified as a unidirectional stream of packets between a given source and destination—both are defined by a network-layer IP address and by transport-layer source and destination port numbers.

Specifically, a flow is identified as the combination of the following key fields are basics to identify the packets, to identify who sends to whom, on which times and other statistics of the network flows in detail.

- ✓ Source IP address
- ✓ Destination IP address
- ✓ Source port number
- ✓ Destination port number
- ✓ Layer 3 protocol type

- ✓ Type of service (ToS)
- ✓ Input logical interface

To identifying assessing the packets which are either ingressed or egressed we have used the algorithms and tools in our research, called NetFlow protocols and Packet tracer respectively.

So the Netflow protocols architectures in diagrammatically mentioned in Fig1. In Below. Which shows about the packet flows and the environments of the networks.

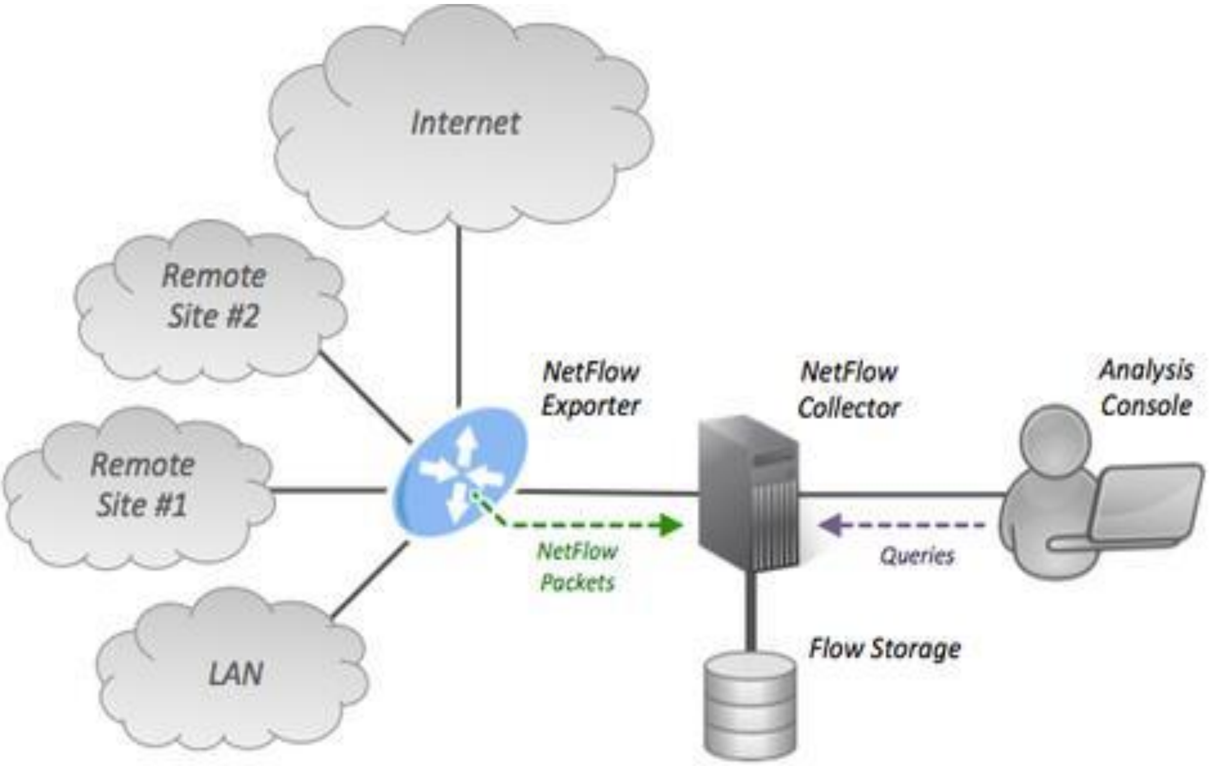


Fig.1: Architectural Design of NetFlow Protocol Implementations. [7]

As Fig 1. Shows the network administrator monitor and can assess each and every packets from the entire networks of the organization which are flowed in or ingress and flowed out or egress data for 24/7 services.

II. +METHODOLOGY

To gather each and every statistics of the network packet in our research we used free and open source software called Cisco Packet tracer which is Versions 6.1 as the simulators, as it mentioned in our experimental results in Fig.2 in below. The protocols that we have implemented in the research work is called NetFlow Protocol which is used to captures data from ingress (incoming) and egress (outgoing) packets. NetFlow gathers statistics of each packet sent and received at what times from which remotes sites. The following ingress IP packets identified by protocol:

IP-to-IP packets
IP-to-Multiprotocol Label Switching (MPLS) packets
Frame Relay-terminated packets
ATM-terminated packets

As it mentioned, in the Fig 2. The protocols which identifies data incoming and outgoing from the router by Fast Ethernet port (FE0 or FE0). The statistics of the overflow is captured in the memory of router called DRAM.

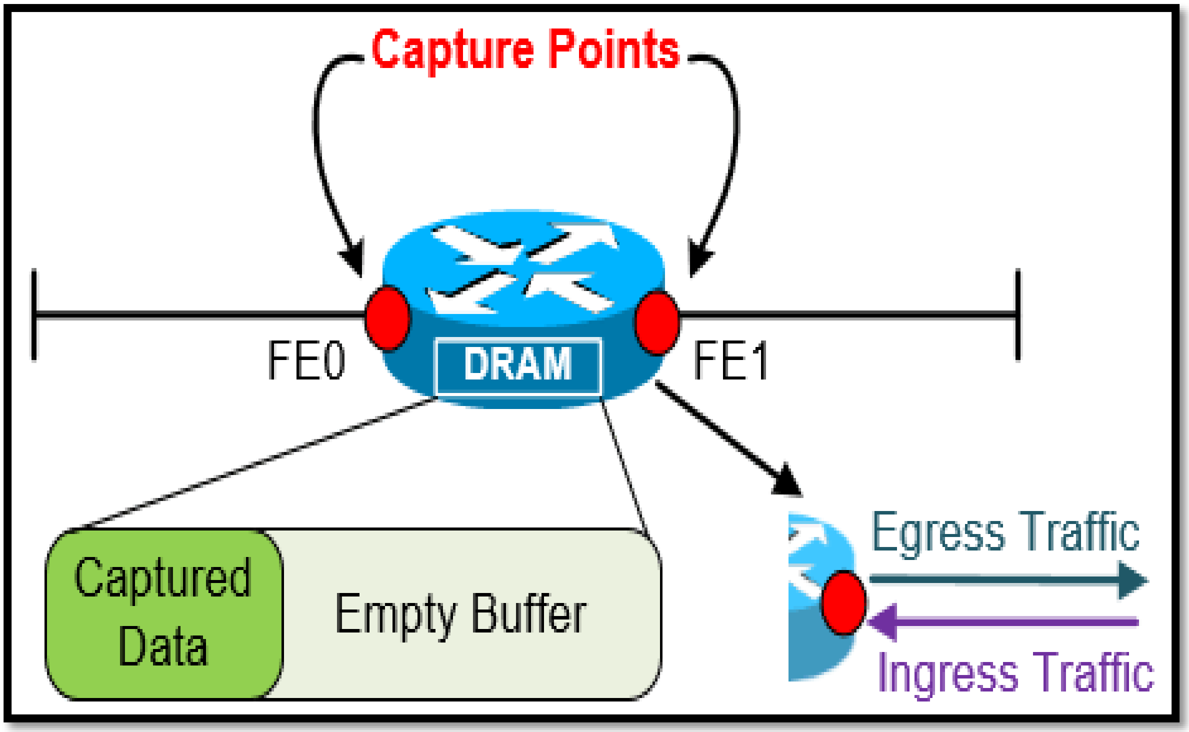


Fig.2: Ingress and Egress Packet [6]

And also: NetFlow captures data for all egress (outgoing) packets through the use of the following features:
Egress NetFlow Accounting:-NetFlow gathers statistics for all egress packets for IP traffic only.
NetFlow MPLS Egress:-NetFlow gathers statistics for all egress MPLS-to-IP packets.
In Netflows statistics the network administrator can assess, identify and answers all **WH** questions like

- ✓ From where the packets sent?
- ✓ To which system/ remote?
- ✓ To whom it sent?
- ✓ By what time interval?
- ✓ How many sizes of packets?
- ✓ How it sent like protocol?

III. RESULTS AND EXPERIMENTAL WORKS

In this study we have used the Packet tracer version 6.1. For the experimental simulation of how the NetFlow protocol is implemented in the real networks and how it's used to monitor and manage the organizational network to create secured network environments.

So, we have done the following steps in our works:
Step 01: Designing the network by using Packet tracer: for this study we have used one router with Fa0/0, DHCP server, Switch, PCs with 24 ports and straight through cables to connect the devices, and also Laptop computer with Console cables to configure the Protocols and network.
Step 02: Configuring the networks by using cisco commands [In this research we have configured the DHCP server and PCs, RouterFa 0/0 with IPAddress 192.168.1.1, 255.255.255.0]
Steps 03: Sending messages from one devices to another [we sent from Pc to PC, Router – PCs..etc]
Step 04: Monitoring the networks by using the Network statistics

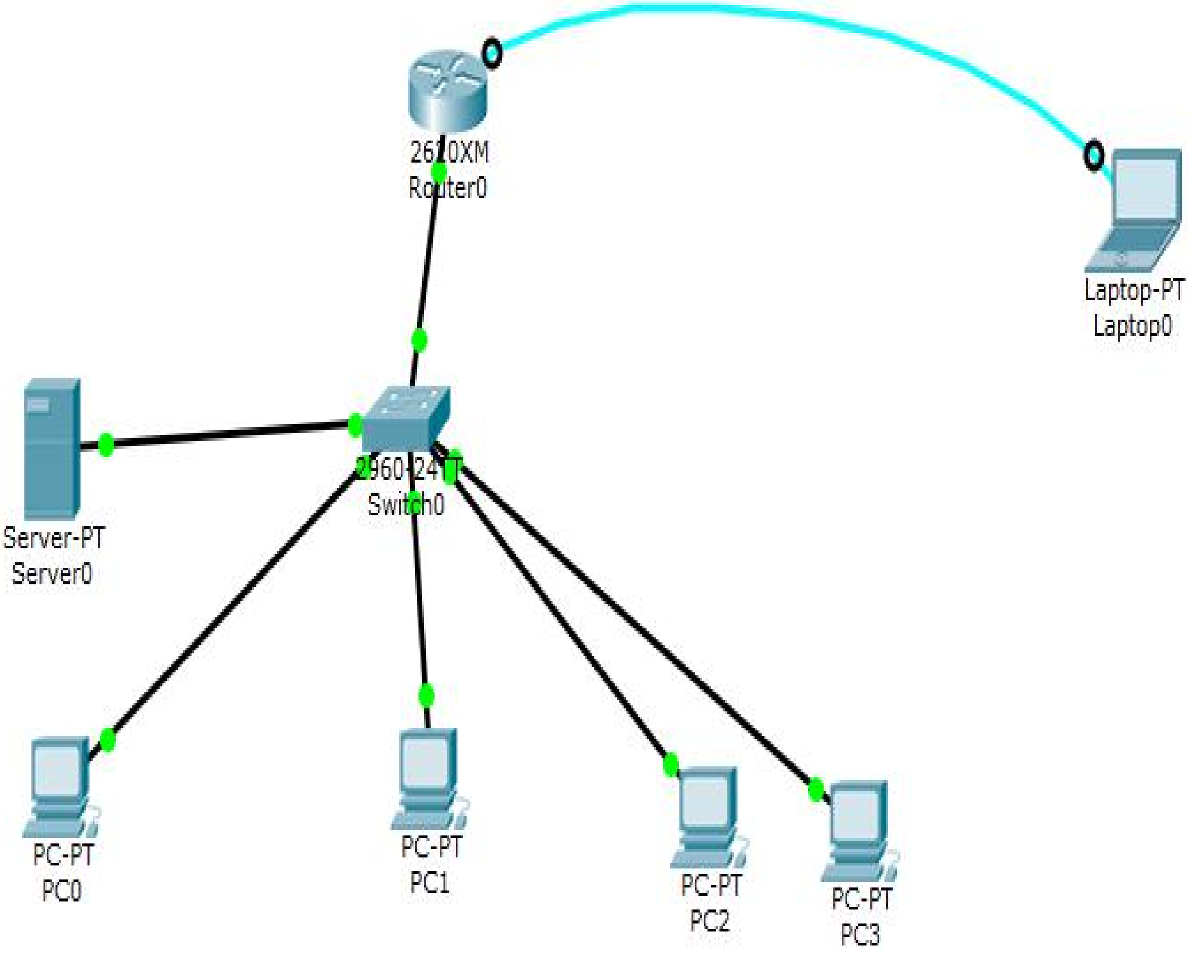
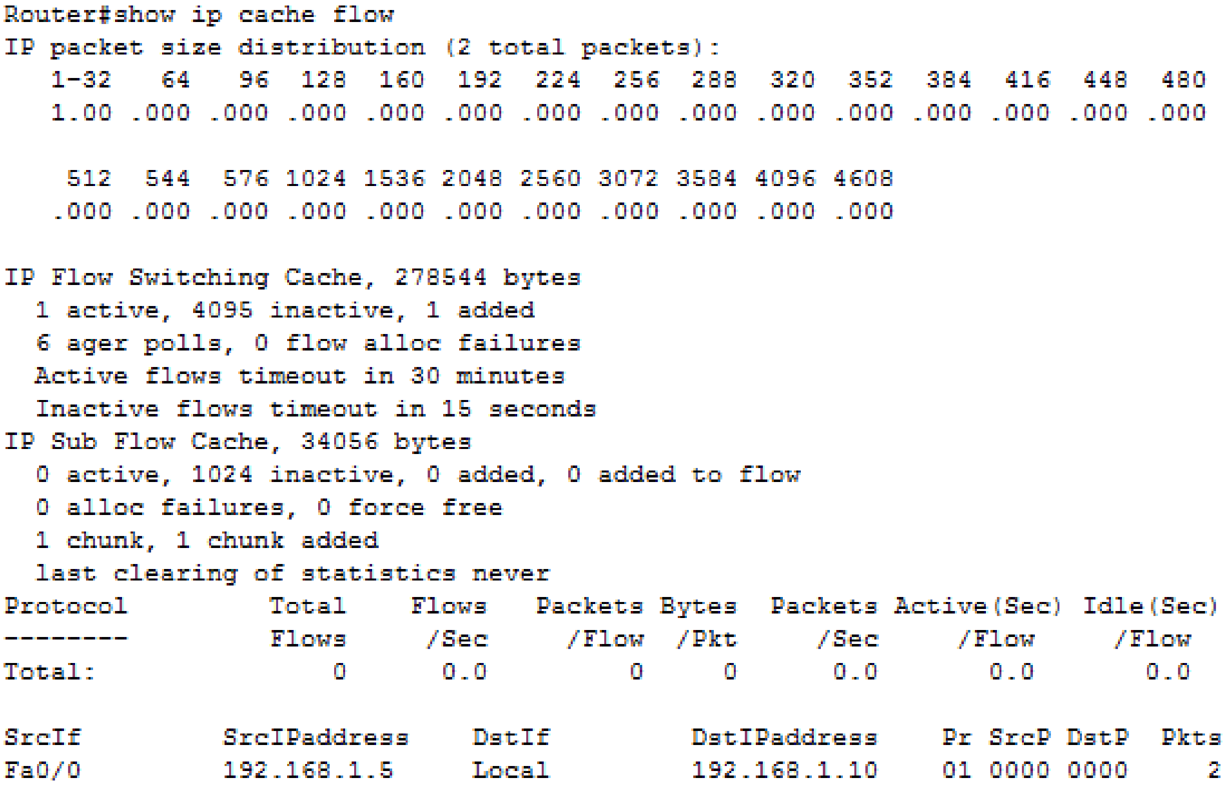


Fig.3: Simple Network Designs and NetFlow Protocol Implementations.

Network Configuration

```
Router Configurations: without username and password
configuring router interface fa 0/0, ip address and enabling the interface
Continue with configuration dialog? [yes/no]: n
Press RETURN to get started!
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fa0/0
Router(config-if)#ip address 192.168.1.10 255.255.255.0
Router(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Configuring The NETFLOW protocol
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fa0/0
Router(config-if)#ip flow ingress
Router(config-if)#ip flow egress
Router(config-if)#exit
Router(config)#ip flow dest
Router(config)#ip flow-export destination 1.0.0.255 2055
Router(config)#ip flow version 9
Router(config)#ip flow-export source fa0/0
Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Router#showip cache flow
```

Fig.4: Captured Statistics of the packet flow.



```
Router#show ip cache flow
IP packet size distribution (2 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   1.00 .000 .000 .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
  1 active, 4095 inactive, 1 added
  6 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
Total:               0      0.0         0     0      0.0       0.0       0.0

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0         192.168.1.5     Local         192.168.1.10    01 0000 0000     2
```

IV. DISCUSSION

Although flow-based analysis solutions are great, there are some areas where packet capture and analysis is still needed. Packet analysis is normally associated with SPAN or mirror ports, which are available on most managed network switches. “Port mirroring is used on a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port” [2]. Port mirroring on a Cisco Systems switch is generally referred to as Switched Port Analyser (SPAN) ; some other vendors have other names for it, such as Roving Analysis Port (RAP) on 3Com switches. Deep packet inspection (DPI) applies to technologies that use packets as a data source and then extract metadata such as application or website names. In contrast, flow data in most cases does not provide any information about what is contained within packet payloads. This network flow based analysis is working on the NetFlow v9 and Internet Protocol Flow Information Export (IPFIX) are available on some Cisco Integrated Services Routers (ISRs) and Cisco ASR 1000 Series Aggregation Services Routers (ASR1ks) with Next Generation Network based Application Recognition (NBAR2) enabled.[1,3,6].

When Network admin has to manage an increasingly complex IT environment, ensuring the reliability, availability and security of business services has become very demanding. Simple Network Management protocol (SNMP) monitoring is not enough anymore. Therefore to answer those challenges mentioned in above admin should have monitor each and every flow of the networks in and out of an organizations by using different methods as like We implemented protocols NetFlow. In general, NetFlow is rooted instrumentation within Cisco IOS Softwareof routers and cisco switches to characterize network operation. Visibility into the network is anvital tool for IT professionals. In short, new requirements and pressures, network operators are finding it critical to understand how the network is behaving including:[4,5,8]

- ✓ Application and network usage
- ✓ Network productivity and utilization of network resources
- ✓ The impact of changes to the network
- ✓ Network anomaly and security vulnerabilities
- ✓ Long term compliance issues

5. Conclusion: The NetFlow protocol is vital in unsecured networks environments which are used to monitor the traffic or packets flows, traffic analysis, security monitor, devices reporting and overall statistics of the networks. Therefore in this study we dully covered the protocol uses and services like we have designed the networks, we have configured the NetFlow protocol in the supportive router by using packet tracer simulator, we have seen the packet passing inside the devices and lastly by using the commands the results of network packet flow statistics is displayed. Generally the network admin should have implemented this protocol in any organizations to secure and monitor the entire network of organizations.

REFERENCES

[1] https://en.wikipedia.org/wiki/NetFlow,

[2] https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html, Accessed on Date July 15, 2017

[3] http://searchnetworking.techtarget.com/definition/ingress-filtering.\

[4] Eric D.Kolayzak(2014), Statistical Analysis of Network Data, Dept of Mathematics and Statistics, Boston University, ppt(1-50).

[5] https://www.netfort.com/wp-content/uploads/PDF/WhitePapers/NetFlow-Vs-Packet-Analysis-What-Should-You-Choose.pdf, Accessed on Date July 15, 2017.

[6] http://en.wikipedia.org/wiki/Traffic_analysis. Accessed on Date Oct 12,2017

[7] http://en.wikipedia.org/wiki/Port_mirroring. Accessed on Date Oct 12,2017

[8] http://unroutable.blogspot.com/2012/04/why-netflow-isnt-web-usage-tracker.html. Accessed on Date Oct 19,2017