VIAVI Solutions

White Paper

Deploying Probes and Analyzers in an Enterprise Environment

As an IT manager, you need visibility into every corner of the network, from the edge to the core. A distributed analysis solution can provide the coverage you need, but where should you deploy probes for maximum visibility at minimum cost? This paper describes by example how to plan and implement a monitoring/analysis infrastructure based on distributed probes. Because every network is different, the examples shown may not look like your network, but the concepts demonstrated will be applicable to most situations.

Background Concepts

Successfully deploying a distributed analysis solution on your network requires that you understand some basic concepts about distributed analyzers and network technologies. Here is a brief overview of some issues that you should understand when purchasing and deploying probe-based distributed analyzers.

Distributed Analysis: What is It?

Most commercial packet analyzers are distributed: Packet captures and some analysis are performed by distributed agents called probes, which in turn send the packets (or the analysis results—e.g., bandwidth utilization statistics, most active stations, etc.) to consoles for further processing and display. Distributed analysis is the only practical way to make different parts of a switched or wireless network visible and therefore manageable. From a single console, an IT administrator can monitor and view traffic from anywhere on the network where a probe has been deployed, from any type of media or topology (Ethernet, wireless, WAN, etc.)

Before you decide where (and what type of) probes should be deployed on your network, there are a few topological issues you should understand.

Accessing Half-Duplex Ethernet Traffic: SPAN Ports

On wired networks with multiple switches, most of the stations are plugged into half-duplex 10/100 ports, even if the backbone or server connections are GigE. Being able to see the traffic local to each switch at the edge can give you insight unavailable from tapping the core connections: For example, client-to-client communications are invisible from the backbone or server connections. It can also be useful to isolate a segment when troubleshooting client-to-core connection problems. The best way to achieve this kind of visibility is to configure SPAN (Switch Port Analyzer) sessions on each switch, and then direct the SPAN output to half-duplex 10/100 probes.

SPANs duplicate traffic on switch ports.

SPANs (also called port mirrors) duplicate the traffic on a switch port or a group of ports, and send the copied data out for analysis. A SPAN session can usually be configured remotely through the switch's administrative interface, allowing you to define which port's traffic to duplicate, and out of which port to send the duplicated traffic stream. A 10/100 half-duplex probe can be a dedicated appliance or a software-only agent installed on any station within the segment.

SPANs and half-duplex probes are inexpensive and convenient, but cannot give you all the visibility you need to manage and troubleshoot a network that also includes gigabit, WAN, and wireless infrastructure. For networks that include these other topologies, other solutions are available. These are described in the section that follows.

Accessing Full-Duplex Ethernet Traffic: Aggregators, TAPs and SPANs

Because full-duplex Ethernet (whether 100 Mb or gigabit) lies at the core of most corporate networks, ensuring completely transparent analyzer access to full-duplex Ethernet traffic is critical. SPAN port access is fine for the half-duplex Ethernet connections to stations at the edge, but may be unable to keep up with the higher-traffic full duplex links to the core.

There are three common ways for a probe or analyzer to gain access to full-duplex streams of data flowing on Ethernet cables:

1) Connect the probe to a SPAN port. Also called a port mirror, a SPAN port can provide a copy of all designated traffic on the switch in real time, assuming bandwidth utilization is below 50% of full capacity.
2) Deploy a port aggregator (sometimes called an "aggregator TAP") on critical full-duplex links.
3) Deploy a TAP (Test Access Port) on critical full-duplex links to capture traffic. For some types of traffic such as full-duplex gigabit links, TAPs are the only way to guarantee complete analysis, especially when traffic levels are high.

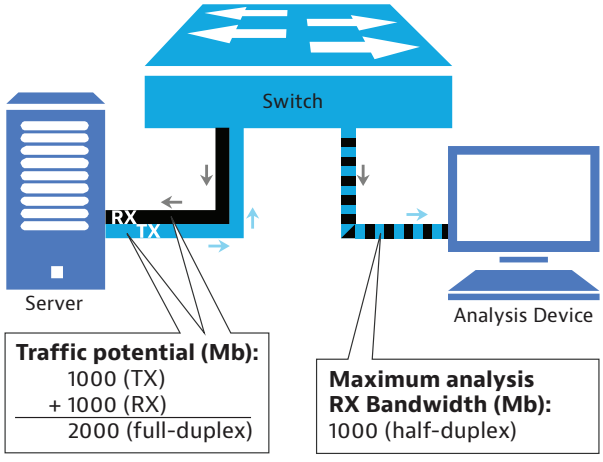
Connecting a probe to a switch SPAN/mirror port or aggregator can provide adequate visibility into most of the traffic local to the switch, assuming that bandwidth utilization is low. However, if the aggregate switch traffic ever exceeds 50% bandwidth saturation, SPAN ports and aggregators simply cannot transmit the data fast enough to keep up; dropped packets (and perhaps sluggish switch performance) will be the result. This is because SPAN ports and aggregators are designed to connect to a standard NIC, which allows them only one side of the fullduplex link to transmit data. A TAP, however, is designed to connect to a dual-receive capture card. By sending data on both sides of the link to the capture card, a TAP has double the transmission capability of the other options, allowing it to mirror both sides of a fully saturated link with no dropped packets and no possibility of degrading switch

performance. And regardless of utilization, SPANs filter out physical layer error packets, rendering them invisible to your analyzer.

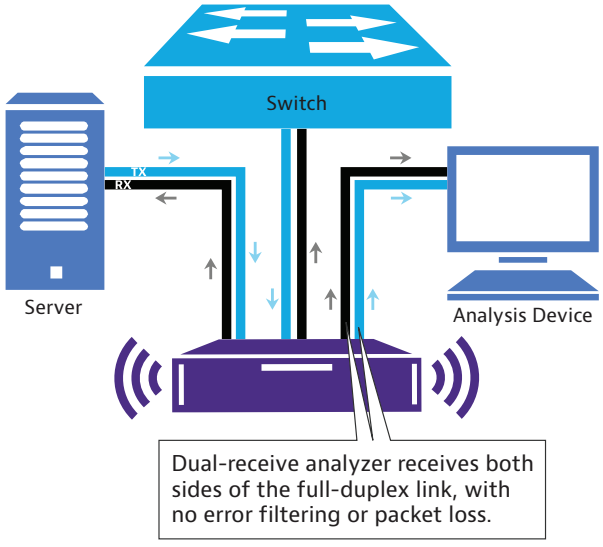
The most critical parts of your network are almost by definition those that see the most traffic. If your network includes a business-critical link (for example, the gigabit link that connects the customer service database to the core switch), a TAP connected to a compatible probe or analyzer is the only way to ensure both complete visibility and complete transparency to the network, regardless of how saturated with traffic the link becomes.

Aggregator TAPs drop packets at high utilization rates.

When analyzing traffic through a SPAN port, the switch's CPU copies the full-duplex signal, integrating RX & TX into one TX signal, routed to the SPAN port.



A TAP delivers both TX and RX signals, separately providing a pass-through signal for network traffic, and a full-duplex, line-rate signal to a monitoring device.



Wireless Probes

If you place an Ethernet probe on a switch to which a wireless access point is connected, you will see the legitimate wireless station traffic connected to your wired network. What you will not see is the 802.11 headers crucial to understanding wireless-specific problems and security threats. You will also not be able to see rogue access points, or illegitimate stations trying to associate with access points. In short, to see all RF signals on the air at your site, you need a wireless probe. In fact, you usually need more than one such probe to see all of the access points and stations (legitimate or illicit) deployed on the site.

Place probes only in busy links to manage their expense.

WAN Probes

A WAN connection is often an excellent place to have complete visibility of everything on the link, encapsulation and all. Not only will a dedicated WAN probe help to determine whether you are getting your money's worth from your Service Level Agreement, it will also be invaluable in enforcing your organization's Internet usage policies.

Without a dedicated WAN probe, encapsulation and control signals such as congestion notifications will be invisible to your analyzer. This is because routers strip the WAN encapsulation before forwarding the packets downstream into your network.

Assessing Your Network Visibility Needs

If your IT department is typical, you have a limited budget. Therefore, before you spend any money on analyzers, TAPs, and probes, you should assess what kinds of traffic you need to see and what kinds of traffic you want to see for effective network management. This will allow you to deploy the correct technology where you need it to meet your particular goals.

Probe Placement

To guarantee that every packet passing between every device on the network, errors and all, is available to your analyzer is practically impossible on a network with multiple switches. It would require placing a TAP on every link to each switch. Fortunately, you need only place probes where the traffic is significant enough to warrant the expense, and a lot of traffic isn't that critical.

Ultimately, where to deploy probes depends on the design of your particular network and where you require visibility. A probe only shows your analyzer the data that is visible to that probe. An Ethernet probe's visibility, for example, is limited to what a particular switch's SPAN port can deliver. A specialized hardware probe (such as WAN or GigE) connected through a TAP sees only the traffic traversing that link. If 100% coverage is important to you, install TAPs on all the high-speed critical links in or near the core of your network, and probe appliances plugged into the SPAN ports of switches on the edge.

For example, placing TAPs on the full-duplex links that connect servers or server farms to core switches will give you complete visibility into all traffic between server(s) and their clients. Connecting additional half-duplex probe appliances to SPAN ports at the edge of the network will let you focus in on any segment or station on the network for detailed problem resolution. Deploying a specialized WAN probe and TAP on a WAN link makes WAN frames and control sequences visible, in addition to showing all traffic flowing in and out through the link.

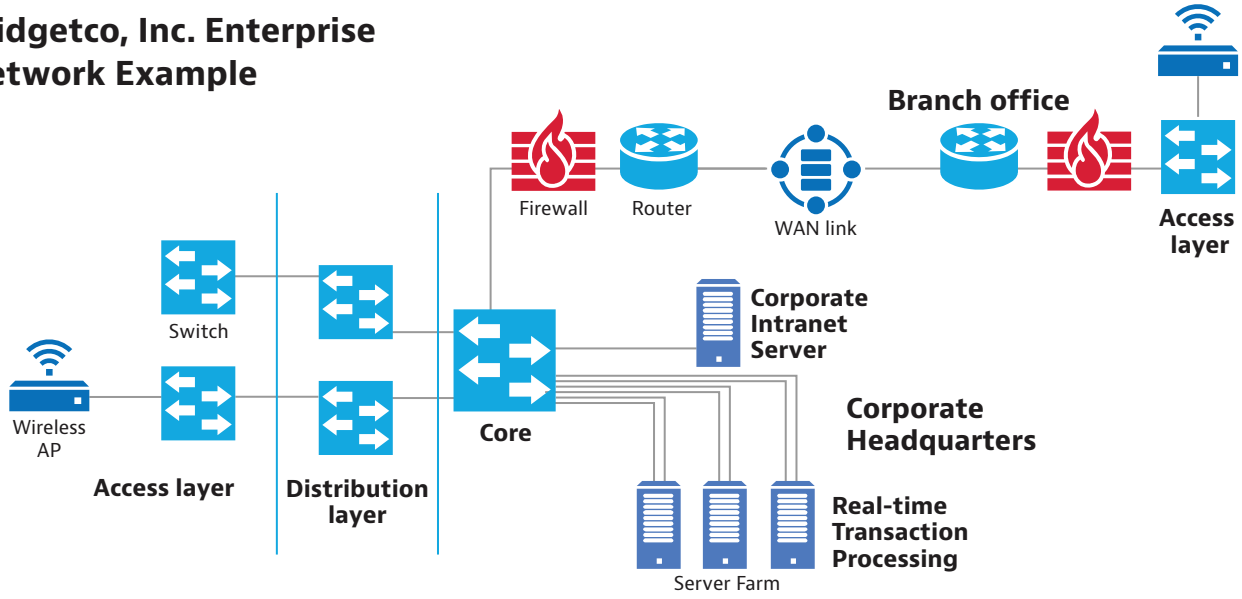
Failure to deploy the right probes in the right place can result in "blind spots" on your network. And an incomplete picture can lead to inefficient troubleshooting and expensive mistakes.

Mission critical trunk links should be monitored by probes.

Deployment Examples

Administrators at Widgetco, Inc. maintain a server farm at corporate headquarters that is linked to the core switch through multiple full-duplex gigabit connections that are defined as a single logical link (i.e., a trunk). Also connected to the core are distribution layer switches, which in turn are connected to access layer switches that service workstations at the edge. Branch offices are connected through a T1 WAN link. In addition to the wired stations, both corporate and branch offices deploy wireless access points.

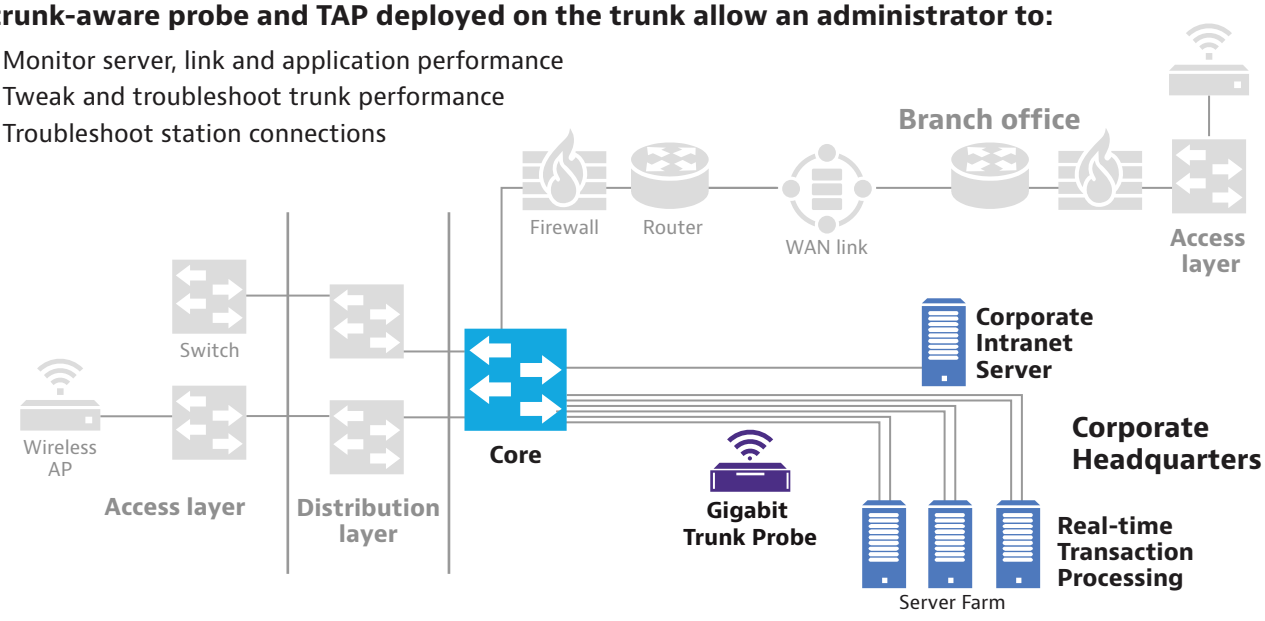
Widgetco, Inc. Enterprise Network Example



Because the real-time transaction processing system depends on it, the gigabit trunk is both business-critical and high-traffic. Therefore a specialized, trunk-aware hardware probe is recommended. Without a trunk-aware probe, administrators would be blind to problems with trunk configuration and aggregation. Trying to troubleshoot connectivity problems exclusively from the edge is not really possible, as you are not seeing enough information, such as physical-layer errors and trunk-specific control flags. A trunk-aware probe ensures Widgetco's administrators will know immediately if there is a problem with a particular physical connection within the trunk, which would be impossible to analyze from the edge of the network. Note that if you need to monitor a standard gigabit-linked server, simply deploy a standard gigabit probe.

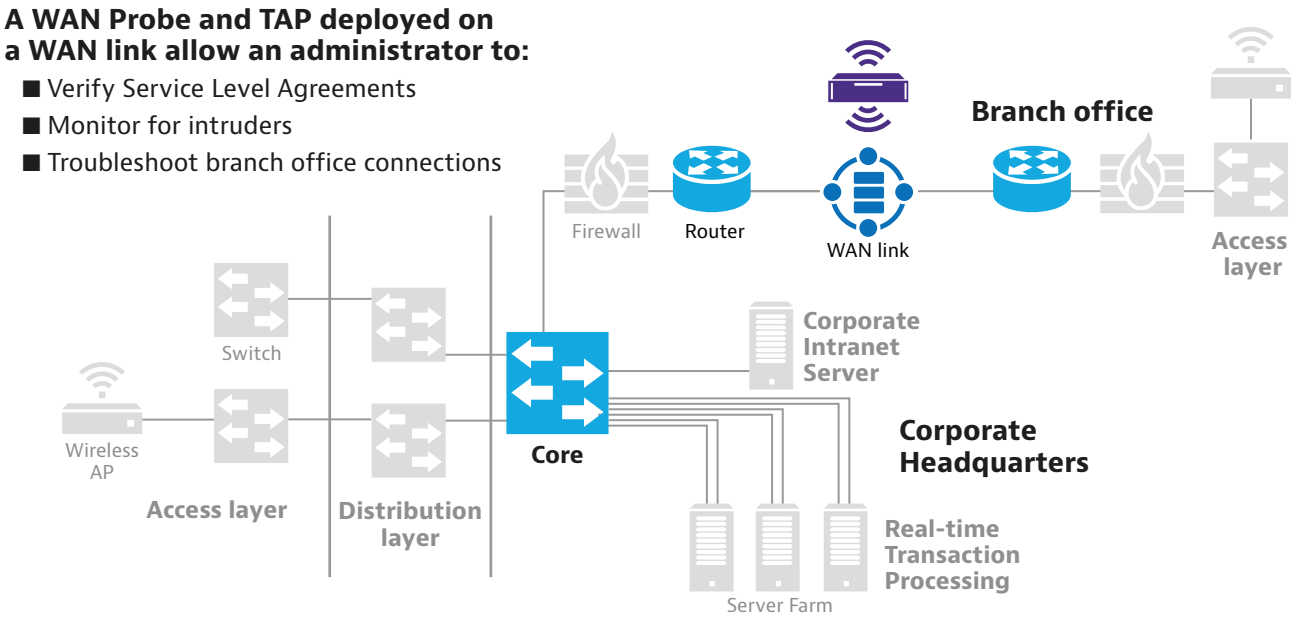
A trunk-aware probe and TAP deployed on the trunk allow an administrator to:

- Monitor server, link and application performance
- Tweak and troubleshoot trunk performance
- Troubleshoot station connections



Widgetco's corporate intranet server, on the other hand, is devoted to electronic versions of the employee handbook, newsletters, internal job postings, etc. Since it is not business critical (and not particularly high-traffic), Widgetco's administrator decides to leave that link to the core switch untapped.

Widgetco also decides to place probes and TAPs on all the WAN links that connect branch offices to corporate:



This is wise for a number of reasons. Its ability to ensure that the WAN service provider is delivering on your Service Level Agreement can pay for the probe rather quickly if there are performance problems. Keeping WAN links provided by ISPs monitored 24/7 has almost become a regulatory requirement for publicly traded companies like Widgetco, given the security concerns of any connection to the Internet.

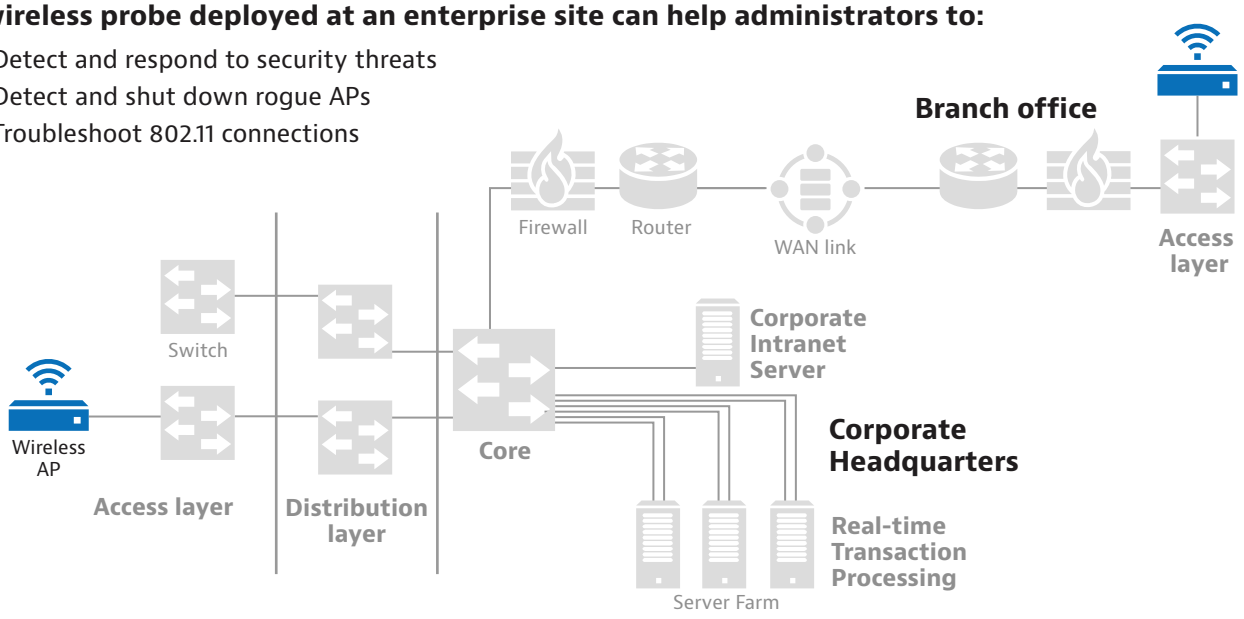
Network core and edge visibility are important today.

For station-level troubleshooting at the edge of the network, Widgetco has deployed a probe appliance on the port mirror of every access-level switch This also provides a way to enforce network usage policies. By monitoring for abnormal, extremely heavy bandwidth usage from stations, and filtering for banned application traffic, Widgetco's administrators can stay on top of peer-to-peer file sharing and other such network misuse.

Widgetco also deploys a number of wireless probes, not because the business depends on wireless, but for security reasons. In fact, Widgetco's administrators deploy wireless probes at branch offices with no officially sanctioned access points, allowing them to detect when employees set up their own (typically unsecured) access points so they can respond appropriately.

A wireless probe deployed at an enterprise site can help administrators to:

- Detect and respond to security threats
- Detect and shut down rogue APs
- Troubleshoot 802.11 connections



With probes and TAPs deployed in such a manner, Widgetco's administrators can see all network traffic wherever they need to, and they can do so from any analyzer console on the network.

Conclusion

If you are maintaining a large corporate network, buying a distributed analyzer is obviously the way to go. But because every network is evolving, being distributed isn't enough; you should look for versatility and scalability in your analysis solution as well. Deploying probes to meet your monitoring and analysis requirements as they change and grow won't be possible if you select a vendor with limited probe options.

In deploying probes, make sure that you understand the visibility requirements unique to your deployment goals and the design of the network you are analyzing. To summarize, for 100% visibility of traffic, which is critical to analyzing network operations:

- Deploy TAPs and specialized high-speed probes on core switch connections to servers, server farms, and other critical network infrastructure.
- Deploy less-costly probe appliances on switch monitor (e.g., SPAN) ports at the edge of your network.

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

© 2021 VIAVI Solutions Inc.
Product specifications and descriptions in this document are subject to change without notice.
probes-entenviro-wp-ec-nse-ae
30176211 901 0914