7 Key Requirements for Distributed Network Monitoring

WHITE PAPER

Distributed network monitoring uses dispersed data-collection points and analysis services to give IT administrators and business managers real-time and historical insight into networks. What are the key requirements for such a solution. Read this paper for answers.

WildPackets, Inc.
1340 Treat Blvd, Suite 500
Walnut Creek, CA 94597
925.937.3200
www.wildpackets.com

7 Key Requirements for Distributed Network Monitoring

Insight into Business-Critical Networks

Organizations run on their networks. In nearly every industry, productivity depends on Internet access, email, file sharing, Web applications, and VoIP, not to mention business services and custom applications. In mid-size and large enterprises, networks deliver even more complex IT services, such as business intelligence, e-commerce, and scientific research.

Because networks are so critical, IT organizations need clear insight into how well they are performing. At any given moment, administrators need to know which applications and services are working, which are not, and why.

When networks become large and complex, spanning locations and data centers, this real-time understanding can be achieved only with a distributed network monitoring solution.

Distributed network monitoring uses disparate data-collection points and analysis services to give IT administrators and business managers real-time and historical insight into their networks. Collecting data systematically from across the network, a distributed network monitoring solution offers both a global view of network health as well as detailed, localized views of specific network segments and applications.

Using distributed network monitoring, IT organizations can:

- **Conduct Capacity Planning**
  Organizations need to understand network utilization so they can accurately provision new network segments and services.
- **Monitor Networks to Support Operations Management**
  To ensure that critical applications are running and meeting the needs of employees, operations teams need both real-time and historical insight into network behavior across all enterprise locations.
- **Troubleshoot Problems and Optimize Services**
  When problems arise, network engineers and help-desk staff need powerful tools for discovering the root cause and making corrections quickly and accurately.

Capacity planning is important not only for the replication of currently deployed services, but also for the deployment of new technologies such as 802.11ac Wi-Fi and 10G and 40G networks.

Operations management requires the monitoring networks at main offices, branch offices, and any other locations and services that employees use in their daily work. Operations management ensures that IT services never compromise employee productivity.

Troubleshooting becomes a critical IT capability when things go wrong. For all kinds of organizations, network outages are expensive: productivity declines, revenue is lost, and reputations suffer.

Just how expensive are IT outages? A 2011 survey by CA found that a typical IT outage cost midsize companies more than $91,000 and large enterprises more than $1,000,000. The same survey estimated that a typical data center outage costs $5,600 per minute. Half the companies surveyed reported that outages had a “damaging” effect on their reputations, and 18% went further and described the effect as “very damaging.”[1]

To minimize the effects of service degradations and network outages, IT organizations need clear, detailed, and

precise information about networks and network activity. They get this information from distributed network monitoring solutions.

Or rather, they try to.

Challenges in Network Monitoring

Despite recent advances in network monitoring technology, many enterprises find it difficult to monitor and troubleshoot their networks. Why?

One of the principal challenges of distributed network monitoring is addressing the breadth of today's enterprise networks. These networks are bigger than ever before, spanning multiple data centers, branch offices, and third-party services. They provide connectivity to not just traditional desktop systems but also to an ever-growing array of mobile devices running a variety of operating systems.

Another part of the challenge lies in the variety of network traffic itself. Traffic is more varied than ever before. Protocols range from CIFS for file access to XML for Web services to VoIP for telephony. File sizes continue to grow. A decade ago, email systems could barely handle 10 MB files. Today, file-sharing solutions routinely transfer files that are 10 GB or larger.

Another challenge is the high speed of networks. 1G networks are common now, and many organizations are investing in new 10G and 40G ports. Network monitoring solutions need to be able to analyze high volumes of high speed traffic. Many network analysis products, whose designs have not changed significantly in many years, have trouble keeping up.

Distributed network monitoring is obviously important. Unfortunately, it is not always easy.

Requirements for Distributed Network Monitoring for Businesses

To support an organization's work in capacity planning, operations management, and troubleshooting, a distributed network monitoring solution should meet the following requirements:

1. **Scalability**
   The solution must be capable of covering all network segments, including those in branch offices, remote data centers, and other locations. Without universal coverage, IT will never be able to troubleshoot and optimize every segment and service, and productivity and data security will be jeopardized.

2. **Expert Analysis**
   Expert Analysis gives IT administrators explanations that provide the context for network activities. It reduces guesswork and speeds diagnosis of problems, which in turn can lead to reduced Mean Time To Repair (MTTR).

3. **VoIP and Video-over-IP Analysis**
   VoIP has become the standard for business telephony, and video over IP is becoming more common, whether it's used for delivering training videos to distributed teams or catching up on ESPN at lunch.[2] Latency issues

that would go unnoticed in other applications become distracting or outright disruptive to VoIP and video users. IT organizations need to be able to monitor VoIP and video traffic using metrics appropriate to each application to ensure that important daily communications are not jeopardized.

4. **Support for Wireless Protocols, including 802.11ac**
   In most organizations, Wi-Fi has become the de facto standard for LAN connectivity. 802.11n is common, but many computer vendors and network vendors are already introducing 802.11ac products, which promise greater throughput and stronger signal strength. Enterprises should ensure that their distributed network monitoring solution can keep up with the evolution of Wi-Fi technology, including new standards such as 802.11ac.

5. **Support for NetFlow and sFlow**
   To increase coverage of distributed networks, monitoring solutions should take advantage of the IP metrics collected by network infrastructure itself. NetFlow metrics are collected and reported by Cisco devices, and sFlow metrics are collected and reported by devices from a long list of vendors, including Alcatel-Lucent, Brocade, Cisco, HP, IBM, Juniper, and NEC. NetFlow and sFlow metrics can complement other more sophisticated flow and packet analysis to provide a broader picture of an organization's network.

6. **Support for Analyzing High-speed Networks – 1G, 10G, 40G, and 100G**
   As enterprises deploy faster networks, they need a network monitoring solution that can support analysis at these higher speeds. Shipments of 10G, 40G, and 100G network ports rose 62% in 2012. Shipments of 10G equipment are expected to double in the coming years, reaching $42 billion in 2017. 10G ports now account for nearly 75% of high-speed networks, so network monitoring solutions should support analysis at 10G speeds.[3]

7. **Long-term Reporting and Trend Analysis**
   For capacity planning, operations management, and the troubleshooting of intermittent problems, IT organizations need access to long-term reporting and trend analysis of their networks. Many IT organizations must commit to year-long Service Level Agreements but lack any year-long reporting that clearly shows which applications and services are operating at the agreed upon service levels. Business managers might want to compare how well certain systems, such as e-commerce systems, perform under the stress of periodic events such as product launches. And some long-term security attacks, such as Advanced Persistent Threats, can be detected through long-term analysis of subtle anomalies. For all these reasons, a distributed network monitoring solution should support long-term reporting and trend analysis.

The WildPackets Solution for Distributed Network Monitoring

WildPackets, a leading provider of network and application performance solutions, offers a comprehensive and scalable solution for distributed network monitoring that meets all these requirements.

Since 1990, WildPackets has delivered network analysis solutions featuring deep packet inspection and rich Expert Analysis in order to help IT professionals monitor, troubleshoot, and optimize network technologies quickly and easily. Building on this legacy of rich data analysis, WildPackets' solution for distributed network monitoring applies packet-level analytics and contextual analysis to the challenge of monitoring and managing large, complex enterprise networks.

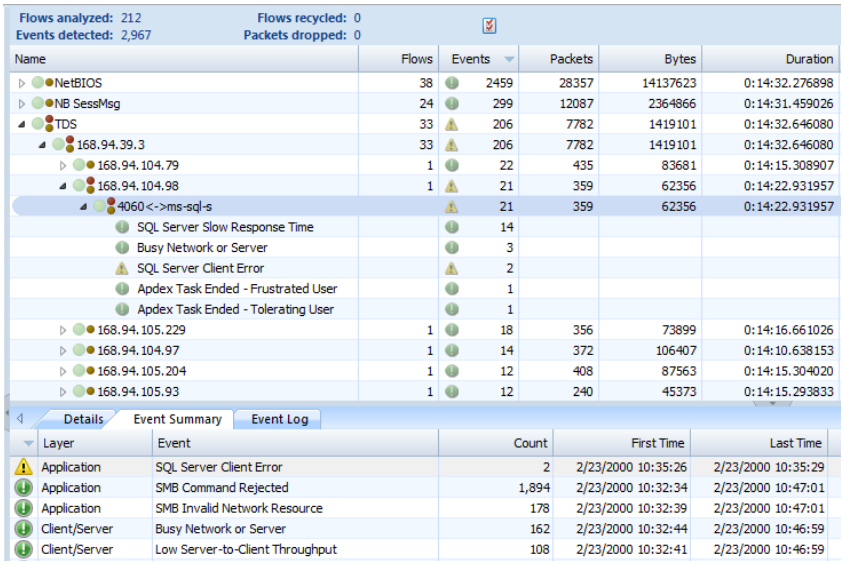
7 Key Requirements for Distributed Network Monitoring

The WildPackets solution for distributed network monitoring includes these products:

- **WatchPoint,** a highly scalable network monitoring solution that applies Big Data analytics to the challenge of collecting and analyzing data from distributed enterprise network in real time. WatchPoint applies WildPackets' best-in-class analytics to even the largest business networks for durations of up to 1 year—without compromising precision through sampling or polling. WatchPoint's single pane-of-glass view of the network and its historical reporting are unprecedented in detail and scope. They help IT administrators and line-of-business managers make better decisions faster about large, complex networks.
- **OmniEngines and Omnipliances,** software and hardware appliances, respectively, which collect and analyze network traffic on local segments and make that analysis available to local and remote users of OmniPeek, WildPackets' flagship network analysis tool, as well as to administrators using the WatchPoint dashboard
- **NetFlow and sFlow Collectors,** enabling organizations to take full advantage of the NetFlow and sFlow data collected by routers and other network equipment in their network.
- **OmniPeek** network analyzers that enable administrators to drill down into packet captures for Expert Analysis and other analytics that help reduce MTTR. OmniPeek analyzers include OmniPeek Enterprise (a stand-alone network analyzer that includes VoIP analysis and works both locally and through connections to OmniEngines and Omnipliances) and OmniPeek Connect (a remote console version of OmniPeek for connecting to OmniEngines and Omnipliances)

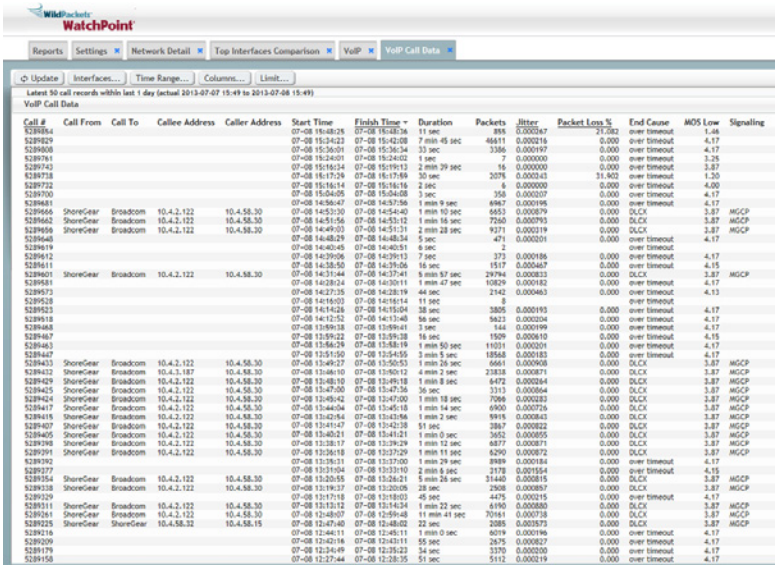
Combined into a single solution for distributed network monitoring, these products offer the following benefits:

- **Scalability**
  The WildPackets solution scales to monitor the largest enterprise networks. A single WatchPoint server can monitor up to 20 network segments. A major energy company uses WatchPoint to monitor the network health of its entire Point of Sale (POS) network in the United States.
- **Expert Analysis**
  OmniPeek, OmniEngines, and Omnipliances all automatically generate Expert Analysis of network traffic. WildPackets Expert Analysis helps IT organizations understand and troubleshoot network issues quickly.
- **VoIP and Video-over-IP Analysis**
  OmniPeek analyzers provide real-time VoIP and video-over-IP analysis.



7 Key Requirements for Distributed Network Monitoring

IT administrators can view the calls in the order in which they were captured, with caller, callee, and end cause information, as well as comprehensive signaling analysis of SIP, Cisco Skinny, MEGACO, and other protocols. OmniPeek Enterprise also evaluates and displays the call setup mechanism, in real-time, measuring call setup durations and providing a Call Detail Record (CDR) for each open call.

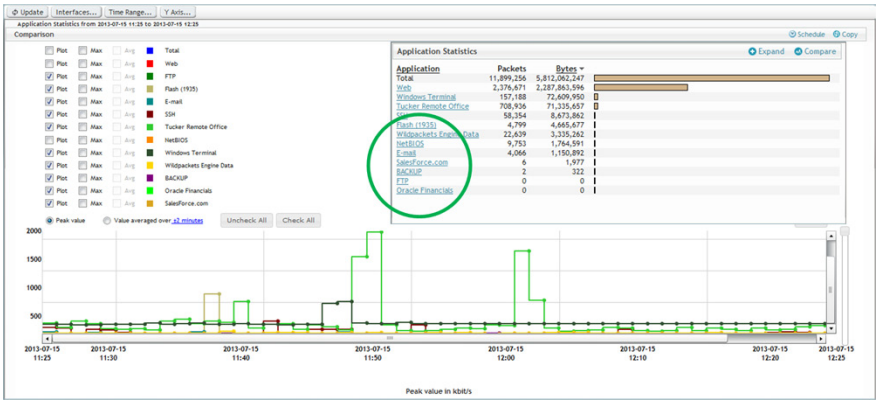


- **Support for 802.11ac and Other Wireless Protocols**
  WildPackets offers the only solution on the market that can address the complexities of today's Wi-Fi networks: multiple APs, multiple channels and sophisticated analysis modules to quickly highlight problem areas, all in real time. Early in 2013, OmniPeek 7.5 became the first network analysis solution capable of capturing and analyzing 802.11ac, the first WLAN specification to break the gigabit barrier, putting wireless networking speeds on par with those of wired networks. These higher speeds create problems for traditional wireless analysis techniques that use consumer-grade USB WLAN adapters.

- **Support for NetFlow and sFlow**
  WildPackets NetFlow and sFlow Collectors collect NetFlow and sFlow metrics and share them with WatchPoint and other analytical tools.

- **Support for Analyzing High-speed Networks**
  WildPackets supports high-speed analysis of networks up to 40G, supporting real-time packet-level analysis.

- **Long-term Reporting and Trend Analysis**
  WildPackets offer types of long-term reporting and trend analysis. WatchPoint analyzes traffic across all network segments under management for up to one year. The TimeLine Network Recorder captures and records all packets from a network segment for a period



ranging from days to weeks, supporting network forensic analysis and transaction analysis of 1G, 10G, and even 40G networks. Whether performing long-term trend analysis for capacity planning or SLA reporting, or zeroing in on a specific period of time for detailed forensic analysis, WildPackets has the reporting and analysis solution IT organizations need.

Through WatchPoint and its supporting products, WildPackets offers enterprises a single, scalable solution that supports both long-term trend analysis and network baselining, as well as immediate drill-down and packet-capture utilities for real-time troubleshooting. The solution enables enterprises to meet their tactical goals for reducing MTTR and optimizing network performance, while also supporting capabilities required for capacity planning, SLA monitoring, and operations management.

WildPackets network analysis solutions are used by leading enterprises and government agencies to monitor, optimize, and troubleshoot distributed networks. To learn more about the WildPackets solution for distributed network monitoring, visit www.wildpackets.com, email sales@wildpackets.com, or call +1 (925) 937-3200.

References

1. http://www.informationweek.com/storage/disaster-recovery/it-downtime-costs-265-billion-in-lost-re/229625441

2. To get a sense of the volume of video traffic, consider that Internet video traffic made up 57% of all consumer Internet traffic in 2012. That number is expected to rise to 69% by 2017, according to Cisco. http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html

3. http://www.infonetics.com/pr/2013/2H12-Networking-Ports-Market-Highlights.asp