



How to identify a "Network Tap Point"

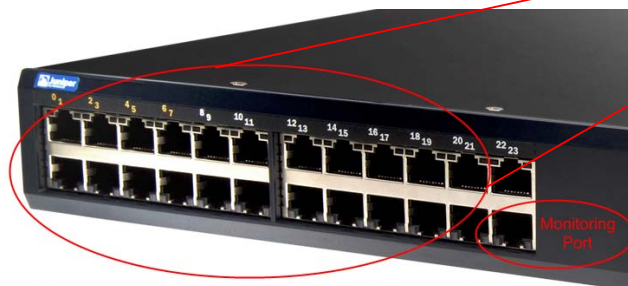
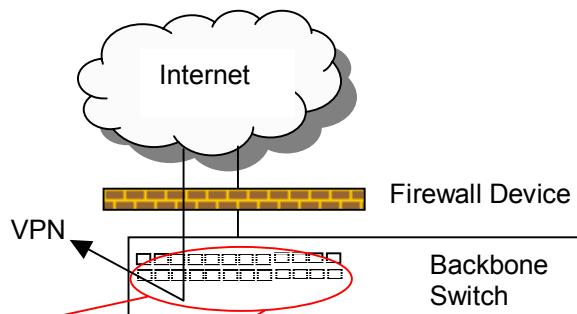
Congruity Inspector™ Software requires a "Network Tap Point" to monitor all traffic and communications entering and leaving the protected local area network. A "Tap Point" is a network device' port configured to mirror (copy) all **INBOUND AND OUTBOUND** traffic entering and leaving the protected network. Each manufacturer has its own name for a monitoring port as noted below. If you are not sure a device has "mirroring" capabilities, do a Web search for the specs and documentation. A monitoring port is needed for proper installation of Congruity Inspector or any other network promiscuous device: Sniffer, Snort, Wire shark. **Clicking on the Vendor's name below links to their "Monitoring Port" set-up documentation.**

Vendor Name:	Term for Dedicated Analyzer Port
CISCO Catalyst , Cisco ASA	Port Spanning (SPAN: Switched Port Analyzer Port)
3Com	Roving Port Analysis
Dell PowerConnect	Mirror Port
Foundry , Extreme , Juniper	Port Mirroring
Nortel	Remote Port Mirroring
Alcatel XLAN	Mobile Port
HP Procurve Manuals , HP Port Conf.	Monitoring Port

Identifying the tap point

You must connect the Congruity Inspector workstation to a dedicated monitoring port on the managed switch located just inside the firewall or router. All the internal traffic (sub-nets, workstations, servers and communications) should aggregate through this device and be visible on the mirror port to profile network status.

NOTE: Congruity Inspector can only monitor network traffic that it can see on the monitoring port. Certain network configurations may not provide a tap point and require special consideration. See information below. VPN circuits, depending on the equipment, may not be visible to the monitoring port.



Configure mirror port to copy all internal traffic, including firewall port, to that single port.

Copy all the internal network ports & firewall port to a single monitoring port

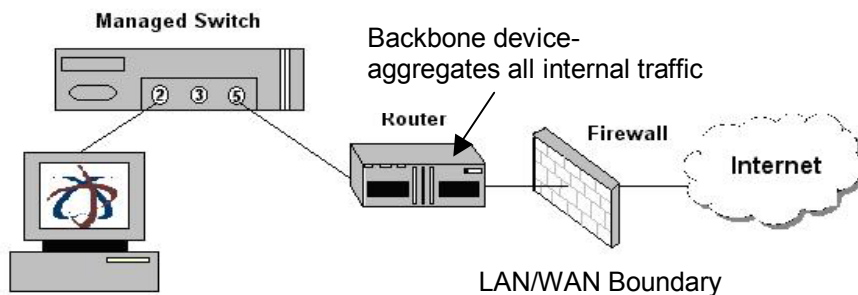
Considerations for Establishing a Tap Point/Monitor port:

1. Understand the capabilities and limitations of your managed switch or router. Most device manufacturer's have on-line manuals to verify if your model can establish a monitoring port or not.
2. Some switches can be configured as "receive-only" or "receive/transmit." Congruity Inspector needs to see both received (inbound) and transmitted (outbound) traffic on mirrored ports so the correct setting should be "receive/transmit".
3. The monitoring port itself should also have the ability to transmit data. This feature is needed in order for Congruity Inspector to perform DNS look-up resolving machine names to IP addresses.
4. Where establishing a native monitoring port is not possible, there are other devices that can be plugged in-between the gateway switch and the firewall to create a way to monitor network traffic. A Flat Hub (single collision domain on all ports) placed in-between the gateway switch and firewall creates a method of monitoring all traffic. Flat hubs, unfortunately, aren't very common these days. Most inexpensive networking devices (Linksys, NetGear) are in fact switches. Each port only sends and receives its own traffic. Another method is using a "[passive tap.](#)" These are in-line devices that can be plugged into the network to unobtrusively monitor traffic. Once installed, they can be left in-place for regular diagnostics, troubleshooting and system monitoring. There are commercial models available and there are instructions available for making your own passive tap. With some modest wire diagrams and components purchased from a local hardware store or Radio Shack, you can make your own "passive tap" for less than \$20 dollars.

Configuration Examples:

Managed Switch/Router with Mirroring/Spanning Capabilities

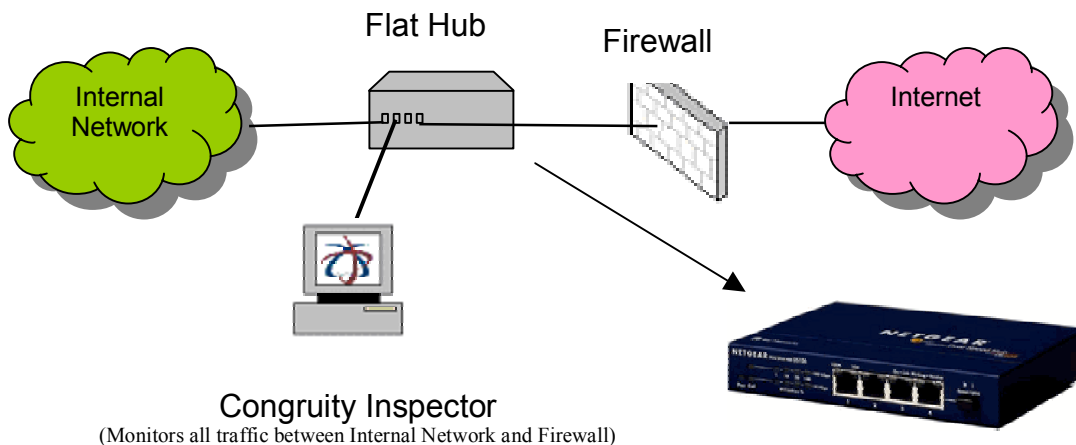
In networks that contain a managed switch or router, you can use the device's configuration software (command line or network management software) to select a port on the switch that is dedicated to a network analyzer such as Congruity Inspector. This port is commonly referred to as the "mirror", "monitoring" or "span" port. All these terms simply mean that the switch has the capability to send a copy of all the network traffic frames that pass through its other port(s) to this special analyzer port. *Not all switches have the capability to mirror or span traffic. Check your switch's documentation to see if this capability exists, and for instructions on how to configure a port for mirroring, monitoring or spanning.



In this example, traffic passing through the router on port 5 is being mirrored to the analyzer port (port 2). Since the Congruity Inspector workstation is connected to port 2, it can see every frame that passes through port 5.

Hub-based Setup or Passive Tap Point:

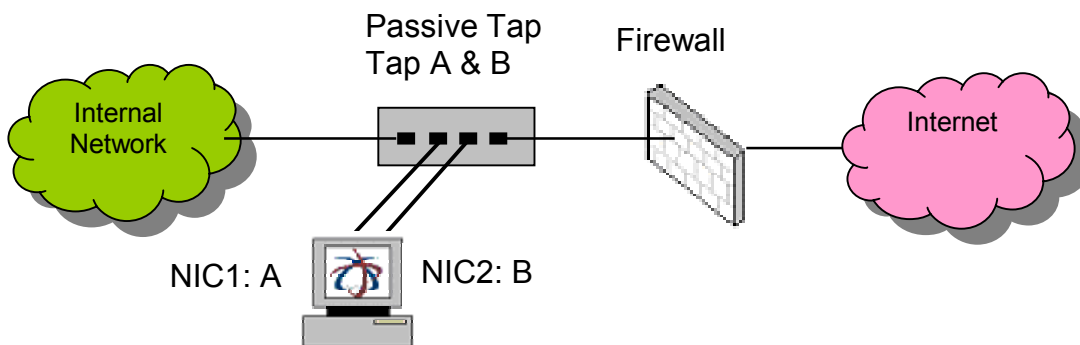
For environments that don't have managed switches/networks or native port monitoring features. In a hub-based setup, all incoming and outgoing network traffic passes directly through the device without the use of a switch. Plug the firewall cable and the cable from the backbone switch into the hub. Consequently, you need only plug the Congruity Inspector workstation into the device to monitor all network traffic.



Hub example: Netgear: 4-port 10/100 Mbps Compact Hub (DS104NA).

Passive Tap Set-Up

A passive network tap device provides visibility into network traffic without introducing a single point of failure.



Congruity Inspector 2 NIC configuration
(Monitors all traffic between Internal Network and Firewall)

Learn how to make a own network tap: [here](#), [here](#) or you can buy a unit on [eBay](#). Commercial Taps: [here](#).

Congruity Inspector V3.23 supports two-card monitoring. At a command prompt in the Congruity install directory type: `dbmaint - cards 2` and hit Enter. You will see a message indicating 2 card mode. Go back to the Inspector GUI interface and Click "Configuration Tab=>Status=>Restart" Click the Restart button at the bottom of the page. When the system has restarted you will have two NIC selections which you can choose for two-card monitoring purposes such as with a passive tap device.

Verifying Proper Set-up of Congruity Inspector

The illustration below creates a monitoring point in-between the firewall and internal network where the PC running Congruity Inspector software can see all inbound and outbound traffic activity. When Congruity Inspector is configured with the local network address scheme and mask, defining the internal protected network, all other IP addresses entering the network are identified as external.

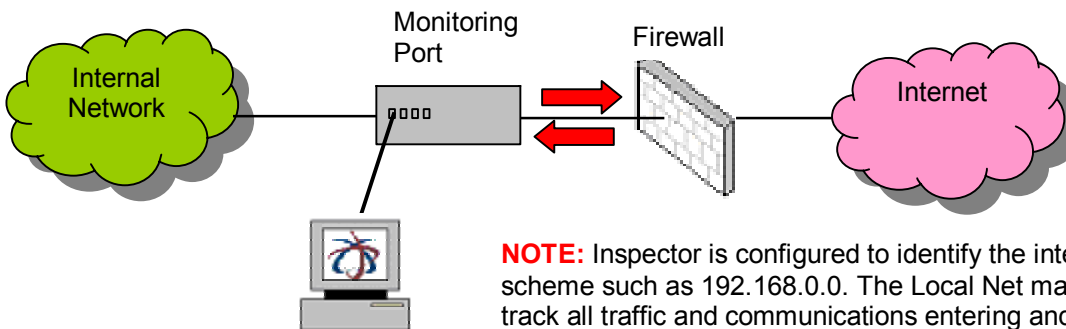
Once the tap point has been set-up with the Congruity Inspector PC connected to the port and the software having collected data for at least 30 minutes, you can verify proper set up by logging into the report interface (**username: Accord password: guest**) and Click on the Clients Tab on the left and =>Clients Tab along the top to review the operational status. See NOTE below.

The screenshot shows the Congruity Inspector web interface. The main content area displays a table titled 'Active TCP/IP Addresses' for the period 3/10/2008 - 3/10/2008. A red circle highlights the 'Bytes' columns (Inbound and Outbound) for each client.

Internal Client	Outbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
congruityone	1081	8	153.61 MB	143.46 MB	10.14 MB
naudit	1257	136	151.84 MB	145.49 MB	6.35 MB
firefly	813	4	95.68 MB	89.73 MB	5.95 MB
congruity	5	0	89.60 KB	36.77 KB	52.83 KB
Totals: 4	3,156	148	401.21 MB	378.72 MB	22.49 MB

NOTE: You should see both **Inbound and Outbound Bytes** column listed for each Internal Client. If there are zeros under one of the Bytes columns, the tap point is only transmitting one side of the bi-directional traffic feed.

Also, if you only see a subset of the internal clients you expected to see, the mirror port may not include all the internal switch ports and network devices.



NOTE: Inspector is configured to identify the internal IP address scheme such as 192.168.0.0. The Local Net mask is used to track all traffic and communications entering and leaving the defined protected network.

Special Network configurations: Congruity Technologies provides engineering assistance to identify optimal circumstances to locate and install the Congruity Inspector PC. [Contact us](#) for more details.