**<https://www.whatsupgold.com/what-is-network-monitoring>**

**Advantages**

Computer networks are connecting millions of computers and computer users throughout the world. The network has become an infrastructure for many applications that affect our daily lives. It is very important that the computer network needs to be managed properly. Management of networking requires monitoring. Network monitoring is a set of mechanisms that allows network administrators to know instantaneous state and long-term trends of a complex computer network.

Network monitoring and measurement have become more and more important in a modern complicated network. In the past, administrators might only monitor a few network devices or less than a hundred computers. The network bandwidth may be just 10 or 100 Mbps; however, now administrators have to deal with not only higher speed wired network (more than 10 Gbps and ATM (Asynchronous Transfer Mode) network) but also wireless networks. They need more sophisticated network traffic monitoring and analysis tools in order to maintain the network system stability and availability such as to fix network problems on time or to avoid network failure, to ensure the network security strength, and to make good decisions for network planning.

Network monitoring can be either active or passive. Passive network monitoring reads data from the line, without affecting the traffic. Active network monitoring adds option to modify the data on the line. Passive network monitoring exists in several forms. Simple monitoring may be easy for manual assessment as the amount of data monitored and produced is small. Monitoring of all sorts of details about the network and its traffic bears a similar hurdle; information about faults and attackers are gathered, but there is so much information that it gets lost in the sea. Also, the more data captured, the more technologically demanding it is to save and handle the data. Therefore, various ways of doing network monitoring compete with each other, as each has different tradeoffs, being targeted for different purposes, environments and users.

**Top Benefits of Network Monitoring**

**Stay ahead of outages**

What causes IT outages? Human error, configuration issues, and environmental factors can all contribute. Implementing network monitoring is one of the most basic and simple ways to prevent these outages from happening in the first place. Network monitoring gives you the visibility you need to stay one step ahead of potential issues. By showing live network performance data in an easy-to-read interface, network monitoring software helps you identify outages that could cause bottlenecks.

**Fix issues faster**

In a down situation, time is money. Network monitoring makes problem-solving easier and faster for time-strapped network professionals. Whether you're dealing with a configuration error or an abnormal traffic fluctuation, network monitoring software helps you get to the bottom of issues once and for all. Live network maps lead you to the origin of problems, and status windows give you performance metrics over time. Also, network automation tools help you go one step further. Not only can you identify problems via network monitoring, but you can fix them automatically, without having to get a person involved.

**Gain immediate ROI**

IT teams face heavy workloads and increasingly complex projects, often without the ideal time, staff, or budget needed to complete them. The right network monitoring tool can deliver immediate ROI. Without the need to manually dig into network performance, staff have time back in their day to work on more critical projects. Seeing the source of issues cuts down on tedious troubleshooting time. And getting ahead of IT outages reduces the costs of outages to your organization.

**Manage growing, changing networks**

With technology innovation and the rise in connected devices, today's IT environments are growing in size. The number of Internet-connected things is expected to reach 25 billion by 2021, according to one Gartner report. Whether that's internet-enabled sensors, wireless devices, or cloud technologies, all this equipment needs to be monitored continuously for major fluctuations and suspicious activity. Networks are also growing in complexity. Whether you're dealing with cloud migrations or IPv6 transitions, you need flexible, reliable tools to help you monitor all your IP assets and ensure smooth performance—even in the midst of change.

**Identify security threats**

When you don't have budget for intrusion detection software, but still want a tier 1 method to help protect against data breaches, network monitoring can help secure your business-critical data. A network monitoring tool can provide that first level of security. The biggest benefit you get is a picture of what "normal" performance looks like for your organization, making it easy to spot anything out of the ordinary—whether that's a spike in traffic levels or an unfamiliar device that's connected to your network. By drilling in to figure out when and on what device an event occurred, you're able to take a proactive approach to network security.

**Remote Control**

* Follow existing report

System shutdown brings the system to a condition in which it is safe to turn off the computer. All file-system buffers are flushed to the disk, then a message box is displayed informing the user that the computer can be turned off. There is also a reboot option that will restart the computer, rather than display this system shutdown message box.

Logging off stops all processes associated with the security context of the process that called the exit function, logs the current user off the system, and displays the logon dialog box. Locking the workstation protects the display from unauthorized use whenever you leave your computer. To unlock the workstation, you must log in.

Log off

The ExitWindows function logs off the current user. You can also call the ExitWindowsEx function with the EXW\_LOGOFF flag. By default, when an application uses ExitWindows or ExitWindowsEx to log off, the system sends the WM\_QUERYENDSESSION message to each window. Applications agree to terminate by returning TRUE when they receive this message. If any application returns FALSE when processing this message, the log-off operation is canceled. If your application handles the WM\_QUERYENDSESSION message, you can allow the user to cancel the log-off operation, even if another application or the system originated the end-session request. For an example, see How to Log Off the Current User. When an application returns TRUE for WM\_QUERYENDSESSION, it receives the WM\_ENDSESSION message and it is terminated, regardless of how the other applications respond to the WM\_QUERYENDSESSION message. To force all applications to terminate, use ExitWindowsEx, and specify the EXW\_FORCE flag. This prevents the system from sending WM\_QUERYENDSESSION messages. The system also sends the CTRL\_LOGOFF\_EVENT control signal to every process during a log-off operation. A console application can register a Handler Routine to process these messages. If the process that called ExitWindowsEx is running in the logon session of the interactive user, all processes in the logon session are terminated. If the process calling ExitWindowsEx is in some other logon session, only the notifications are made; no processes are terminated.

**Network Device**

* Follow exiting report

Ipconfig

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. This command is most useful on computers that are configured to obtain an IP address automatically. This enables users to determine which TCP/IP configuration values have been configured by DHCP, Automatic Private IP Addressing (APIPA), or an alternate configuration.

* If the Adapter name contains any spaces, use quotation marks around the adapter name (that is, "Adapter Name").
* For adapter names, ipconfig supports the use of the asterisk (\*) wildcard character to specify either adapters with names that begin with a specified string or adapters with names that contain a specified string.
* For example, Local\* matches all adapters that start with the string Local and \*Con\* matches all adapters that contain the string Con.

**Network Monitor**

Network monitoring continuously collects current status information from your IT network to determine the availability and utilization of devices and to measure bandwidth usage. The IT administrator is informed immediately via email, text message, or other means if delays, malfunctions, or even failures are recorded. Historically collected data gives a long-term overview of the overall health and usage of the network. Systematic network monitoring helps prevent outages, optimize

networks, and improve services: Save time and money!

A network monitor is a software tool that scans the network for connected devices. It is also used for diagnostic and investigative purposes to find and categorize what devices are running on a network. This tool takes an IP address or a range of IP addresses as input and then scans each IP Addresses sequentially and determines whether a device is present on that particular IP address or not. It scans the network and returns an IP address and it’s corresponding MAC address if the device is present.

How does it work?

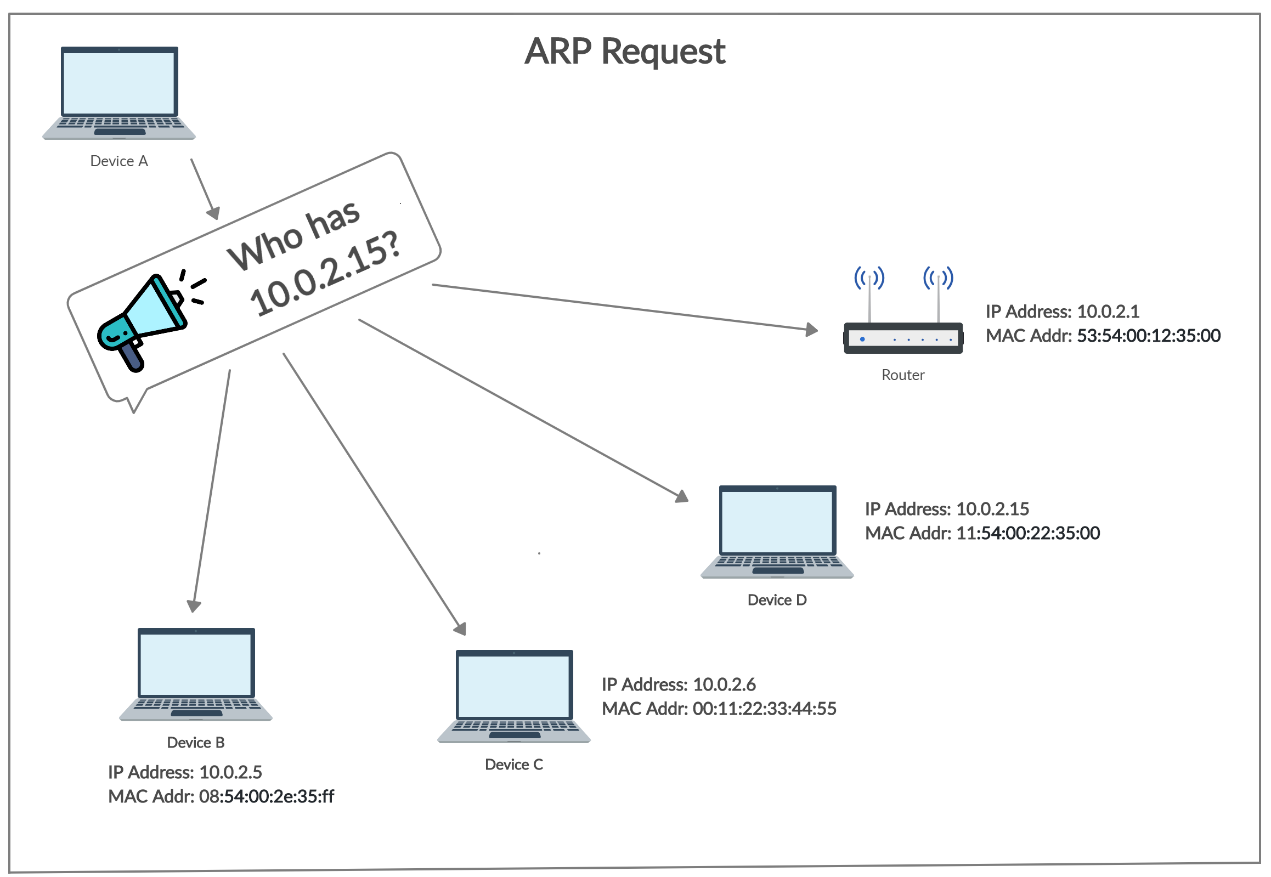
To understand how the Network Monitor scans the entire network we need to first understand what is ARP (Address Resolution Protocol).

In a network, most of the computers use the IP Address to communicate with other devices, however, in reality, the communication happens over the MAC Address. ARP is used to find out the MAC Address of a particular device whose IP address is known. For instance, a device wants to communicate with the other device on the network, then the sending device uses ARP to find the MAC Address of the device that it wants to communicate with. ARP involves two steps to find the MAC address:

1. The sending device sends an ARP Request containing the IP Address of the device it wants to communicate with. This request is broadcasted meaning every device in the network will receive this but only the device with the intended IP address will respond.
2. After receiving the broadcast message, the device with the IP address equal to the IP address in the message will send an ARP Response containing its MAC Adress to the sender.

Network Monitor uses ARP Request and Response to scan the entire network to find active devices on the network and also to find their MAC Addresses.

If it is still not clear what ARP is and how it works then refer to the images below.



**Port Scanner**

A port scanner is an application designed to probe a server or host for open ports. Such an application may be used by administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities.

A port scan or portscan is a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port; this is not a nefarious process in and of itself.[1] The majority of uses of a port scan are not attacks, but rather simple probes to determine services available on a remote machine.

To portsweep is to scan multiple hosts for a specific listening port. The latter is typically used to search for a specific service, for example, an SQL-based computer worm may portsweep looking for hosts listening on TCP port 1433.

A port scanner is a computer program that checks network ports for one of three possible statuses – open, closed, or filtered.

Port scanners are valuable tools in diagnosing network and connectivity issues. However, attackers use port scanners to detect possible access points for infiltration and to identify what kinds of devices you are running on the network, like firewalls, proxy servers or VPN servers. Here, we’ll take you through the ins and outs of a port scanner, including:

A port scanner sends a network request to connect to a specific TCP or UDP port on a computer and records the response.

So what a port scanner does is send a packet of network data to a port to check the current status. If you wanted to check to see if your web server was operating correctly, you would check the status of port 80 on that server to make sure it was open and listening.

The status helps network engineers diagnose network issues or application connectivity issues, or helps attackers find possible ports to use for infiltration into your network.

What is a Port?

A port is a virtual location where networking communication starts and ends (in a nutshell). For a more in-depth explanation, we need to establish a little background information. There are two kinds of network ports on each computer (65,536 of each for a total of 131,082 network ports):

TCP and UDP

Each computer has an Internet Protocol (IP) address, which is how the network knows which computer to send packets to. If you send a packet to the IP address, the computer knows what port to route the packet to based on the application or packet contents. Each service running on the computer needs to “listen” on a designated port.

The first 1023 TCP ports are the well-known ports reserved for applications like FTP(21), HTTP(80), or SSH(22) and the Internet Assigned Numbers Authority (IANA) reserves these points to keep them standardized.

TCP ports 1024 – 49151 are available for use by services or applications, and you can register them with IANA, so they are considered semi-reserved. Ports 49152 and higher are free to use.

Port Scanning Basics

A port scanner sends a TCP or UDP network packet and asks the port about their current status. The three types of responses are below:

1. Open, Accepted: The computer responds and asks if there is anything it can do for you.
2. Closed, Not Listening: The computer responds that “This port is currently in use and unavailable at this time.”
3. Filtered, Dropped, Blocked: The computer doesn’t even bother to respond.

Port scans generally occur early in the cyber kill chain, during reconnaissance and intrusion. Attackers use port scans to detect targets with open and unused ports that they can repurpose for infiltration, command and control, and data exfiltration or discover what applications run on that computer to exploit a vulnerability in that application.

**Ping**

Verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages are displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution.

You can use ping to test both the computer name and the IP address of the computer. If pinging the IP address is successful, but pinging the computer name is not, you might have a name resolution problem. In this case, ensure that the computer name you are specifying can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.

To test a TCP/IP configuration by using the ping command:

* To quickly obtain the TCP/IP configuration of a computer, open Command Prompt, and then type ipconfig. From the display of the ipconfig command, ensure that the network adapter for the TCP/IP configuration you are testing is not in a Media disconnected state.
* At the command prompt, ping the loopback address by typing ping 127.0.0.1
* Ping the IP address of the computer.
* Ping the IP address of the default gateway. If the ping command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.
* Ping the IP address of a remote host (a host that is on a different subnet). If the ping command fails, verify that the remote host IP address is correct, that the remote host is operational, and that all of the gateways (routers) between this computer and the remote host are operational.
* Ping the IP address of the DNS server. If the ping command fails, verify that the DNS server IP address is correct, that the DNS server is operational, and that all of the gateways (routers) between this computer and the DNS server are operational.

**Network Trace**

Tracert: Determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination with incrementally increasing Time to Live (TTL) field values. The path displayed is the list of near-side router interfaces of the routers in the path between a source host and a destination. The near-side interface is the interface of the router that is closest to the sending host in the path. Used without parameters, tracert displays help.

This diagnostic tool determines the path taken to a destination by sending ICMP Echo Request messages with varying Time to Live (TTL) values to the destination. Each router along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it.

Effectively, the TTL is a maximum link counter. When the TTL on a packet reaches 0, the router is expected to return an ICMP Time Exceeded message to the source computer. Tracert determines the path by sending the first Echo Request message with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum number of hops is reached. The maximum number of hops is 30 by default and can be specified using the -h parameter.

The path is determined by examining the ICMP Time Exceeded messages returned by intermediate routers and the Echo Reply message returned by the destination. However, some routers do not return Time Exceeded messages for packets with expired TTL values and are invisible to the tracert command. In this case, a row of asterisks (\*) is displayed for that hop.

Example:

To trace the path to the host named www.google.co.in use following command

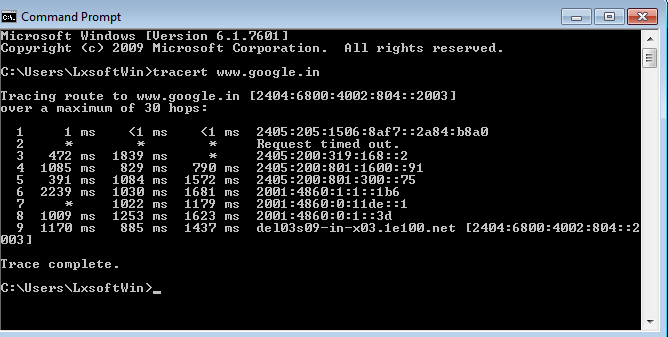
**tracert www.google.co.in**

To trace the path to the host named www.google.com and prevent the resolution of each IP address to its name, type:

**tracert -d www.google.com**

To trace the path to the host named www.google.com and use the loose source route 10.12.0.1-10.29.3.1-10.1.44.1, type:

tracert -j 10.12.0.1 10.29.3.1 10.1.44.1 www.google.com



Parameters

-d Prevents tracert from attempting to resolve the IP addresses of intermediate routers to their names. This can speed up the display of tracert results.

-h MaximumHops Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops.

-j HostList Specifies that Echo Request messages use the Loose Source Route option in the IP header with the set of intermediate destinations specified in HostList. With loose source routing, successive intermediate destinations can be separated by one or multiple routers. The maximum number of addresses or names in the host list is 9. The HostList is a series of IP addresses (in dotted decimal notation) separated by spaces.

-w Timeout Specifies the amount of time in milliseconds to wait for the ICMP Time Exceeded or Echo Reply message corresponding to a given Echo Request message to be received. If not received within the time-out, an asterisk (\*) is displayed. The default time-out is 4000 (4 seconds).

**Log**

Display log every activity done in Network Monitoring Portal. Log via activity name, file name, date and time activity has been done.