



Metron Frequently Asked Questions

1. What is Metron?

Metron is a network technology that monitors and controls individual and department level bandwidth usage, surfing, and IM/chat time. Metron is a simple to install, plug-and-play appliance that will give you in-depth network insight, providing valuable business intelligence and forecasting capabilities. Metron can be used to preserve network bandwidth by rate limiting access speeds to websites that have not been deemed as mission critical.

Metron tracks bandwidth by person and department, identifying top bandwidth users. With this technology, you can query, report, and sort on total bandwidth usage by date range, which can then be used for bandwidth accounting and Internet usage policy enforcement.

The Enterprise version of Metron includes a Locate Primary Server, which enables real-time and historic tracking of the person to their IP address, MAC address (PC), and switch port, even as they change computers or IP addresses. Metron will work with any network infrastructure.

2. What components (hardware/software) make up a Metron system?

Metron is available as a 1U, 2U, or small footprint network appliance. The Standard version of Metron comes with Collection software deployed on Active Directory servers that provides the personal identifying information used in Metron. The Enterprise version of Metron includes a Locate Primary Server appliance, which maps IP addresses, MAC addresses, and people to switch port. You can read more about Locate's features at <http://www.etelemetry.com/products/locate.aspx>

Standard 2U Version – Metron 2U Appliance + Collection Software

Standard 1U Version – Metron 1U Appliance + Collection Software

Enterprise 2U Version – Metron 2U Appliance + Locate Primary Server Appliance

Enterprise 1U Version – Metron 1U Appliance + Locate Primary Server Appliance

SE Small Appliance Version – Metron Small Appliance + Collection Software

3. Where do I install Metron on my network? Does Metron work on all network environments?

When Metron is deployed inline for rate limiting, Metron must be installed between the core router and the Internet gateway. When deployed in a passive mode, non-rate limiting, Metron's sniffer interface must be connected to a port mirroring all incoming and outgoing Internet traffic. Therefore, it requires a switch with mirroring capability, such as SPAN.

Metron's web-based management interface requires a standard, non-mirrored connection to the network.

4. How difficult is it to install Metron?

Metron is easy to install. Since it is appliance-based, Metron can be up and running within an hour. The unit has four physical ports:

- Gig-E management port
- Gig-E sniffer port for detecting network traffic (that must be connected to a mirrored switch port at the Internet gateway)
- Gig-E outside interface that connects to the Internet gateway
- Gig-E inside interface that connects to the core router

Setting up a Metron appliance entails entering some basic configuration information, such as IP address, Subnet mask, Gateway, and Nameserver. Metron also requires information from two sources: information about your people typically found in an Active Directory or LDAP server or a staff directory uploaded via a CSV file.



For Standard versions of Metron, the eTelemetry Collection software must be installed and configured on Active Directory servers. This process is simplified with the eTelemetry Collection Software Setup Wizard. This step is not necessary for networks without a network operating system or central authentication.

For Enterprise versions of Metron, the eTelemetry Locate appliance must be linked to Metron. In order to do this, you must upload a basic CSV file with Metron's serial and IP address information into Locate.

Once configured, Metron starts collecting data immediately. All information and reports are accessed from an easy-to-use, central web interface.

5. How does Metron gather data? Will this impact my network performance?

Metron passively gathers data by sniffing packets from an Internet gateway mirror. The impact of running a gateway mirror on a switch is minimal. Metron can be configured to poll user information from an LDAP on your network. This is done periodically (every 4 hours) and has minimal network impact.

Metron also works on a decentralized network using patented algorithms to identify users and dynamically match IPs to users from the staff directory uploaded in the initial configuration.

Metron Enterprise Version: Locate reports information to Metron in real time. The amount of traffic generated is a very small percentage of the total traffic monitored by Locate.

Metron Standard Version: eTelemetry Collection Software reports in real time to Metron each time a user authenticates. The amount of traffic generated is a very small percentage of the total traffic generated by a typical user to the Active Directory server.

6. Who has access to Metron's data? Can users be given different access privileges? Can views of data be segmented by a user's need to know?

The Metron appliance comes pre-configured with default passwords for four levels of access. User access is then configured by the Administrator who can change the passwords. The following levels of access are provided in Metron:

User Type	Access Privileges
Administrator	Full Access
Power User	Manage alerts, customize user parameters, search/timeslice
Restricted User	View alerts, customize user parameters, search/timeslice
Guest	View alerts, search/timeslice

7. What bandwidth does Metron measure?

Metron measures a user's total Internet bandwidth usage. Internal bandwidth is not measured.

8. What protocols does Metron track and measure?

Metron monitors all Internet bandwidth and provides detailed reporting on the following protocol/applications over their standard TCP ports:

- HTTP/HTTPS
- Instant Messaging (including AOL IM, Yahoo! IM, MSN Web Messenger, and Google Talk)
- Remote Desktop (Microsoft Remote Desktop)



9. We have several offices with Internet gateways. How would Metron work in this environment?

A Metron appliance needs to be installed at each Internet gateway.

10. How does Metron quantify Surf Time and Chat Time? For example, what constitutes one hour of surf time or one hour of chat time?

The length of these activities is determined by a combination of detected network activity and session timeout. For instance, when Metron first detects chat activity, it logs a chat session for the user initiating the chat. While the user continues to chat, the session is extended. The session is only ended when the user stops chatting for a length of time equal to the session timeout (for chatting, this is one minute).

Surfing thresholds are determined by the parameters set in the alert. For instance, the administrator can set an alert to notify him or her when a user surfs for a total of one hour in an eight-hour day. If a user surfs for 45 minutes and then later surfs for 15 minutes, an alert will be triggered. To be notified when a user surfs contiguously for one hour, the administrator should then set an alert for one hour of surfing in one hour of time. This alert will trigger only if the user surfs continuously for an hour. If he/she stops at 59 minutes, no alert will be triggered. However, all time spent surfing and chatting is captured and this individual's activity may appear in a "Top Surfer" report for the day, week, or month.

11. Can Metron block or filter websites that people visit?

Yes. When Metron is deployed inline, access speeds to websites can be rate limited to help preserve available bandwidth for mission critical applications such as email. If desired, access to websites can be completely blocked.

12. What is Social/Organizational Network Analysis (ONA) and how does it work?

Social/Organizational Network Analysis (ONA) is the visual representation of nodes which are generally individuals or groups. The closer the proximity of nodes indicates a greater volume and frequency of contact between them. Progressive organizations have used ONA to identify departmental silos, key connectors, and leaders among entry level staff. This insight enables organizations to streamline operations and mitigate risk. For example, if a single key person connects two groups, you can take steps to create additional connections that eliminate bottlenecks and reduce the risk of operational disruption if he/she leaves the firm.

Metron dynamically captures employee email, surfing, and chatting activity to create real-time ONA analysis. Metron eliminates manual steps in ONA data gathering and enables "on the fly" follow-up assessments of the impact of BPRs on communication (i.e., are departments collaborating better now?). Like a scan of the organization's "body," these tools enable early detection of issues and on-going tuning of organizational processes that depend on cooperation. Metron reveals the "real" organizational chart and is exportable to be analyzed by third party ONA software, including Orgnet's InFlow.

13. Can you perform a full packet capture on an individual? How does it work?

Metron allows you to record all Internet traffic of a designated person into an industry format standard network capture file (pcap). Because of eTelemetry's patented people-to-IP technology, this packet capture will follow the individual even if he or she changes PCs or switch ports. This capture file can be downloaded for off line analysis with any 3rd party tool capable of reading pcap format.

14. I am a non-technical manager/executive, how can I use Metron to better manage my people?

For the majority of organizations, employees are both the most important resource and the largest expenditure. Metron provides reports and charts that are readily understood by non-technical managers and can be immediately exported to incorporate into management reports.

For example, total surfing time by department can be used by the CEO gain a new view into productivity. Top 10 employee surfers/chatters can be used by operational managers to enforce policies. If your employee is using Remote Desktop to tunnel to their home PC, Metron will let you know so you check on why home PC access is needed during the business day.



15. What reports are available in Metron?

Metron provides a variety of reports through an easy-to-use web application, including:

- Monthly Bandwidth Usage by Department – To assist in departmental bandwidth usage chargebacks
- Internet Usage Summary View – 10-day summary report of bandwidth and user behavior
- 14 Day User Summary – Daily totals of bandwidth and behavior for a given user
- Top Bandwidth Users – Users with highest bandwidth usage
- Total Gateway Bandwidth – Internet gateway bandwidth over time
- Highest Bandwidth Sites – Sites with the most total bandwidth
- Top Surfers – Users with the most time spent surfing during the specified date/time range
- Top Internet Chatters – Users with the most time spent chatting during the specified date/time range
- Most Surfed Sites – A list of Internet sites surfed from the most frequently visited to the least frequently visited
- Hourly Activity Report – Two-day hourly activities (chat, surf, SSH, RDC) by person or department
- User Surf History Report – History of sites surfed by a given user

16. How do I know where my people have been surfing?

The “Most Surfed Sites” report details the sites users have visited most frequently. The “User Surf History” report will show you all the sites surfed by a specified user.

17. Can I monitor their chat conversations?

No.

18. What alerting capabilities come with Metron?

Metron can be configured to alert on the following conditions:

- Total incoming bandwidth exceeds a specified limit
- Time spent surfing the web exceeds a specified time limit
- Time spent chatting exceeds a specified time limit
- Time spent using remote desktop exceeds a specified time limit
- Time spent using SSH exceeds a specified time limit

The alerts can be set for a specific user you wish to monitor or they can be generic and alert on any user that exceeds the threshold set.

19. Will installing the A/D server collection software have an impact on my A/D server's performance?

The eTelemetry Active Directory Collection Software is a small, low-impact, .NET Windows Service that is installed on Windows Server domain controllers. When a user or machine authenticates to Active Directory, the eTelemetry Active Directory Collection Software forwards the authentication information (user account, machine account, IP address) to Locate. As a passive service, it only runs and consumes CPU cycles when a security event occurs. The eTelemetry Active Directory Collection Software is a free alternative to deploying a Locate Collection Node.