NEXUS TELECOM
NETWORK MANAGEMENT SOLUTIONS

WHITE PAPER

# The NexusTRACE Pseudo Port

## Displaying Directional Information of Network Traffic


::: **Issued Date** 08 MAY 2007

::: **Author** Walter Sachs

::: **Issued by** Nexus Telecom, Switzerland

::: **Document** T-21-25015


We work to improve your network

# Table of Contents

# 1 Introduction

There are currently just two ways of monitoring network traffic of a remote workstation, located in another town, for example:

1. Travel to the remote site, break the cable and physically install a protocol analyzer; or,
2. Install a software protocol analyzer demon on the remote workstation.

A more convenient way to monitor a remote workstation's traffic would be to monitor the traffic from a central point in the network (e.g., the backbone). By filtering the traffic and analyzing source/destination fields within the data blocks, the precise port traffic can also be captured. The only problem, of course, is determining the data direction of each captured block (i.e., send or receive), which is only available when monitoring the traffic directly at the remote workstation's port.

This paper examines the possibility of utilizing what we refer to as a "Pseudo Port" in order to capture and display the direction of IP-based traffic information — even if the tapping point is in the backbone.

## 1.1 The Problem Identifying Data Direction

With Internet Technology (IT), it is quite common for two switches, each with many IP-devices, to be connected via a trunk.

When, for example, Server 2 is not operating properly and troubleshooting technicians want to analyze the network traffic sent and received by Server 2, they would have to set up a network analyzer to troubleshoot this port. (See Figure 1 in which a Network Analyzer is shown running on Server 2.)

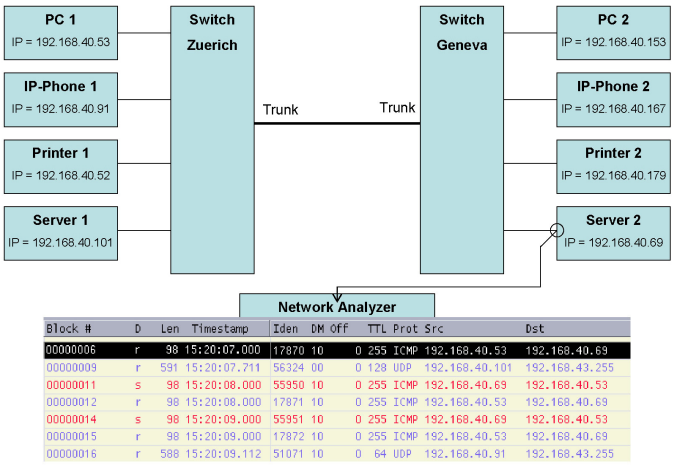



**Figure 1**

The protocol analyzer screenshot in Figure 1 shows the port traffic at Server 2. In this case, the direction of each packet (receive/send) is easily observed. However, if the Network Operating Center (NOC) is located in Zuerich, physically installing such a network analyzer would require the technician or engineer to travel from the NOC in Zuerich to the site of Server 2, incurring travel time and man hours costs for the physical set-up of the TAP at Server 2, not to mention likely service disruptions.

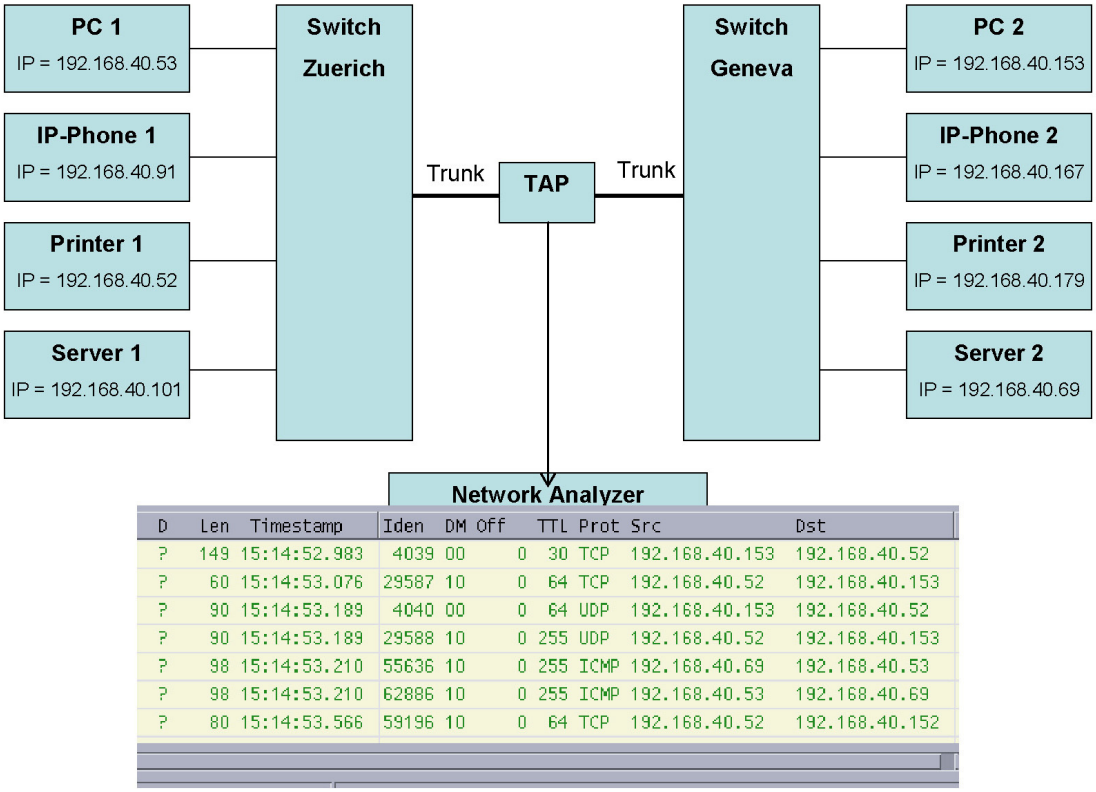



**Figure 2: D for Direction and ? for Passing Block**

To avoid these expenses, an alternative solution would be to set up a TAP on the trunk between the switches, which is much closer to the NOC. Network filters can be used to limit the amount of traffic seen on the network analyzer, isolating the traffic going to/from Server 2. With the TAP on the trunk, however, the network traffic's direction can only be seen from the TAP's point of view (i.e., the TAP sees all blocks as "passing blocks"). Send/receive information is not directly observable.

It is not possible to mark a block as `sent` or `received`, even if the source (`Src`) and destination (`Dst`) information is processed, because the observer's point of view is not unique. For example, in Figure 1 where the Network analyzer is directly and internally attached to the port of Server 2, the observer's point of view is clear — all packets are shown from the perspective of Server 2's port (i.e., network packets leaving the server are marked as `sent`, packets incoming to the server [`ingress traffic`] are marked as `received`).

As an example, we can examine two ICMP packets, as shown in Figure 3. From the TAP's point of view, all blocks are passing blocks and it is impossible to identify which network device sent the Echo and which one replied — the information of the direction (D) is lost, as represented in Figure 3 by the question mark (?).

| Block # | D | Len | Timestamp | Type | Code | Description |
|---|---|---|---|---|---|---|
| 00000191 | ? | 70 | 15:14:52.062 | 5 | 1 | Redirect |
| 00000192 | ? | 70 | 15:14:52.102 | 11 | 0 | Time Exceeded |
| 00000193 | ? | 98 | 15:14:52.210 | 8 | 0 | Echo |
| 00000194 | ? | 98 | 15:14:52.210 | 0 | 0 | Echo Reply |
| 00000201 X | ? | 98 | 15:14:53.210 | 8 | 0 | Echo |
| 00000202 | ? | 98 | 15:14:53.210 | 0 | 0 | Echo Reply |
| 00000208 | ? | 98 | 15:14:54.225 | 8 | 0 | Echo |

**Figure 3**

## 1.2 The Pseudo Port Solution

By shifting the observer's point of view away from the TAP to the network device under observation, two problems are solved:

- Unnecessary packets are not displayed anymore, i.e. only packets sent or received by the network device under observation are displayed.
- Traffic direction can now be added to the displayed packets.

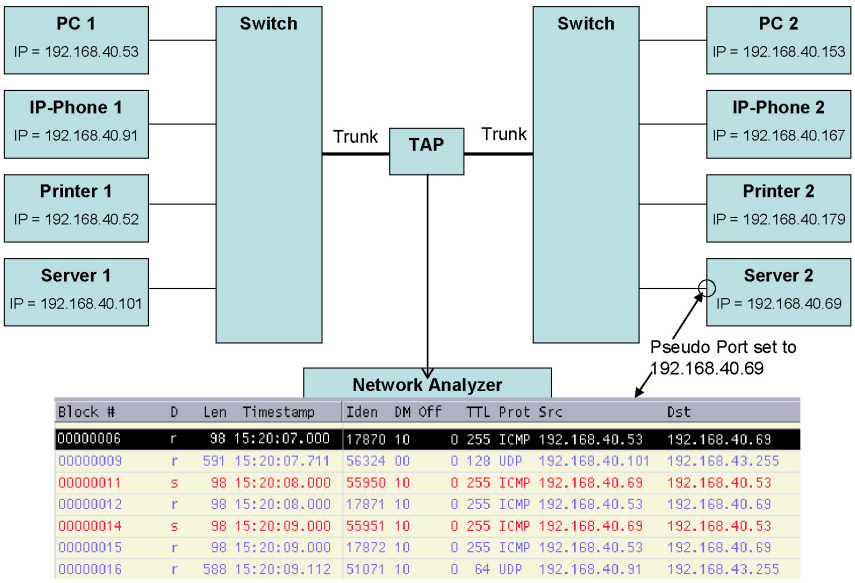
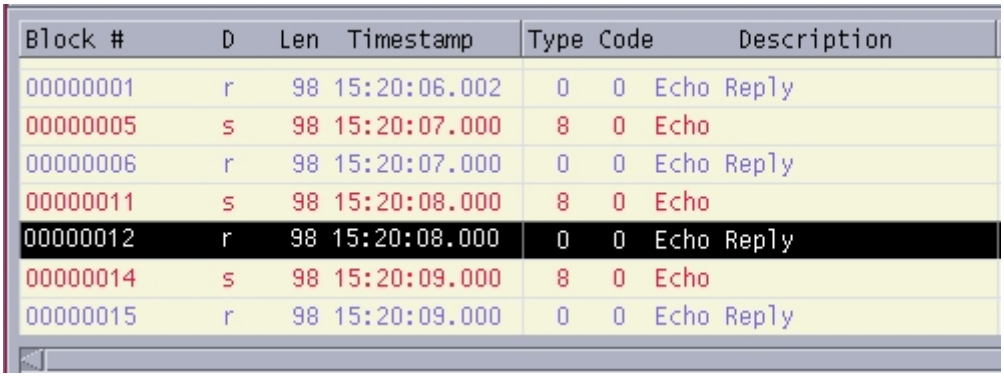



**Figure 4**

With the amount of displayed data reduced (i.e., only blocks sent and received by Server 2 are displayed and color-coded [red is sent]), the observer's point of view is now that of Server 2's port.

Further drill-down also shows which device sent the ICMP Echo request:



| Block # | D | Len | Timestamp | Type | Code | Description |
|---|---|---|---|---|---|---|
| 00000001 | r | 98 | 15:20:06.002 | 0 | 0 | Echo Reply |
| 00000005 | s | 98 | 15:20:07.000 | 8 | 0 | Echo |
| 00000006 | r | 98 | 15:20:07.000 | 0 | 0 | Echo Reply |
| 00000011 | s | 98 | 15:20:08.000 | 8 | 0 | Echo |
| 00000012 | r | 98 | 15:20:08.000 | 0 | 0 | Echo Reply |
| 00000014 | s | 98 | 15:20:09.000 | 8 | 0 | Echo |
| 00000015 | r | 98 | 15:20:09.000 | 0 | 0 | Echo Reply |

**Figure 5**

Server 2 is sending the Echoes, while another device(s) is responding.

## 1.3 Shifting the Observer's Point of View - A Technical Perspective

As we have seen, it would be beneficial to set the observer's point of view. This can be achieved by examining the Protocol stack on the IP or MAC layer to determine whether a block is sent or received.

### 1.3.1 NexusTRACE

NexusTRACE is the telecom industry's remote protocol analyzer of choice for Nortel MSS/Passport and Alcatel 3600 networks.

NexusTRACE is also the network technician's tool of choice for decoding, interpreting and troubleshooting complex protocol stacks in IP networks. Even without on-switch trace capability of IP switching elements, NexusTRACE can still perform remote protocol analysis and troubleshooting using the Pseudo Port principle described in this paper.

*NOTE: The Pseudo Port functionality will be available with NexusTRACE 7.2.*

Figure 6 shows how a Pseudo Port is set up in a Network Protocol Analyzer. From this NexusTRACE window, the user can define a Pseudo Port (i.e., the observer's point of view).

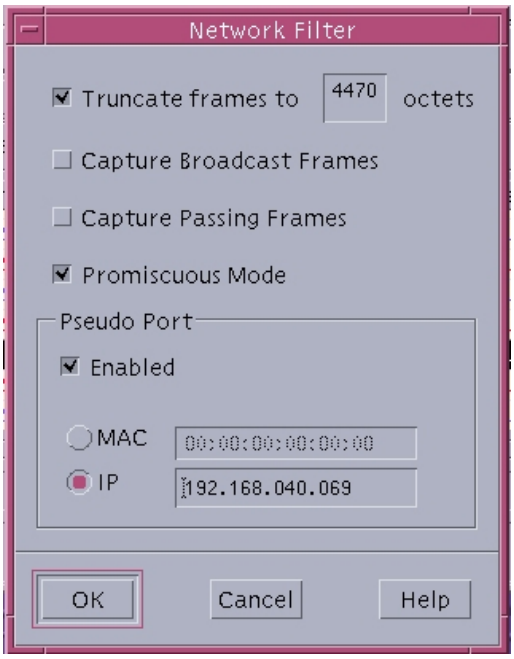



**Figure 6**

Thus the Protocol Analyzer is able to mark the blocks as `sent` or `received` by examining the Protocol stack (see Figure 7).

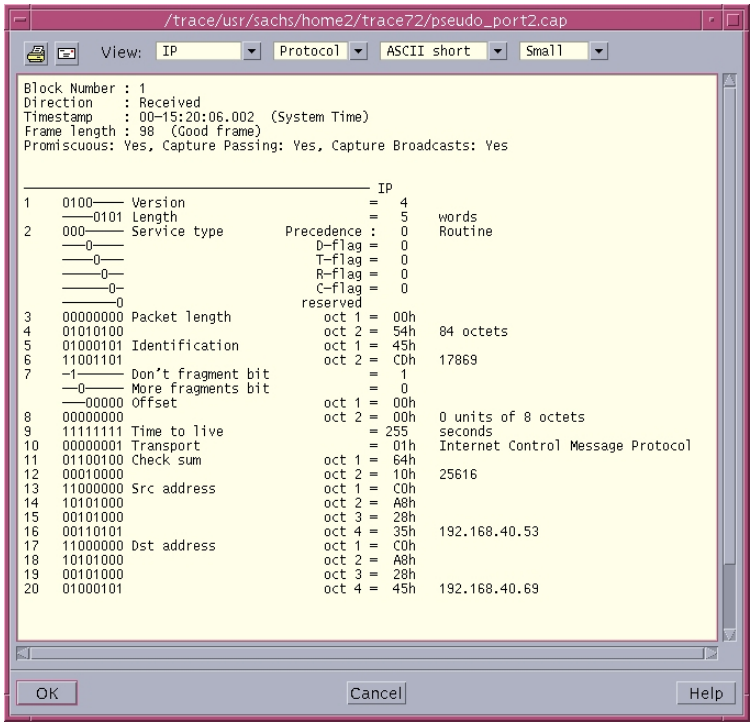



**Figure 7**

The direction, as seen from the Pseudo Port's point of view, is determined by comparing the Pseudo Port IP (e.g., as defined in Figure 6) to the `Src` and `Dst` address of each frame.

If a match is found for the `Src` address, the frame is marked as `Sent`; if a match is found for the `Dst` address, the frame is marked as `Received`.

The Pseudo Port can be set up on the MAC-layer as well, for which the same logic applies, with the check held against the MAC addresses.

*NOTE: Special care has to be taken for broadcast and passing frames.*

## 1.4 Conclusion

When Port Mirroring, Tapping or Spanning an Ethernet device, we are presented the captured data in a non-intuitive format and are, as such, unable to properly analyze the data.

The NexusTRACE Pseudo Port feature displays data as it would appear when coming directly out of the Network device it is monitoring and makes network analysis on Trunk/Backbone lines possible for the first time. This greatly simplifies troubleshooting scenarios.

By implementing a Pseudo Port to shift the observer's point of view to the device under investigation, the network data can be presented in an intuitive way, as if one were sitting directly on the IP-device's network interface.

It is possible to implement a Pseudo Port for any kind of network analysis, including non-Ethernet networks, as long as it is possible to extract the `Src` and `Dst` information from the captured frames. A Pseudo Port could even be applied to IP-Subnets, VLANS or MPLS networks.

With an established Pseudo Port, all statistics and utilization data from any device within the network can be adapted for view by an NOC-operator by simply tapping/mirroring one or more central points of the Network.

The Pseudo Port is also useful for local and remote port mirroring: Where the network traffic direction is lost, the Pseudo Port can "re-capture" and display this data.

Lastly, the Pseudo Port can support forensic analysis (i.e., network analysis after an attack), because the Pseudo Port enables continuous network monitoring and tracing on central points. In the event of a network attack, the appropriate Pseudo Port settings can be retroactively applied to the captured data and changed as required, thus making it possible to view different devices offline and to replay the network traffic from different point of views.

# 2 About Nexus Telecom

Founded in 1994, Nexus Telecom (www.nexustelecom.com) is a privately-held company with headquarters in Zurich, Switzerland and a North American subsidiary in Ottawa, Canada. With over 200 employees, Nexus Telecom is a major OSS/BSS vendor delivering sophisticated state-of-the-art telecom management solutions to 2G, 3G, NGN and VoIP service providers and network operators worldwide.

Nexus Telecom specializes in Service Assurance, Revenue Assurance and Network/Service Testing solutions, supporting the most recently developed technologies and standards. Nexus Telecom's fast time-to-market strategy is to gain early in-depth know-how about upcoming network technologies through strong development partnerships with leading network manufacturers such as Siemens, Lucent, Nortel, Nokia, and Ericsson, to name a few.

**Nexus Telecom Zurich**

With solutions deployed in over 100 countries, Nexus Telecom's installed customer base spans the globe, assuring service quality and revenue streams for many of the world's best-known telecom operators. For small and large service providers alike, including the world's largest GSM/UMTS network operated by T-Mobile, the highly scalable and modular E2E solutions from Nexus Telecom maximize the service provider's competitive edge through excellent ROI, quick and smooth launch of new services, and greatly increased end-customer satisfaction.

Nexus Telecom is certified according to the ISO 9001 Quality and Management Standards.


We work to improve your network



**Nexus Telecom AG**
**Wireless Network Systems**

Muertschenstrasse 27, P.O. Box 1413
8048 Zurich, Switzerland
Tel: +41 44 355 6611
Email: sales@nexustelecom.com

**Nexus Telecom AG**
**System Solutions**

Feldbachstrasse 80, P.O. Box 215
8634 Hombrechtikon, Switzerland
Tel: +41 55 254 5111
Email: sales@nexustelecom.com

**Nexus Telecom (Americas) Inc.**
**(NA and CALA)**

Suite 100, 1101 Prince of Wales Drive
Ottawa, Ontario, Canada K2C 3W7
Tel: +1 613 224 2637
Email: sales@nexustelecom.com