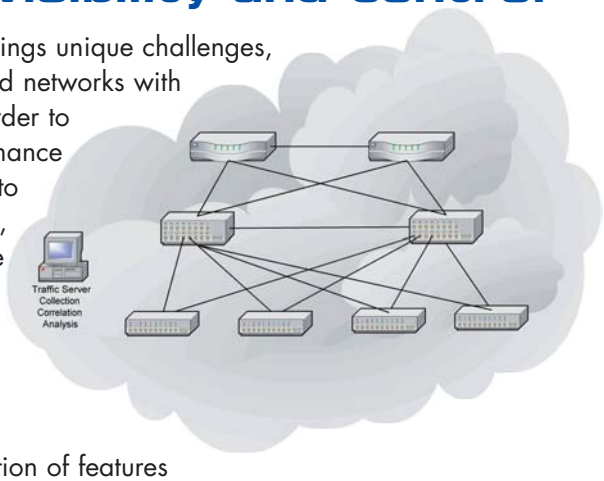
InMon internet monitoring

Traffic Server

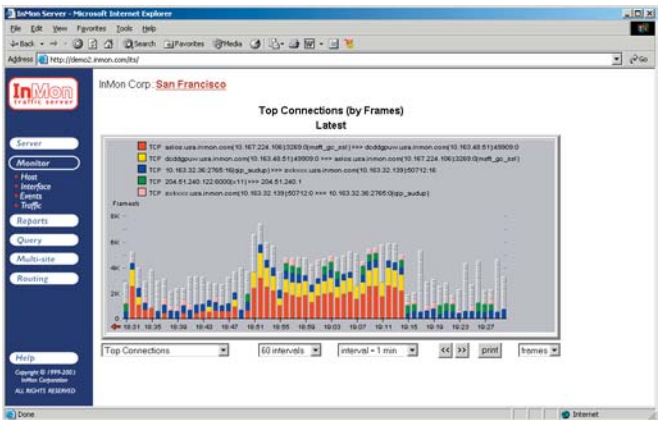
Complete network visibility and control

- Continuous monitoring and analysis of network traffic across tens of thousand of switch ports ranging from 10/100 to 10 Gigabit speeds
- Identify real-time congestion issues and troubleshoot network problems
- Protect against Denial of Service attacks and unauthorized usage
- Manage quality of service for active services
- Plan for cost effective upgrades
- Account and bill for usage
- Optimize BGP peering and routing policies

Managing today's large, high-speed networks brings unique challenges, combining the problems of managing L2 switched networks with the complexity of routing and BGP peering. In order to provide cost-effective, uninterrupted, high-performance network services, it must be possible to respond to real-time congestion and quality of service issues, defend against security threats, generate revenue from value-added service usage, and plan for future resource deployment. Visibility into current and historical traffic patterns across the entire network makes this possible.



InMon Traffic Server provides a unique combination of features that meet these challenges. At its core, Traffic Server has a highly scalable traffic correlation engine capable of continuously monitoring tens of thousands of switch/router ports. Sophisticated statistical algorithms combine traffic data and routing/switching data to build accurate and detailed, real-time and historical traffic flow information across the whole network. This detailed traffic information is easily accessed. Real-time, overall network performance status can be seen at a glance, with an intuitive drill-down interface to instantly guide you to the cause of problems. Detailed historical traffic flow information is accessed by standard and customizable automatic reports.



Traffic Server accepts data from a variety of different data sources. sFlow™ (RFC 3176) provides the richest information.

By continuously monitoring traffic flows on all ports in the network, Traffic Server generates alarms on congestion and rapidly identifies the sources of traffic and associated application level conversations. This allows the situation to be controlled at source, for example, with rate control or prioritization of traffic. Problems with enterprise applications are often first observable in abnormal traffic patterns. By continuously monitoring traffic flows network-wide, Traffic Server makes these abnormal traffic patterns visible with sufficient detail to enable rapid diagnosis and correction.

A network manager must continuously defend against external and internal security threats. A continuous onslaught of denial of service attacks, port scans, system infiltration, and unauthorized usage requires constant vigilance. Traffic Server's complete network surveillance and ability to link traffic with routing information allows it to quickly trace these security threats. Its always-on monitoring provides a baseline of normal behavior from which anomalies and suspicious activity are detected.

Traffic Server's unique "traffic-directed trace" capability provides continuous, automatically scheduled quality of service and route stability testing. By scheduling active tests based on real-time traffic measurements Traffic Server is able to correlate quality of service problems with routes, drilling-down to the individual router hop where delay and/or packet loss is occurring. The impact of the problem is determined by identifying the applications and customers that depend on the route.

InMon internet monitoring

Traffic Server

Traffic Server correlates traffic data into a single, network-wide history providing detailed layer 2 – 7 traffic flow information. This detailed historical traffic flow information and customizable automatic reporting highlight the cause of emerging congestion problems, traffic growth trends and violation of service level agreements.

Detailed network usage information is needed to charge fairly for network services and recover costs for providing value-added services. The detailed layer 2 – 7 traffic accounting information maintained by Traffic Server can be used to provide each department or customer (identified by MAC, VLAN, subnet etc.) with traffic totals and breakdowns by top users and applications.

Managing peering relationships and optimizing the routes is a particular challenge. Traffic Server's ability to correlate traffic with detailed routing information provides valuable information for optimizing routes: highlighting routes that carry important traffic, candidates for peering, and customers affected by routing problems.

Other Key Benefits

- Access to traffic data from any web browser or web-aware application
- Detailed contact information for hosts and AS
- Customizable interactive and scheduled reporting
- Delta reporting for anomaly detection
- Custom link profiling with RRD
- Easy integration with other applications through open interface and web-based queries

Technical Specifications

Protocols Monitored

Full layer 2 – layer 7 analysis:

- Ethernet/802.3/SNAP
- IPv4/IPv6/ICMP/UDP/TCP
- IPX
- AppleTalk
- DecNet4
- BGP4 source, destination, peer, full path analysis

Layer 2 analysis:

- Full duplex port statistics
- Traffic priority by port
- VLAN statistics

Standard reports:

- Network-wide thresholds and alarms
- Congestion (identifying the busiest links and the causes)
- Service Level Agreement violations
- Event frequency
- Compromised or infected host and illicit server
- Unauthorized access
- Traffic profiling and trending (host, protocol, link)
- IP Multicast sources, channels, and trends
- BGP AS Path analysis
- Inter-site availability and response time measurements

Data Sources

- Monitors 20,000+ switch ports from a single server
- Accepts sFlow (RFC 3176), Cisco NetFlow, Hewlett-Packard Extended-RMON as data sources
- Monitors at wire speed for 10/100/1000/10,000

System Requirements

Traffic Server is a web-based appliance that runs on dedicated hardware under RedHat Linux.

Typical Small Configuration (branch office)

CPU: 1 x Pentium III 700 MHz
Memory: 512MB
Disk: 10GB IDE
Network: 10Mbps

Typical Medium Configuration (small campus or data center)

CPU: 2 x Pentium III 700 MHz
Memory: 1 GB
Disk: 40GB SCSI
Network: 100Mbps

Typical Large Configuration (Large campus, data center, or internet backbone)

CPU: 4 x Pentium III 1 GHz
Memory: 2 GB
Disk: 100GB SCSI
Network: 100Mbps

sFlow ENABLED

www.inmon.com

Tel: (415) 661-6343 • Fax: (415) 661-5541 • 1404 Irving Street, San Francisco, CA 94122