Network Monitoring & Network Security

Akhilesh Kanduri

Cyber Crimes Investigator, Cyber Security and Cyber Forensics Expert

---***---

Abstract – *Network traffic monitoring refers to the oversight of a computer network using specialized management software tools. Network monitoring systems ensure the availability and overall performance of computers and network services. Network admins monitor access, routers, slow or failing components, firewalls, core switches, client systems, and server performance—among other network data. Network monitoring systems are typically employed on large-scalecorporate and university IT networks.*

1. INTRODUCTION

This Network traffic monitoring is an essential requirement for businesses that heavily rely upon IT for day-to-day operations. Many businesses deploy network monitoring as a means of reducing network infrastructure problems, improving network performance and increasing employee productivity. When it comes to ongoing daily operations, network monitoring is a critical part of maintaining the overall health of your internal network.

Network Traffic Management uses network monitoring tools and management techniques such as bandwidth monitoring, deep packet inspection and application-based routing to ensure optimal network operation. In doing so it helps maximise the performance and security of existing networks.

It also allows for the identification of network intensive operations that can be incorporated into network planning and growth strategies. Network Traffic Management is used alongside other optimisation techniques like Application Traffic Management as part of an overall Application Delivery Network solution.

In this article we will provide you with a general understanding of what network monitoring is, why it is used, how it works, and some of the tools that are used in the process.

Fig 1: Sample monitoring assumption

2. Network monitoring using Wireshark

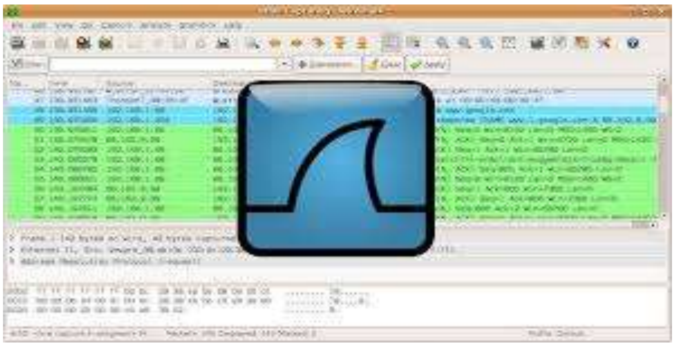


Fig 2: Wireshark interface

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course). In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

3. Some intended purposes

Here are some reasons people use Wireshark:

- Network administrators use it to troubleshoot network problems

- Network security engineers use it to examine security problems

- QA engineers use it to verify network applications

- Developers use it to debug protocol implementations

- People use it to learn network protocol internals Wireshark can also be helpful in many other situations.

Features

The following are some of the many features Wireshark provides:

- Available for UNIX and Windows.

- Capture live packet data from a network interface.

• Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many

other packet capture programs.

• Import packets from text files containing hex dumps of packet data.

• Display packets with very detailed protocol information.

• Save packet data captured.

• Export some or all packets in a number of capture file formats.

• Filter packets on many criteria.

• Search for packets on many criteria.

• Colorize packet display based on filters.

• Create various statistics.

4. Live capture from many different network media:

Wireshark can capture traffic from many different network media types, including Ethernet, Wireless LAN, Bluetooth, USB, and more. The specific media types supported may be limited by several factors, including your hardware and operating system.

5. Import files from many other capture programs:

Wireshark can open packet captures from a large number of capture programs. For a list of input formats see Input File Formats.

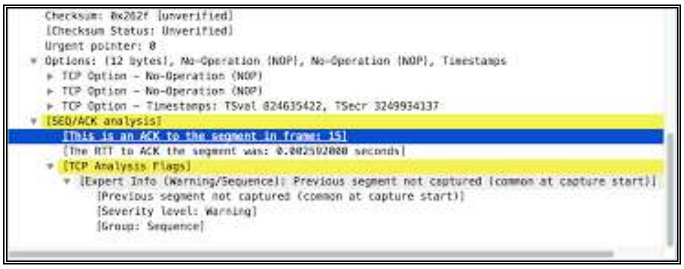
6. Export files for many other capture programs:

Wireshark can save captured packets in many formats, including those used by other capture programs. For a list of output formats see Output File Formats.

7. Open Source Software:

Wireshark is an open source software project, and is released under the GNU General Public License (GPL). You can freely use Wireshark on any number of computers you like, without worrying about license keys or fees or such. In addition, all source code is freely available under the GPL. Because of that, it is very easy for people to add new protocols to Wireshark, either as plugins, or built into the source, and they often do!

What Wireshark is not Here are some things Wireshark does not provide: • Wireshark isn't an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on. • Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things (except domain name resolution, but that can be disabled).



```
    Checksum: 0x202f [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▾ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    ▸ TCP Option - No-Operation (NOP)
    ▸ TCP Option - No-Operation (NOP)
    ▸ TCP Option - Timestamps: TSval 824635422, TSecr 3249934137
  ▾ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 15]
      [The RTT to ACK the segment was: 0.002592000 seconds]
    ▾ [TCP Analysis Flags]
      ▾ [Expert Info (Warning/Sequence): Previous segment not captured (common at capture start)]
          [Previous segment not captured (common at capture start)]
          [Severity level: Warning]
          [Group: Sequence]
```

Fig 3: Analysis of Wireshark

8. Network Security:

Network security is an integration of multiple layers of defenses in the network and at the network. Policies and controls are implemented by each network security layer. Access to networks is gained by authorized users, whereas, malicious actors are indeed blocked from executing threats and exploits.

Our world has presently been transformed by digitization, resulting in changes in almost all our daily activities. It is essential for all organizations to protect their networks if they aim at delivering the services demanded by employees and customers. This eventually protects the reputation of your organization. With hackers increasing and becoming smarter day by day, the need to utilize network security tool becomes more and more impotent.

9. Types of Network Security:

- Antivirus and Antimalware Software
- Application Security
- Behavioral Analytics
- Data Loss Prevention (DLP)
- Email Security
- Firewalls
- Mobile Device Security
- Network Segmentation
- Security Information and Event Management (SIEM)
- Virtual Private Network (VPN)
- Web Security
- Wireless Security
- Endpoint Security
- Network Access Control (NAC)

10. CONCLUSION:

Network traffic refers to the amount of data moving across a network at a given point of time. Network data is mostly encapsulated in network packets, which provide the load in the network. Network traffic is the main component for network traffic measurement, network traffic control and simulation. The proper organization of network traffic helps in ensuring the quality of service in a given network. Network traffic is also known as data traffic.

11. REFERENCES:

1. Ouritdept.co.uk

2. Technpedia.com

3. Official website of Wireshark.com

4. Cybercrime book by Akhilesh kanduri

5. Enterprise.comodo.com