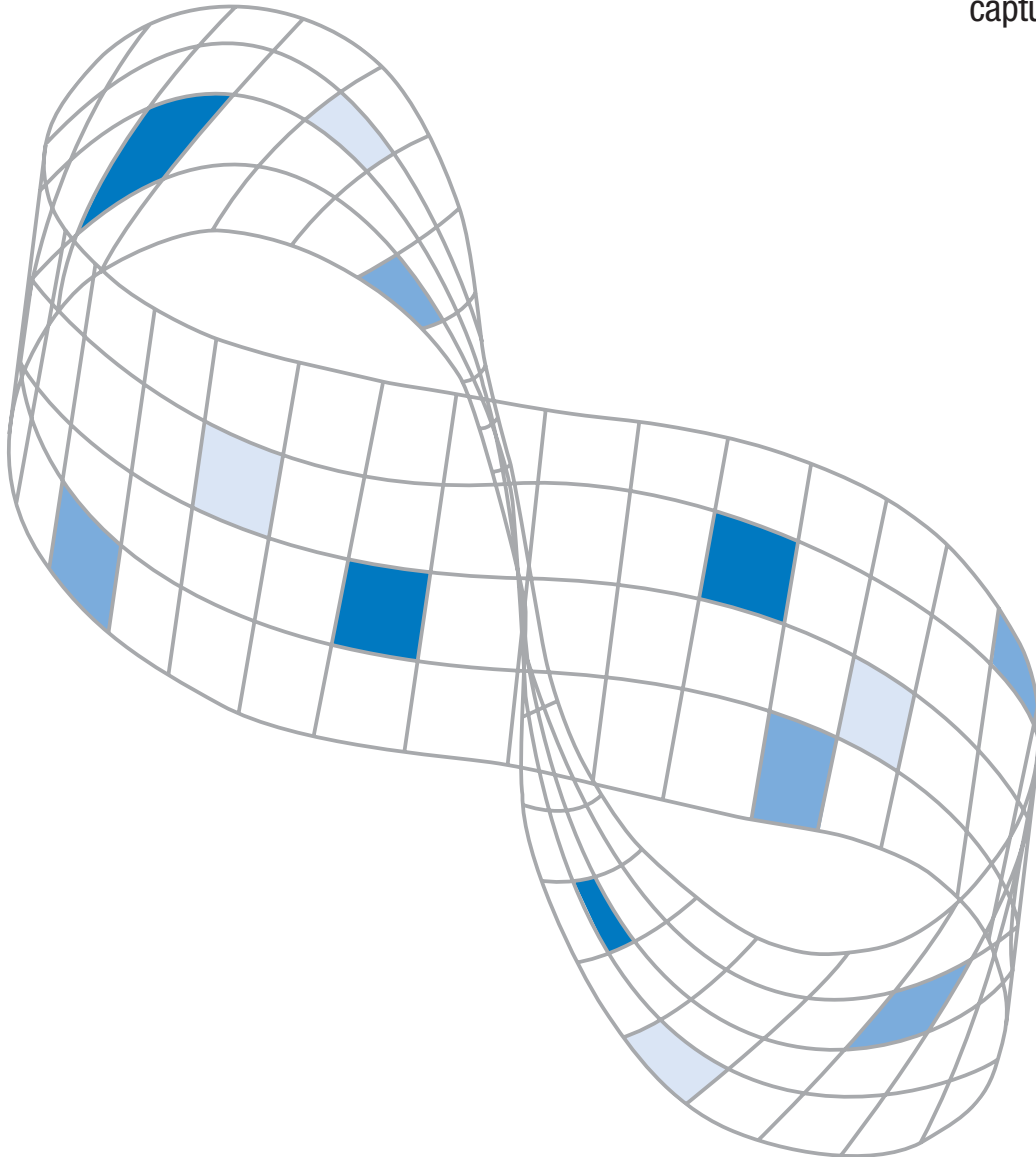


Analyzing Trunked Gigabit Ports

Monitoring Traffic in a Load-balanced Environment

Port trunking presents unique challenges for network analysis tools. This white paper examines the types of trunks currently being implemented and the implications for packet capture and analysis.



Analyzing Trunked Gigabit Ports

Summary

As hunger for bandwidth increases and the price of gigabit hardware drops, "making a bigger pipe" through port trunking is becoming more and more common. Such trunks present unique technical challenges for protocol analysis. This paper describes how Network Instrument's GigaTrunk Probe™ (GT Probe) solves these problems.

Keywords

Gigabit, full duplex, real-time statistics, trunks, GigaTrunk

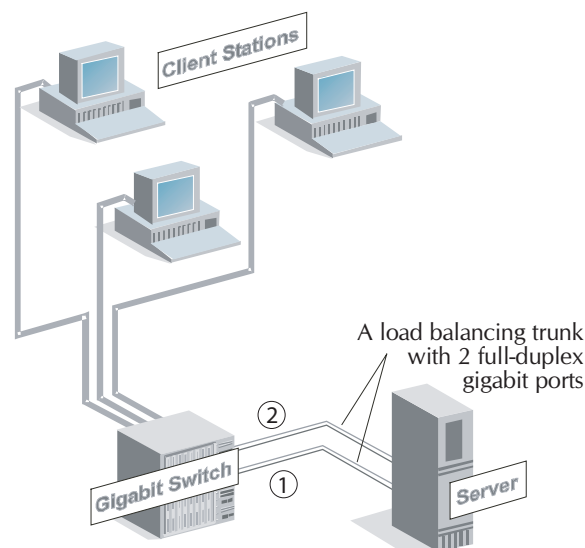
What is a trunk?

A trunk is a logical link consisting of multiple physical connections between network devices. Multiple connections increase bandwidth, and, more importantly, provide failover redundancy. Trunks ensure the high availability of business critical servers and inter-switch connections.

There are several methods to create trunks:

- Trunks implemented on Layer 2, such as Cisco Fast EtherChannel and Sun Trunking 1.0, depend on coordination with the switch to assign a single MAC address to multiple connections. This method is completely transparent to the rest of the network, and is easily configured to actively balance traffic load to make most efficient use of all connections.
- Trunks implemented on Layer 3, such as **Balance.nlm**, depend on specialized protocols that map a single network address to multiple MAC addresses. Layer 3 trunks can only balance the load in one direction without deploying a custom network protocol stack.
- Trunks implemented on Layer 1 (such as ISDN bonding) bond links at the physical layer, and require complex packet fragmentation and reassembly to perform load balancing.

Although Network Instruments GT Probe can be configured to analyze trunks implemented on Layers 1, 2, and 3, this paper focuses on load balanced layer 2 trunks, by far the most common configuration.



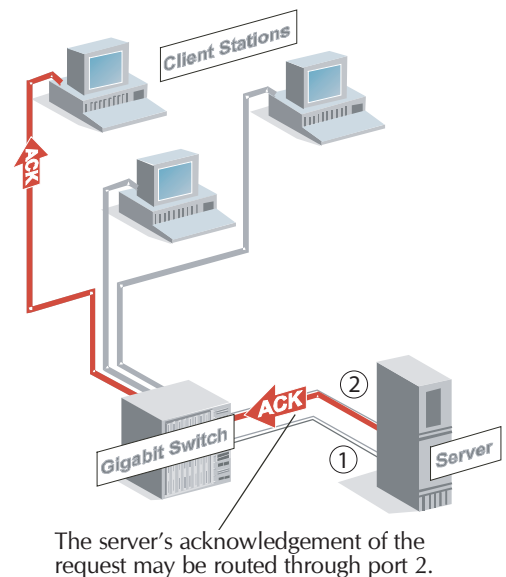
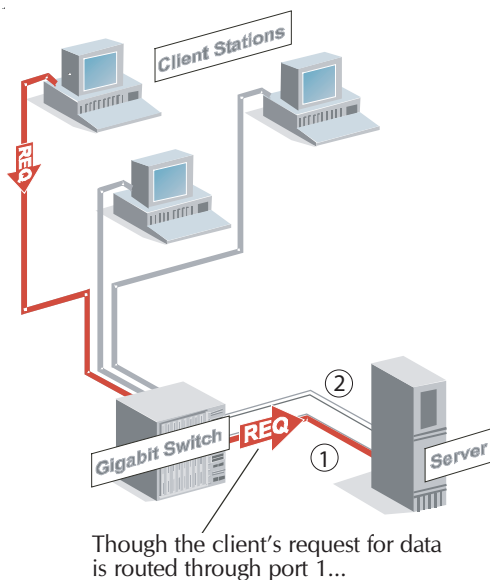
In client/server conversations, a packet going in either direction could travel on either port of the trunk.

How does load balancing affect your ability to monitor traffic?

Load balancing makes it impossible for a standard gigabit probe (or even multiple probes) to provide the analyzer console with a coherent view of the traffic because any piece of traffic can travel through any connection. For example, a client request to the server and the server's response could be routed through different connections. While this is all transparent to the client and server, it is not transparent to the analyzer, which must collect the data stream from each full-duplex connection with a separate TAP (Test Access Point).

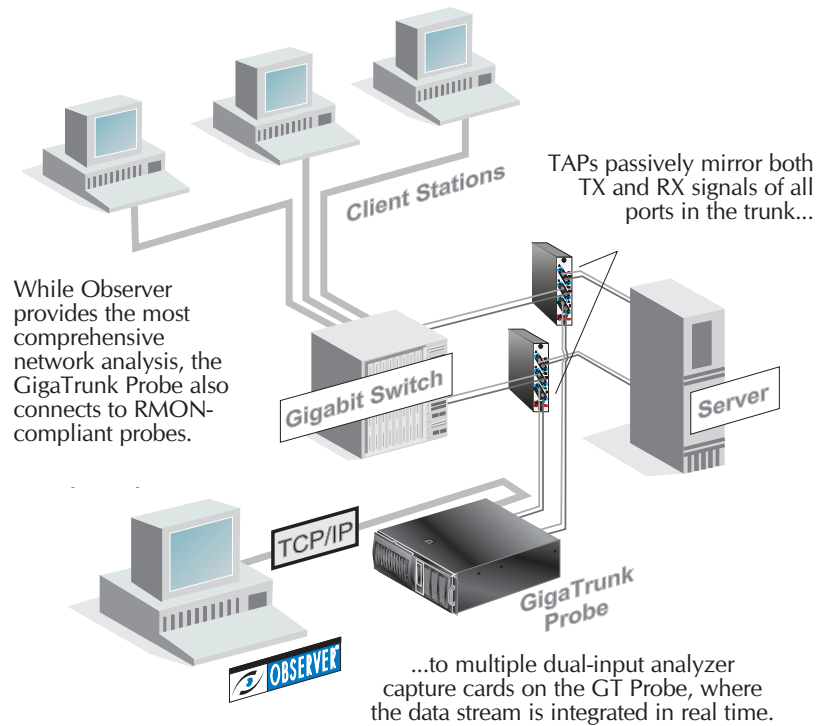
For example, imagine a two-connection trunk. If you TAP into each connection with separate probes, the console would not be able to integrate the two data streams for a coherent view of traffic.

The analyzer could show invalid errors such as missing ACKs because it would be incapable of putting the independent data streams together in the correct sequence. Accurately analyzing network conversations is entirely dependent on seeing the sequence of packets as well as their contents.



Network Instruments GigaTrunk Probe

Network Instruments GigaTrunk Probe integrates the data streams coming from all of the trunked connections (up to 8), feeding the console a complete, fully integrated stream of traffic data from all ports (TX and RX), sequenced correctly by timestamps. The GT Probe is a high performance rack mount system equipped with multiple full-duplex gigabit analyzer capture cards, and specialized software to integrate the data stream.



Conclusion Network Instruments' GigaTrunk Probe plus Observer: Putting the Pieces Together for You

Network Instruments has engineered the high-performance solution you need to dependably monitor the trunked connections in your mission critical network infrastructure. And, it's part of Network Instruments' Distributed Network Architecture (NI-DNA™), meaning that it works seamlessly with Observer's family of software and hardware based network analysis solutions.

Network Instruments, LLC, 8800 West Highway Seven, Fourth Floor, Minneapolis, MN 55426 telephone (952) 932-9899 fax (952) 932-9545
Network Instruments, 7 Old Yard, Rectory Lane, Brasted, Westerham, Kent TN16 1JP United Kingdom telephone +44 (0) 1959 569880 fax +44 (0) 1959 569881