ENTUITY
NETWORK ANALYTICS

TECHNICAL DATA SHEET

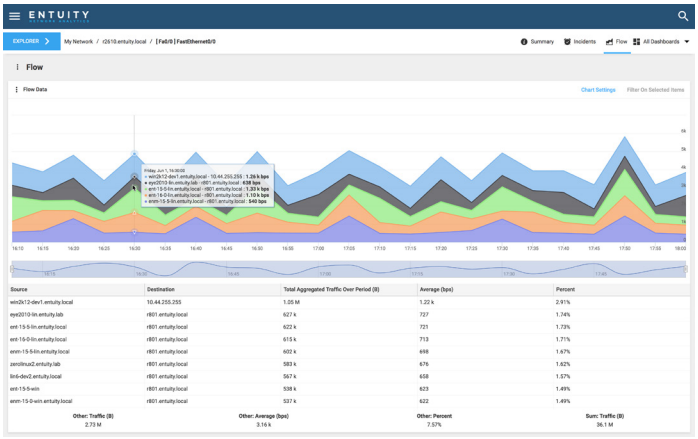
FLOW

ENA's Integrated Flow Analyzer Premium (IFAP) gives you detailed flow information about your network traffic, so you can deliver continuous availability for critical applications.

Understand your network traffic

ENA's flow capabilities help complete your network visibility, showing who's talking to whom, for how long, at what intervals, using which protocols and ports, and how much data is exchanged. With a top-down flow perspective that can easily scale to any network size, our flow monitoring helps you reduce MTTR and MTRS across your customers' networks and your own.

Plan for future growth with insight into the interfaces that see the most and least traffic. Through our flexible and customizable dashboard-centric UI, ENA presents both element- and flow-based perspectives in context to one another.



Provide bandwidth for critical business applications

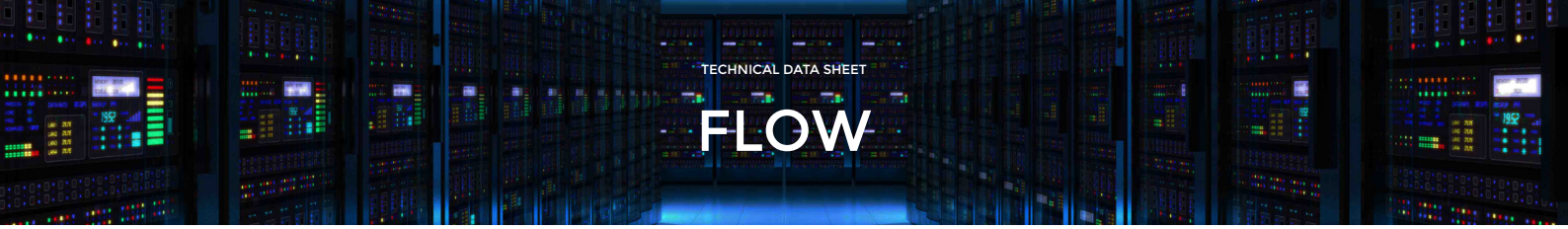
Observe traffic patterns with increments as precise as 1 minute, so you can see exactly which traffic classes and protocols are suffering from bandwidth starvation. Keep an eye on which users are causing bottlenecks, or the most resource-hungry traffic types. Find causes of network congestion and act appropriately to keep crucial business services up. Determine bandwidth patterns for confident and accurate capacity planning.

Monitor traffic between subnets and cloud applications

As cloud computing grows, you have greater need to understand the cumulative effects of a mass of workstations in specific locations (e.g. offices, departments, subnets) that communicate with applications on public and private cloud. IFAP gives you immediate access to traffic patterns and historic trends for specific subsets of traffic, so you can see where the network is meeting availability and performance requirements.

Integrated Flow Analyzer Premium

- All flow analysis in one place. Flow collection consolidated into a simple process. Collect flow from local collector, and manage collection from remote servers.
- Real-time visibility into top conversations, showing hosts with suspciously high numbers of active conversations.
- Support distributed pollers for unlimited NetFlow scalability.
- Extensive reports on historical data that display up to a month of data per report.
- Custom analysis of data with combinations of eleven breakdowns: conversations, interfaces, applications, ports, hosts, listeners, talkers, protocols, QoS classes, DSCP classes, IP precedence classes.
- Flexible grouping controls - group multiple hosts, web servers and users into a single chart, with an aggregation of data. Group traffic by application type and/or IP address.
- Collection of data with granularity down to one minute.
- Adjustable data retention settings, store years of rolled-up data dependent only on memory size.



TECHNICAL DATA SHEET

FLOW

Gauge network impacts on business services

Networks are increasingly distributed, with a huge number of endpoints. Use flow monitoring to understand which business services are supported by which links in the network. Keeping tabs on where your traffic is allows you to prioritize allocation of resources for precise troubleshooting and proactive management.

Expansive networks are also more difficult to defend - use IFAP to detect potential DDOS attacks through abnormal network traffic behavior. Networks are holistic, and so ENA helps you to gauge how the network affects traffic flow and vice versa.

Comprehensive flow protocol support

ENA supports a range of network flow protocols, giving you insight into all traffic across your network:

- NetFlow v5, v6, v7, v9 (support for the most commonly used templates)
- Sampled NetFlow v5, sampled NetFlow v9
- NetFlow monitoring on Cisco ASAs
- IPFIX, comparable support to that delivered for NetFlow v9
- Netstream v5, v9
- sFlow v4, v5
- JFlow
- VMware distributed virtual switch flows, including support for NSX VXLAN tenant information where applicable
- OOTB support for Cisco, 3COM, Juniper, Huawei, Hewlett Packard, Brocade and more

Manage application port mappings

Identifying application data within flow data is integral to efficiently managing your network bandwidth. When a connection is made from a client to a server, the TCP or UDP port on the server end of the connection determines the application in use, and ENA identifies the application data by mapping the TCP and UDP port number to an application. In doing so, ENA can remove ephemeral port records from the database for greater efficiency.

Dedicated dashlets to monitor flow

- Flow Data
- Flow Summary
- Flow-Enabled Devices
- Flow TopN Summary

Spot long-term traffic trends

Understanding flow patterns is essential to spotting traffic trends and where capacity may quickly become depleted. Find previously unknown underutilized areas of the network, enabling you to alter existing connections and eliminate unnecessary hardware costs. Store as much rolled up data as your hard drive can hold, and easily group it in ways that allow you to analyze and report on it from a variety of perspectives.

Save on management costs by identifying the causes of high utilization, rather than simply upgrading the congested link. Use flow to provide accurate QoS settings

Flexible configuration

You have complete control over the collection of flow data. It's easy to enable or disable flow collection through the Flow Inventory page, from specific flow dashlets, or the Context Menu of the selected device. Manage and gain insight into all network flow collection from the Flow Inventory page. ENA sets no limit to the number of flow collectors you can assign to Entuity servers, and deploy additional servers to seamlessly handle large volumes of collection or when traffic must be localized geographically - all this with a light administrative burden.

Complement Cisco NBAR technology

Alongside providing for flow-related technologies, ENA supports Cisco NBAR to help ensure the quality of application performance. Flow and NBAR are complementary technologies - whilst Flow records all conversations passing through an interface and can tell you the source and destination of every conversation, NBAR enables you to categorize the traffic across an interface.

Use flow to see how much traffic is flowing from one router to another, and then use NBAR to intelligently breakdown the traffic types into applications. Use Flow and NBAR to find traffic spikes and precisely determine their cause.

ENTUITY
NETWORK ANALYTICS