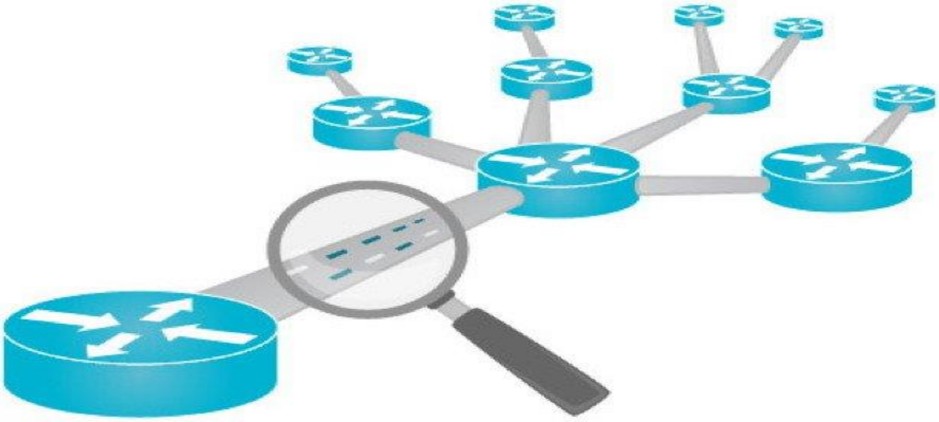
Monitoring and Analyzing Network Traffic

Network Traffic Monitoring and Analysis

Network traffic monitoring is the process of capturing network traffic and inspecting it closely to determine what is happening on the network. Network administrators should constantly strive to maintain a smooth network operation. If a network were down even for a small period of time, productivity within a company would decline. In order to be proactive rather than reactive, administrators need to monitor the traffic movement and performance to ensure a security breach doesn't occur within the network.



The network monitoring process involves sniffing the traffic flowing through the network. It requires capturing network packets and conducting a signature analysis to identify any malicious activity. Administrators should continuously monitor and analyze the network traffic to look for the presence of attack signatures.

Network operators use network-traffic analysis tools to identify malicious or suspicious packets hiding within the traffic. They monitor download/upload speeds, throughput, content, traffic and behaviors to understand what is going on in the network operations.

Advantages of Network Traffic Monitoring and Analysis

Network traffic analysis is done to get in-depth insight into what type of network packets or data is flowing through a network. Typically, it is done through network monitoring or network-bandwidth monitoring utilities. The traffic statistics from the network traffic analysis helps:

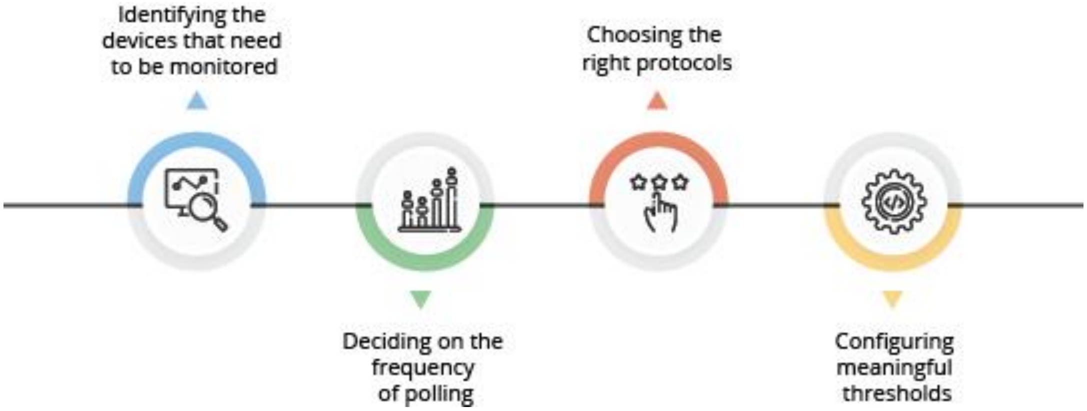
- Understand and evaluate the network utilization
- Download/upload speeds
- Type, size, origin, destination, and content/data of packets
- Understand how data flows in your network
- Optimize network performance
- Avoid bandwidth bottlenecks
- Detect signs of malicious activity
- Find unnecessary and vulnerable applications
- Investigate security breaches

The typical network monitoring advantages are:

- **Proactive**: Network monitoring proactively detects the applications that consume maximum bandwidth and reduce bandwidth. It manages the server bottleneck situation and other systems connected to the network. Network monitoring delivers an efficient quality of service to users. Network monitoring creates a record of all the irregularities occurring in the network that administrators handle later.
- **Utilization**: It is important to analyze the need for network utilization, especially with all the new and evolving technology. Network monitoring provides all the details on the infrastructure. This provides an idea about how much a network can handle during heavy traffic periods, which leads to the required utilization of the space in the network.
- **Optimization**: Network monitoring techniques gather the network infrastructure information in a timely manner and saves it for the administrator. The admin can then take the required actions before the situation worsens. Applications that prove vulnerable to the network are located by this technique.
- **Minimizing Risk**: Network monitoring techniques comprise all the required SLAs and compliance applicable to users or consumers. The complete infrastructure information is required when drafting the SLAs. Real-time monitoring of network topologies and channels helps document these SLAs.

Network Monitoring and Analysis: Techniques

A network administrator can implement two types of techniques to monitor their network. Each technique has advantages and disadvantages. It is recommended that both router-based and non-router-based techniques be used for the network-monitoring task.


Identifying the devices that need to be monitored
Deciding on the frequency of polling
Choosing the right protocols
Configuring meaningful thresholds

Router-based monitoring technique

In router-based monitoring, the functionality is hardcoded into the router. To use this functionality, it must first be enabled and configured using the router interface. With its built-in feature, it is less expensive, but offers less flexibility. This inbuilt feature uses SNMP monitoring, Netflow monitoring, and remote monitoring techniques to monitor the network.

Advantage: Extra software or hardware is not needed

Disadvantage: Less flexibility

Non-router-based monitoring technique

In non-router-based monitoring, a dedicated external hardware device or additional software is required to monitor your network. Because of this, it is more expensive than using a router-based technique. However, it offers more flexibility in monitoring than a router-based technique.

Advantage: More flexibility

Disadvantage: Extra monitoring software or hardware is required

Router-Based Monitoring Techniques

SNMP Monitoring

Simple Networking Monitoring Protocol (SNMP) is a part of the TCP/IP suite and functions on the application layer. SNMP helps administrators manage network performance by resolving network issues it encounters. The passive sensors implemented from a router to a host gather traffic statistics.

Elements of SNMP-based Monitoring

SNMP consists of a SNMP manager, SNMP agent, managed devices, and a management information base (MIB).

SNMP Manager: The SNMP manager is a system that maintains the proper network function. The communication between the SNMP manager and agents uses a message format. The SNMP manager controls and monitors the activities of the host. The main role of a SNMP manager is:

- Querying the SNMP agents
- Receiving a response from the SNMP agent
- Implementing changes to the agents
- Monitors asynchronous events from the agent

SNMP Agent: The SNMP agent maintains and saves the data for network devices. This data is passed on to the managing systems of the network. An SNMP agent can only work when a relationship is defined between a SNMP manager and a SNMP agent. The main role of SNMP agents is:

- Gathering management information
- Storing and retrieving management information
- Notify the SNMP manager if an event has occurred

Managed Devices: Network-based devices such as routers, switches, and servers require some form of monitoring and management.

Management Information base (MIB): The SNMP manager uses the device records saved by the SNMP agent. The sharing of this database is known as the Management Information Base. The MIB allows the SNMP manager to query SNMP agents about the devices.

SNMP Commands: The SNMP commands make the implementation of SNMP less complex for administrators. Here are the SNMP commands:

- **GET**: It retrieves the information from the managed device. It is used by SNMP managers
- **GET NEXT**: Works similar to GET and also retrieves the object identifiers from the MIB
- **GET BULK**: Retrieves large amounts of data from the MIB
- **SET**: SNMP managers use this command to modify or assign the value of the managed device
- **TRAPS**: SNMP agents use this command to notify SNMP managers about an event occurring in the network
- **INFORM**: Similar to TRAPS, but it includes the SNMP manager’s acknowledgement to receive the notification
- **RESPONSE**: The SNMP manager uses this command to carry the actions back to the agents

Information collected by SNMP helps to control the network by resolving the issues in real time before affecting the productivity of the organization.

Example: Steps to enable SNMP-based routing on CISCO router/switches

- Create or modify a SNMP view record (optional)

- Create or modify an access control for the SNMP community (required)
- Specify a SNMP server engine name (ID) (optional)
- Specify SNMP server group names (optional)
- Configure SNMP server hosts (required)
- Configure SNMP server users (optional)
- Enable the SNMP agent shutdown mechanism (optional)
- Set the contact location ad serial number for the SNMP agent (optional)
- Define the maximum SNMP agent packet size (optional)
- Limit the number of TFTP servers used by SNMP (optional)
- Monitor and troubleshoot the SNMP status (optional)
- Disable the SNMP agent (optional)
- Configure SNMP notifications (required)
- Configure the router as a SNMP manager (optional)

Netflow Monitoring

The Netflow monitoring technique has the ability to collect the IP network traffic while entering or exiting the interface. This helps administrators determine the source and destination of the traffic, class of service, and reason for traffic congestion—whenever it occurs. Netflow monitoring allows a network a wide view of the traffic, enhancing the performance monitoring and security of the network. Cisco devices support Netflow-based network monitoring.

Elements of Netflow-Based Monitoring

- **Netflow Exporter**: The Netflow exporter collects all the packets and transfers the data toward the collector
- **Netflow Collector**: The Netflow collector involves pre-processing the flow of data received from the Netflow exporter
- **Analysis Console**: Administrators are responsible for the analysis console that analyzes the intrusion detection or traffic profiling

Non-Router-Based Monitoring Techniques

Non-router-based monitoring techniques use active or passive monitoring (or a combination of these) to monitor the network. The administrator uses a variety of tools to help them monitor their network performance and analyze traffic patterns. Typically, these tools involve packet sniffing, network monitoring, and bandwidth monitoring. Network and bandwidth monitoring tools use SNMP to monitor devices, bandwidth, performance, and availability for all devices and services. Packet-sniffing tools are used to analyze the traffic pattern and identify anomalies in the network traffic.

Network Monitoring

Positioning your Machine at the Appropriate Location

Administrators should place and connect their system so they can view all the inbound and outbound traffic flowing through their network. Network administrators should ensure that each packet is inspected against policy violations. The machine must be placed as described in the figure below. It should connect to the switch in front of the firewall and it should be installed with the required packet sniffing and network monitoring tools.

Connecting Your Machine to a Managed Switch

Administrators should ensure the switch is connected and configured as a managed switch. A managed switch can only view the network traffic flowing through the network. Configure the switch as a managed switch by enabling the port monitoring or port-mirroring feature on a specific port in the switch. Different vendors have different names for this feature. For example, the port-mirroring feature on a CISCO switch is known as a Switched Port Analyzer (SPAN) port. The port-mirroring process includes copying the switch network traffic and sending it to another port in the switch so the monitoring tool can analyze it. The managed switch can configure, manage, and monitor the LAN. It allows the administrator to have greater control over the flow of data traversing the network. With accessibility to manage the data flow, the chances of an intrusion are much lower. Though a managed switch may cost more than an unmanaged switch, it assures better security and filtered data transmissions in the system.

Network Traffic Signatures

A signature is a set of characters that define network activity, including IP addresses, TCP flags, and port numbers. It includes a set of rules used to detect malicious traffic entering a network. Signatures are used to:

- Alert for unusual traffic on the network.
- Identify suspicious header characteristics in a packet.
- Configure an intrusion detection system to identify attacks or probes.
- Knowledge about a specific attack that happened or a vulnerability to be exploited.

- Match patterns in a packet analysis.

Type of Signatures

Signatures are classified into two main categories depending on their behavior:

Normal Traffic Signatures: They include the normal network traffic regularly flowing to and from the network. These signatures are defined based on a normal traffic baseline for the organization. These signatures do not contain any malicious signature patterns and can be allowed to enter the network.

Attack Signatures: The traffic patterns that look suspicious are generally treated as attack signatures. These signatures should not be allowed to enter the network. If allowed, they often are the reason for a network security breach. These signatures deviate from the normal signature behavior and should be analyzed.

Baselining Normal Traffic Signatures

The network traffic baseline helps understand the behavioral patterns of the network. Baselining creates a set of metrics to monitor network performance. These metrics define the normal working condition of an enterprise's network traffic. The network traffic is compared with metrics to detect any changes in the traffic, which could be an alert to the security of the network. A network traffic baseline establishes the accepted packets, which are safe for the organization. Baselining the traffic makes it easier to detect suspicious activities on the network. Any deviation from the normal traffic baseline can be considered suspicious traffic signatures. The administrator should define a network baseline for their organization and validate the traffic against it. Baselining is more effective if it works in parallel with the organization's policy. With the help of normal traffic baselining, administrators can judge the requirements needed to secure the network.

Although there is no industry standard to measure network traffic performance baselines, there are network-monitoring tools that provide estimates on what type of traffic is normal. A network traffic baseline should be defined for all incoming and outgoing Internet traffic and WAN links. The network traffic baseline should also contain the traffic for critical business data and backup systems.

Suspicious Traffic Signature Categories

Network traffic deviating from its normal behavior is categorized as a suspicious traffic signature. It is classified into four categories: Informational: The informational traffic signature detects normal network activity. Although this may not look suspicious, the data gathered through the information signature can be used for suspicious activities. For example, the informational traffic signatures may include:

- ICMP echo requests
- TCP connection requests
- UDP connections

Attack Signature Analysis Techniques

Attack signature analysis techniques are classified into four different categories including:

Content-Based Signature: Content-based signatures are detected by analyzing the data in the payload and matching a text string to a specific set of characters. If undetected, these signatures can open backdoors in a system, providing administrative controls to an outsider. Inspecting packets for unusual/suspicious header information such as:

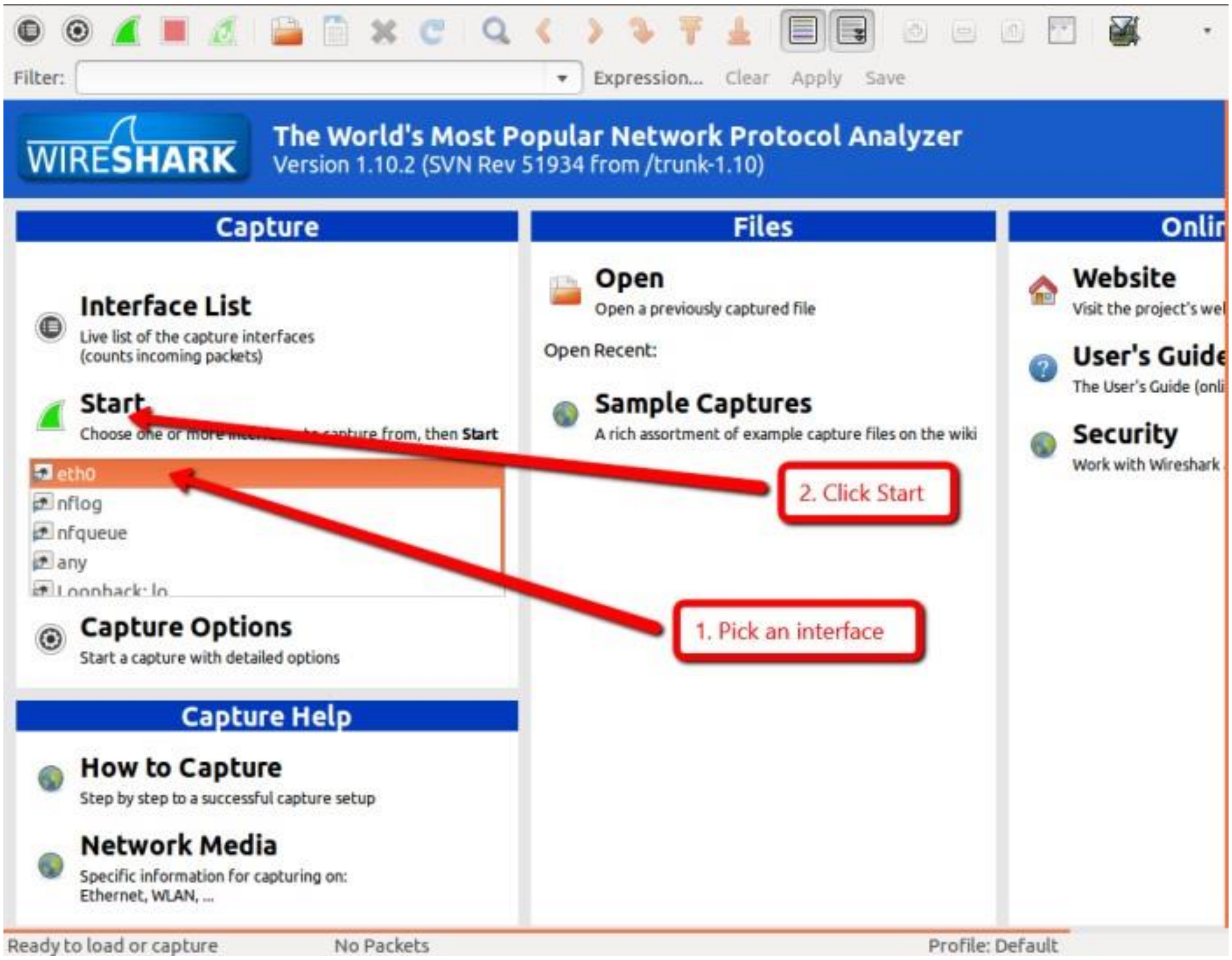
- Source and destination IP address
- IP options, protocols, and checksums
- Source and destination port number

Packet Sniffer: Wireshark

A packet analyzer or packet sniffer is a tool that can intercept and log traffic passing through the network. The sniffer is used in network management because of its monitoring and analyzing features, which help to detect intrusions, supervise network contents, troubleshoot the network, and control traffic. Network administrators use them to analyze the behavior of an application or device causing network issues. The information running through a network is a valuable source of evidence to counter intrusions or anomalous connections. The need to capture this information has led to the development of packet sniffers.

Wireshark

Wireshark is an open-source, cross-platform packet capture and analysis tool. It is available for Windows and Linux operating systems. The GUI window gives a detailed breakdown of the network protocol stack for each packet. Wireshark can also save packet data to a file for offline analysis, as well as export and import packet captures to and from other tools. Statistics can also be generated for packet-capture files. Wireshark can be used for network troubleshooting, to investigate security issues, and to analyze and understand network protocols. The packet sniffer can exploit information passed in plain-text.



The World's Most Popular Network Protocol Analyzer
Version 1.10.2 (SVN Rev 51934 from /trunk-1.10)

Interface List
Live list of the capture interfaces (counts incoming packets)

Start
Choose one or more interfaces to capture from, then **Start**

eth0
nflog
nfqueue
any
Loopback: lo

Capture Options
Start a capture with detailed options

How to Capture
Step by step to a successful capture setup

Network Media
Specific information for capturing on:
Ethernet, WLAN, ...

Open
Open a previously captured file

Open Recent:

Sample Captures
A rich assortment of example capture files on the wiki

Website
Visit the project's wel

User's Guide
The User's Guide (onli

Security
Work with Wireshark

2. Click Start

1. Pick an interface

Ready to load or capture No Packets Profile: Default

Features: Wireshark has a rich feature set that includes the following:

- Identify poor network performance due to high path latency
- Locate inter-network devices that drop packets
- Validate optimal configuration of network hosts
- Analyze application functionality and dependencies
- Optimize application behavior for best performance
- Analyze network capacity before application launch
- Verify application security during launch, login, and data transfer
- Identify unusual network traffic, which could indicate potentially compromised hosts
- Deep inspection of hundreds of protocols
- Live capture and offline analysis
- Standard three-pane packet browser
- Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI or via the TTY-mode TShark utility

Monitoring and Analyzing FTP Traffic

The FTP protocol is used to transfer files over TCP and its default port is 21. FTP doesn't offer a secure network environment nor does it offer secure user authentication. Individuals do not need authentication to access the FTP server in the network. This provides an easy method for attackers to get on the network and access resources. FTP does not provide encryption in the data transfer process. The data transfer between the sender and the receiver is in plain-text. The critical information, such as usernames and passwords, is exposed to attackers. Implementation of FTP in an organization's network leaves the data accessible to external sources. Deploying FTP in a network can lead to different types of attacks such as FTP bounce, FTP brute-force, and packet sniffing. Administrators should monitor the FTP traffic using Wireshark. It provides the administrator with complete information about the FTP traffic on the network. Applying a FTP filter helps detect unauthorized sessions running on the server. Apart from monitoring the traffic on the FTP server, administrators should also monitor the existing file content and the file size stored in the server.

Monitoring and Analyzing TELNET Traffic

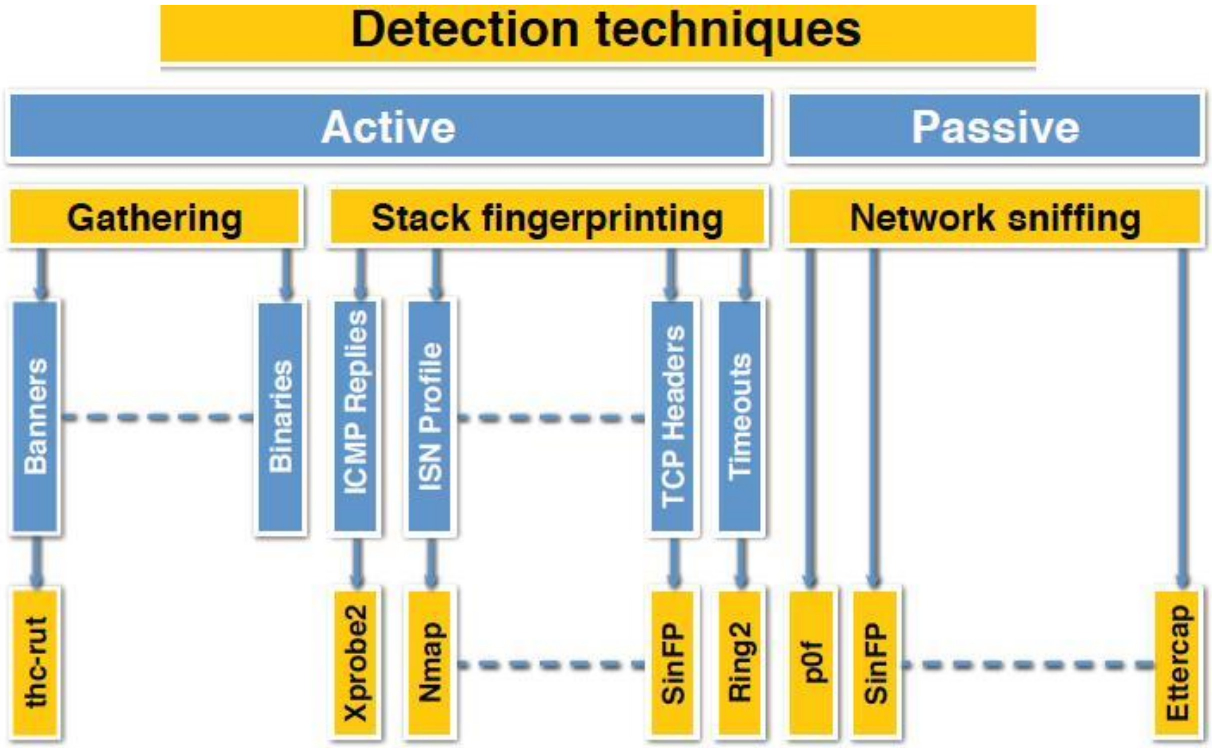
The Telnet protocol works on a client-server model. It provides access to remote network equipment and operating systems. The data transferred through Telnet is not encrypted, making it easy for intruders to eavesdrop. If a person has access to a network device with Telnet configured, they can gain access to the network and user account information. Generally, Telnet should be disabled in the organization.

Monitoring and Analyzing HTTP Traffic

Applications implementing HTTP send data in clear-text format. Implementing HTTP can pose security risks to the organization, as sensitive information (such as username and passwords) is sent over as HTTP requests. The attacker can easily sniff the traffic and steal sensitive information for malicious use. Administrators have to ensure that their HTTP traffic is sent over an encrypted protocol such as HTTPS. At the same time, they should monitor and ensure their applications do not send data over HTTP. Monitoring the HTTP traffic also helps detect the volume of HTTP traffic flowing through the network. Monitor and analyze HTTP traffic to:

- Check if there is any sensitive information using HTTP
- Detect malicious traffic
- Check the traffic against a policy violation
- Detect applications using unnecessary/restricted services

OS Fingerprinting Detection



OS fingerprinting is a process of gaining information about the target host's OS. Attackers use this method during their reconnaissance phase. Once the target OS is identified, the attacker can then find out what possible vulnerabilities exist in the OS or a specific version of the OS. An attacker can get into the network by way of the vulnerabilities existing in the OS. The attacker can attempt both active and passive OS fingerprinting to detect the target OS.

Passive OS Fingerprinting

In this technique, the attacker does not send any packets to the target; instead, they sniff the TCP/IP ports and analyze the default value for the various IP packet fields.

Active OS Fingerprinting

In this technique, the attacker sends packets to the target. If the target responds to the packets, the attacker analyzes the responses and identifies the underlying OS.

Detecting Passive OS Fingerprinting Attempts

In passive OS fingerprinting, the attacker does not send any packets in the traffic; rather, they sniff the TCP/IP ports. The detection of the target OS is done based on verifying the various IP header fields. The IP header consists of a field such as initial TTL, do not fragment flag, maximum segment size, window size, and sack OK. The default values of these fields can help administrators to detect the fingerprinting attempt. Administrators should inspect these fields to detect OS fingerprinting attempts on their network. However, the default values for these fields may vary when the packet traverses between one router and another. It is very difficult to detect a passive fingerprinting attempt. Firewalls or other security devices cannot detect passive OS fingerprinting either. It has become essential for administrators to detect these attempts manually with the help of packet-sniffing tools.

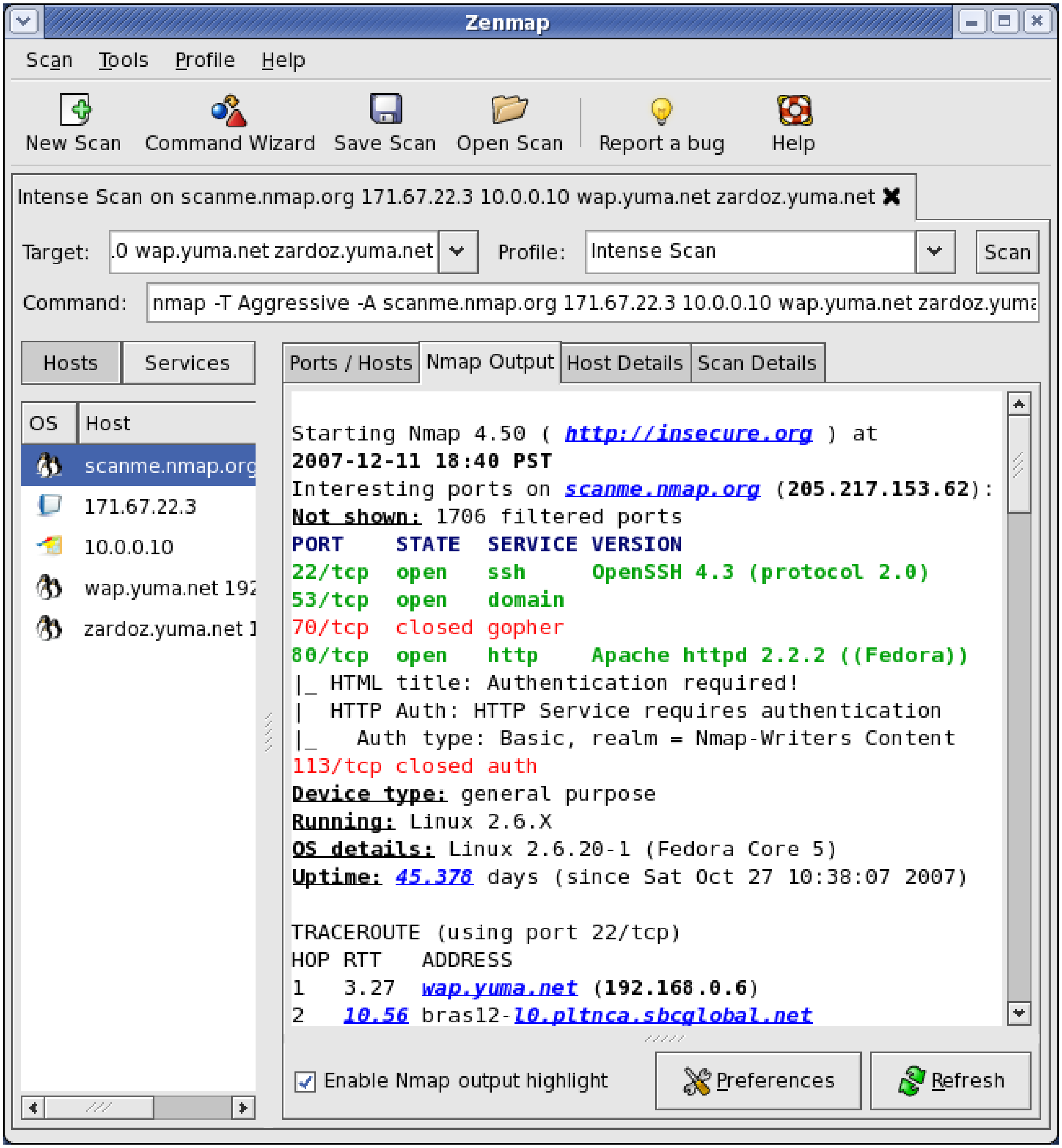
Detecting Active OS Fingerprinting Attempts

In active OS fingerprinting, an attacker sends packets to the target and waits for the reply. They will then analyze the reply received from the target to determine the OS. An attacker performs active OS fingerprinting in two ways. They can either use ICMP probes or TCP probes to detect the target OS. The attacker then analyzes the reply from the target and makes an educated guess based on the reply obtained from the target. Administrators can detect active OS fingerprinting attempts much easier than passive OS fingerprinting attempts. Administrators use specific Wireshark filters to filter out the OS fingerprinting traffic.

Examine the Nmap Process for OS Fingerprinting

In most cases, attackers generally use Nmap to perform targeted OS fingerprinting. It is necessary to understand how Nmap is used to perform OS fingerprinting. Knowing the Nmap process for OS fingerprinting will help to detect OS detection attempts made using Nmap. Examine the Nmap Process for OS Fingerprinting using Wireshark:

- ICMP Echo Request (Type 8) with no payload
- ICMP Echo Request (Type 8) with 120 or 150-byte payload of 0x00s
- ICMP Timestamp Request with Origin Timestamp value set to 0
- TCP SYN with 40-byte options area
- TCP SYN with Window Scale Shift Count set to 10
- TCP SYN with Maximum Segment Size set to 256
- TCP SYN with Timestamp Value set to 0xFFFFFFFF
- TCP Packet with options and SYN, FIN, PSH, and URG bits set
- TCP packet with options and no flags set
- TCP Acknowledgement Number field as non-zero without the ACK bit set
- TCP packets with unusual TCP window-size field values
- The Nmap Process for OS Fingerprinting



Intense Scan on scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net

Target: .0 wap.yuma.net zardoz.yuma.net

Profile: Intense Scan

Command: nmap -T Aggressive -A scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma

```
OS  Host
    scanme.nmap.org
    171.67.22.3
    10.0.0.10
    wap.yuma.net 192
    zardoz.yuma.net 1
```

```
Starting Nmap 4.50 ( http://insecure.org ) at
2007-12-11 18:40 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
Not shown: 1706 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 4.3 (protocol 2.0)
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Authentication required!
|  HTTP Auth: HTTP Service requires authentication
|_   Auth type: Basic, realm = Nmap-Writers Content
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 45.378 days (since Sat Oct 27 10:38:07 2007)

TRACEROUTE (using port 22/tcp)
HOP RTT   ADDRESS
1   3.27  wap.yuma.net (192.168.0.6)
2   10.56 bras12-10.pltnca.sbcglobal.net
```

Detecting a PING Sweep Attempt

A ping sweep scan helps attackers discover the active systems in the network. It involves sending multiple ICMP, TCP, or UDP ECHO requests to target ports and then analyzing the ECHO reply obtained from the port.

In an ICMP ping sweep, the attacker sends an ICMP type 8 ECHO request followed by an ICMP type 0 and analyzes the ECHO reply. To detect the ICMP ping sweep, find the ICMP type 8 and ICMP type 0 ECHO requests in the network traffic. It is recommended that a filter is used to accomplish this task. Use the filter icmp.type==8 or icmp.type==0 to detect an ICMP ping sweep attempt.

In a TCP/UDP ping sweep, an attacker sends an ECHO request packet to the TCP/UDP port 7. To detect the TCP/UDP ping sweep attempt, find the TCP ECHO request packets going to port 7 and the UDP ECHO request packets going to port 7 in the network traffic. Use the filter tcp.dstport==7 to detect the TCP ping sweep and udp.dstport==7 to detect the UDP ping sweep attempts. If the target port doesn't support an ECHO reply, then this technique will not work.

Detecting an ARP Sweep/ARP Scan Attempt

Similar to a ping sweep scan, an attacker also uses an ARP Sweep/ARP Scan to locate active IPs in the network. Attackers use this method when a firewall is implemented in between them and the target network. If a firewall is implemented in the network, the ping sweep method will not work. In an ARP sweep, an attacker broadcasts ARP packets to all the hosts in the selected subnet and waits for a response. If they get an ARP response from a specific host, this indicates the host is live.

ARP communications cannot be disabled to restrict an ARP sweep attempt on the network, as all TCP/IP communication is based on it. If ARP communication is disabled, it will also break the TCP communication. However, administrators can easily monitor and detect this type of attempt using an ARP filter in Wireshark. If they detect an unexpected number of broadcast ARP requests, then they also know it indicates an ARP sweep attempt on the network.

Detecting TCP Half-Open/Stealth Scan Attempts

The attacker uses a TCP Half-Open/Stealth scan to detect open or closed TCP ports on the target system. It involves sending a SYN packet to the target port exactly like normal TCP communication and waiting for the response. If they receive a SYN+ACK packet in the response, then it indicates the target port is open. If they receive a RST or RST+ACK packet in the response, then it indicates the port is closed. If the target port is behind a firewall, then they will receive an ICMP type 3 packet with a code 1, 2, 3, 9, 10, or 13 in the response. The TCP half-connection can act as an open gate for attackers to get in to the network. It is necessary for administrators to detect the TCP Half-Open connection. If there are too many RST packets or ICMP type 3 response packets in Wireshark, then it can be a sign of a TCP Half-Open/Stealth scan attempt on the network. A Stealth scan or TCP full-connect scan attempt is recognized if there are a large amount of RST or ICMP type 3 packets.

- Go to Statistics -> Conversations and click on the TCP tab to view and analyze multiple TCP sessions
- If the communication is less than 4 packets, then it is a sign of a TCP port scan on the network

Detecting a TCP Full-Connect Scan Attempt

A TCP full-connect scan or a TCP connect scan is the default scan that establishes a complete three-way handshake connection. A successful three-way handshake means that the port is open. To establish a TCP full-connect scan, the attacker sends a SYN probe packet to the target port. If the port is open, the attacker will receive a SYN/ACK packet in the response. It indicates the target port is open. The attacker will complete the communication by sending an ACK flag and will send a RST flag to terminate the session. If the port is closed, the attacker will receive the response as a RST/ACK. If the target port is behind a firewall, they will receive an ICMP type 3 packet with a code 1, 2, 3, 9, 10, or 13 in the response.

Detecting a TCP Null Scan Attempt

A TCP null scan helps attackers identify the listening ports in the network. A TCP null scan is a series of TCP scan packets containing a sequence number of 0 and no set flag. Since the null scan does not contain any set flags, it can penetrate through a router and a firewall that filters incoming packets with particular flags set.

In the TCP null scan, the attacker sends a TCP packet to the target port. If the port is closed, it will receive a RST flag. If the port is open, the port will not respond because there are no flags sent with the packet. A TCP null scan sets all the TCP headers (ACK, FIN, RST, SYN, URG, and PSH) to NULL. By applying the filter tcp.flags==0x000 in Wireshark, administrators can detect a TCP null scan on UNIX servers. A TCP null scan does not support Windows.

Detecting a TCP Xmas Scan Attempt

In the TCP Xmas scan, attackers scan the entire network and look for the machines that are up and running. It also scans for the services running on those machines.

The Xmas scan involves sending packets set with URG, PSH, ACK, and FIN flags. If the port is closed, it will receive a RST flag. If the port is open, the port will not respond, as there are no flags sent with the packet.

The TCP Xmas can scan through the firewall and ACL filters. An ACL filter blocks the ports with the help of SYN packets. However, the FIN and ACK packets bypass this security.

FIN scans do not work on many operating systems. Operating systems like Microsoft Windows send a RST flag to any malformed TCP segment. This makes it difficult for the attacker to distinguish between the open and closed ports.

Detecting a SYN/FIN DDOS Attempt

In a SYN attack, the attacker sends a succession of SYN requests to a target system in order to make the system unavailable for legitimate users. It exploits a known weakness in the TCP connection.

Typical TCP communication (TCP three-way handshake) works as follows:

1. Client sends the SYN packet to request a connection

2. Server responds back with SYN-ACK

3. Client then responds with an ACK to establish the connection

Detecting a SYN/FIN DDOS Attempt

In a SYN attack, the attacker sends a succession of SYN requests to a target system in order to make the system unavailable for legitimate users. It exploits a known weakness in the TCP connection.

Typical TCP communication (TCP three-way handshake) works as follows:

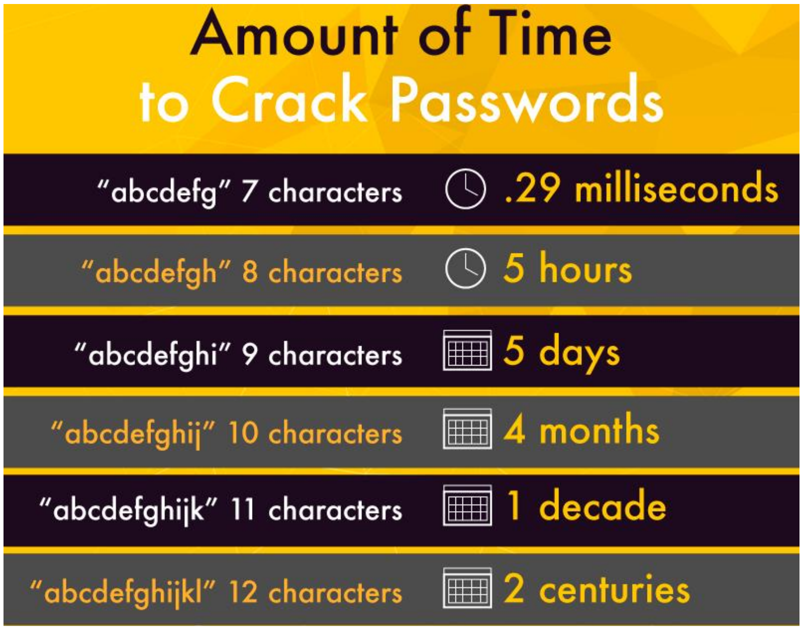
1. Client sends the SYN packet to request a connection

2. Server responds back with SYN-ACK

3. Client then responds with an ACK to establish the connection

Detecting Password-Cracking Attempts

Password cracking is a process of gaining or recovering passwords either through trial and error or running a password-guessing attempt using an available file. These contain the most commonly used passwords. These techniques are called a brute-force attack and a dictionary attack respectively. Attackers can make several password-cracking attempts on network services such as FTP, SSH, POP3, HTTP, Telnet, RDP, etc.

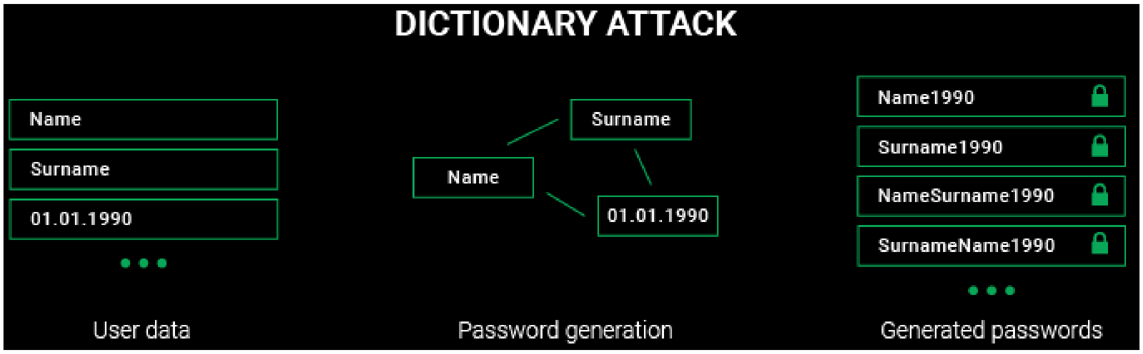


Amount of Time to Crack Passwords

"abcdefg" 7 characters	.29 milliseconds
"abcdefgh" 8 characters	5 hours
"abcdefghi" 9 characters	5 days
"abcdefghij" 10 characters	4 months
"abcdefghijk" 11 characters	1 decade
"abcdefghijkl" 12 characters	2 centuries

Brute-Force Attack

Though brute-force attacks can be a lengthy process, attackers use various tools to implement an attack on the network.



Dictionary Attack

The attacker uses a limited set of words to perform a dictionary attack. With SSH services running in the network, it is easier for attackers to perform a dictionary attack. SSH dictionary attacks rely on the log files or on the network traffic. The dictionary attack can be accomplished easily on an account that has a weak password. This type of attack is performed on a single target machine or on the network. An administrator can detect this type of attack by monitoring the number of login attempts made from the same IP address or with the same username.

Detecting FTP Password Cracking Attempts

The file transfer protocol (FTP) is a standard protocol to transmit files between systems over the Internet using the TCP/IP suite. FTP is a client-server protocol relying on two communication channels between a client and a server. One manages the conversations and the other is responsible for the actual content transmission. A client initiates a session with a download request, which the server responds to with the requested file.

Detecting Sniffing (MiTM) Attempts

Sniffing or man-in-the-middle attacks are a form of eavesdropping where an attacker captures packets by placing themselves between a client and a server. Sniffing is attempted using either an active form or a passive form.

Active Sniffing

Sniffing performed over a switched network is called active sniffing. The attacker injects packets into the network traffic to gain information from the switch, which maintains its own ARP cache known as content addressable memory (CAM).

Passive Sniffing

Sniffing performed on the hub is called passive sniffing. Since a hub broadcasts all packets, an attacker only has to initiate the session and wait for someone else to send packets on the same collision domain. The methods used in sniffing are:

- MAC flooding
- ARP poisoning

Additional Packet-Sniffing Tools

Network Sniffer

Network Sniffer can help you locate network problems by allowing you to capture and view the packet-level data on your network. It consists of a well-integrated set of functions that can resolve network problems. It can list all the network packets in real time from multi-network cards (Modem, ISDN, ADSL, etc.) and can also support capturing packets based on applications (SOCKET, TDI, etc.).

VisualSniffer

VisualSniffer is a packet-capture tool and protocol analyzer (IP sniffer or packet sniffer) for a Windows system. VisualSniffer can be used by LAN administrators and security professionals for network monitoring, intrusion detection, and network traffic logging. It can also be used by network programmers for checking what the developing program has sent and received—or by others to get a full picture of the network traffic.

SniffPass Password Sniffer

SniffPass captures the passwords that pass through the network adapter. SniffPass can capture the passwords of the following protocols: POP3, IMAP4, SMTP, FTP, and HTTP (basic authentication passwords).

Capsa Packet Sniffer

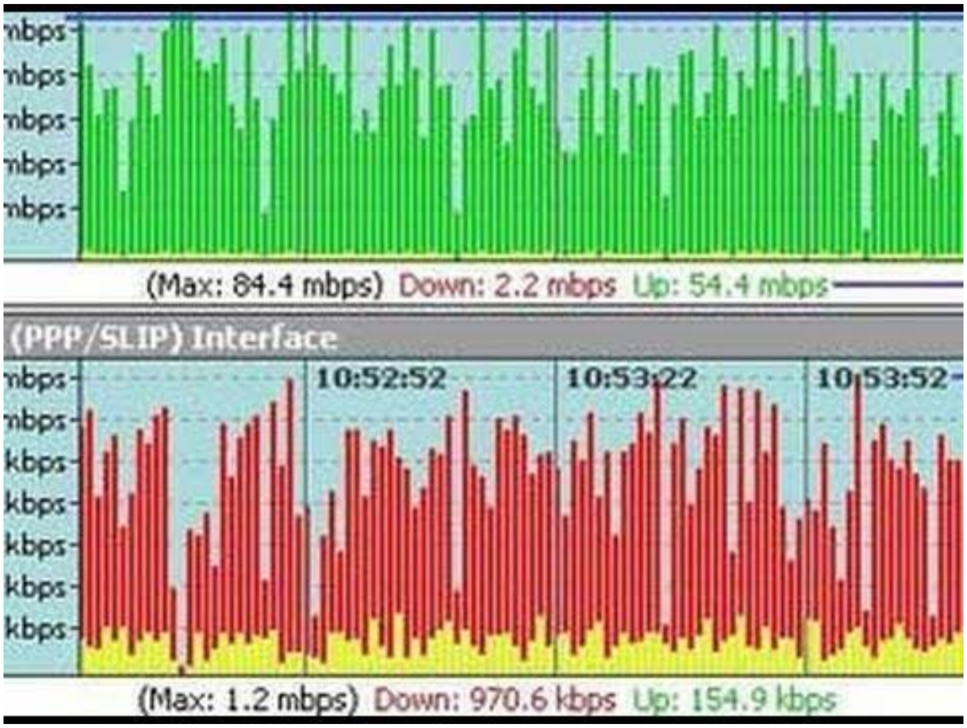
Capsa Packet Sniffer is a network analyzer for Ethernet monitoring, troubleshooting, and analysis. It monitors network activities, pinpoints network problems, and enhances network security.

Network Monitoring and Analysis using the PRTG Network Monitor

PRTG Network Monitor is a network monitoring software that supports remote management using any web browser or smart phone, various notification methods, and multiple location monitoring. Administrators can use this utility for availability, usage, and activity monitoring—covering the entire range from website monitoring to database performance monitoring.

Bandwidth Monitoring

Bandwidth is the amount data that can be transferred from one point to another. Bandwidth is one of the criteria defining network performance. An effective bandwidth is the one that provides the highest transmission rate. The bandwidth-monitoring test will identify the maximum throughput of a system. Bandwidth-monitoring tools provide output of the real-time network traffic for any device. The tools provide bandwidth information at the interface level and the device level. If the bandwidth detected is low, it degrades the functioning of the network.



An organization works on two types of bandwidth speed: upload and download. The speed at which the data is sent to the destination is called the upload speed. The speed at which the destination receives the data is called the download speed. With growing networks and huge volumes of data, organizations have started to maximize their upload and download speeds.

It is also important to consider the bandwidth capacity in the network. Bandwidth capacity involves the maximum data rate a link can transfer. With hundreds of users in the network, it is important to know the bandwidth usage required per day. Although it can be a tedious job for administrators to determine the daily-usage capacity of the bandwidth, a blueprint of the usage can help draft a proper bandwidth-monitoring plan. Bandwidth monitoring includes monitoring various bandwidth utilizations that are implemented in the organization. Many software tools allow you to monitor bandwidth in real time. Bandwidth-monitoring benefits are:

- Bandwidth monitoring helps determine the network utilization for the system. Systems using high bandwidth amounts should be monitored closely, as they can be suspicious activities or have become a victim of suspicious activity.
- High amounts of network traffic lead to network congestion and affect the function of the organization. Deploying a network limit will provide an alarm when the network is about to reach the maximum bandwidth.
- If the network congestion is high, and depending on the size of the organization, additional links can be added to the network. An additional link in the network will boost the network performance, resulting in reduced network congestion.

Focus on the following considerations to lower the bandwidth requirements:

- Server-side computing

- Data caching
- Data compression
- Latency mitigation
- Loss mitigation

Bandwidth Monitoring - Best Practices

The following best practices can also be helpful in effective bandwidth monitoring:

- Educating or training the employees (in a timely manner) about excessive bandwidth consumption can create awareness among them concerning bandwidth usage.
- Monitor the traffic consumed by the network components in the organization.
- Implement a QoS policy to prioritize bandwidth usage as per the application requirement.
- Optimize the WAN capacity to increase the bandwidth of the network.
- Back up the devices that are configured on the network. During a power failure or network failure, these backups act as a good configuration and keep the bandwidth stable.
- It is recommended to use only a single bandwidth-monitoring tool to assess the current utilization of bandwidth for the organization.
- Define and categorize the bandwidth need based on the application, user, user groups, time period, etc.
- Calculate the total number of nodes that contribute to the overall bandwidth requirement including workstations, shared printers, and servers.
- Calculate the average bandwidth required per node.
- Always consider peak bandwidth requirements for the organization.

Bandwidth-Monitoring Tools

BitMeter OS

BitMeter OS keeps track of how much of the Internet/network connection is used; it allows an administrator to view this information either via a web browser or by using the command-line tools.

FreeMeter Bandwidth Monitor

FreeMeter Bandwidth Monitor is used to monitor the network bandwidth and any or all network interfaces. It also provides supporting utilities, including Ping, Trace, UPnP utilities, etc.

BandwidthD

BandwidthD monitors the amount of traffic being received/transmitted by specific machines or subnets. It tracks the usage of TCP/IP network subnets and builds HTML files with graphs to display utilization.

PRTG Bandwidth Monitor

PRTG Bandwidth Monitor analyzes the traffic in the network and provides detailed results—tables and graphs. It monitors network devices, bandwidth, servers, applications, virtual environments, remote systems, IoT, and many more.

NetWorx

NetWorx monitors all the network connections or just a specific network connection, such as wireless or mobile broadband. The incoming and outgoing traffic is represented on a line chart and logged into a file, so the statistics can always be viewed about the daily, weekly, and monthly bandwidth usage and dial-up duration. The reports can be exported to a variety of formats, such as HTML, MS Word and Excel, for further analysis.

SolarWinds Real-Time Bandwidth Monitor

With the Real-Time Bandwidth Monitor, critical and warning thresholds can be set to instantly see when usage is out of bounds.

Rokario Bandwidth Monitor

Rokario Bandwidth Monitor enables an administrator to keep a close eye on the amount of bandwidth accumulated over the current hour, day, week, month, or year. Advanced logging tools make it easy to view the bandwidth usage and alter bandwidth logs