Introduction to TAPS

A guide for monitoring network traffic with Test Access Ports

Ideal for security, network monitoring and end-to-end performance analysis

What is a TAP

TAP stands for Test Access Port. It is a network device that is placed on an Ethernet segment which can then provide a copy of that traffic for analysis with network tools like Wireshark, Snort or other monitoring tools.

Why use TAPS

- For secure 24/7 point of access for network tools for for troubleshooting
- All fiber taps are passive devices and will not be a single point of failure
- They make copies of data in real-time with very little or no traffic delay
- They are physical layer devices, able to provide all traffic over that link for analysis
- TAPs are low cost and a highly reliable way to provide data non-intrusively to network tools
- They can be used to provide the physical layer traffic to other aggregation devices, complementing the collection from a SPAN or Port Mirror captures for improved analysis
- They allow you to retain use of ports on network switches

Aggregation?

Use an Aggregation Tap when:

- You need to monitor both directions of full duplex transmissions but your monitoring tool only has one NIC (full duplex aggregation)
- You need to monitor aggregated* or non-aggregated** traffic from one link with multiple tools (regeneration)
- You need to monitor aggregated or non-aggregated traffic from multiple links with one tool (link aggregation)
- The number of links you need to monitor exceeds the number of tools you have available (link aggregation)
- Your network links and tools are not the same made up of various media types (media conversion)

* The sum of aggregated traffic from all network links should not exceed 100% of the monitoring port bandwidth

** Most models can be configured to perform aggregation and/or function like a standard nonaggregating tap

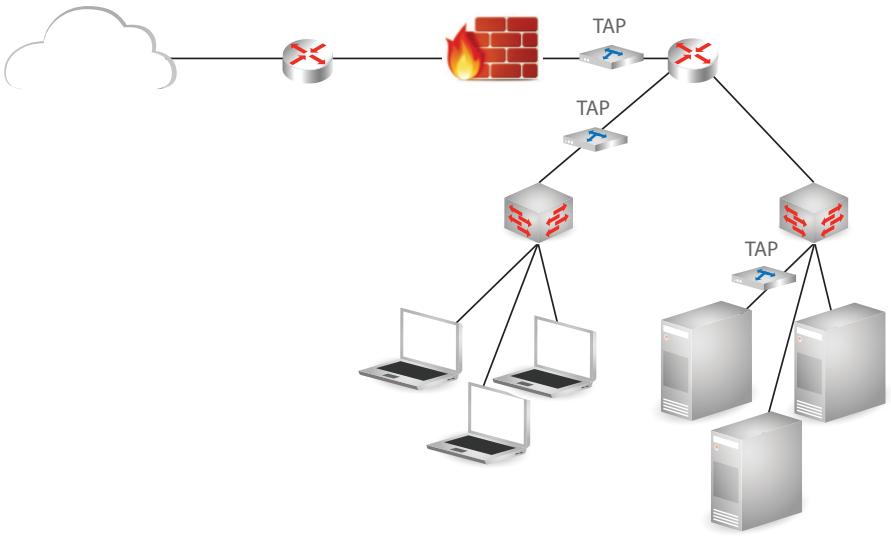
Who Needs TAPs

- Companies who require 24 x 7 monitoring capabilities (Intrusion Detection, VoIP Recording, etc)
- Service organizations who may need to "plug in" to conduct troubleshooting in support of an SLA agreement, avoiding SPAN or Port Mirror configuration of a switch or router which may be tied to a configuration change policy at the customer location.
- Compliance Requirements where all data needs to be captured and analyzed -- combination of tapping and SPAN/Port Mirrors.
- Companies looking to reduce operational expenses and mitigate risk

Where to place TAPs

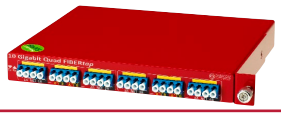
Placement of TAPs is typically in the locations with the most critical information in the network. TAPs will provide continuous monitoring on links where critical information travels, or on links leading to servers or storage devices where the data resides. TAPs are designed around a hardware-based architecture that minimizes latency, so their deployment can be made anywhere in the network.

Similar to security probes, some common locations for TAPs include inside the firewall, network trunks or links to or from critical servers.



DATACOM SYSTEMS INC

Network Taps from Datacom Systems

Product	Photograph	Media Type	Speed	Inline	Network (TAP) Ports*	Monitor Ports	Port Types**	Aggregation
10-100 AT		Copper	10/100		1	2	10/100 Network Tap (RJ45). 2 Monitoring 10/100 (RJ45).	N
CTP-1000		Copper	10/100/ 1000 Full Duplex		1	2	10/100/1000 Network Tap (RJ45). 2 Monitoring 10/100/1000 (RJ45).	Y
FTP 1000 Series		Fiber	40/10/1 Gb		1	2	MTP/MPO or LC or SC 50/50 or 70/30 split ratio 50 Micron and 9 Micron	N
FTP 2000 Series		Fiber	10/1 Gb		2	2	LC 50/50 or 70/30 split ratio 50 Micron and 9 Micron	N
FTP 4000 Series		Fiber	10/1 Gb		4	4	LC 50/50 or 70/30 split ratio 50 Micron and 9 Micron	N
FTP 8000 Series		Fiber	10/1 Gb		8	8	LC 50/50 or 70/30 split ratio 50 Micron and 9 Micron	N
FTP 9000 Series		Fiber	10/1 Gb		24	24	LC 50/50 or 70/30 split ratio 50 Micron and 9 Micron	N
SS1204BT-BT-S		Copper Input Copper Output	10/100/ 1000 Full Duplex		1	2	10/100/1000 Network Tap (RJ45). RJ45 Management. Serial (rear) DB9F	Y
SS1204BT-SFP-S		Copper Input. SFP Output	10/100/ 1000 Full Duplex		1	2	10/100/1000 Network Tap (RJ45). 2 Monitoring 10/100/1000 Any-to-Any. Management RJ45 at 100 Mbps Full Duplex. Serial (rear) DB9F	Y
SS1204SX-BT-S		Fiber Input. Copper output	1 Gb Full Duplex		1	2	SX Network Tap. 2 Any to Any Management Ports RJ45 at 100 100 Mbps Full Duplex	Y
SS2206BT-BT-S		Copper Input Copper Output	10/100/ 1000 Full Duplex		2	2	2 x 10/100/1000 Network Taps (RJ45). 2 Monitoring 10/100/1000 Any-to-Any. Management RJ45 at 100 Mbps Full Duplex. Serial (rear) DB9F	Y
SS2206SX-SFP		Fiber Input. SFP Output	1Gb Full Duplex		2	2	2X SX Network Taps. 2X SFP Any-to-Any Monitoring Ports. Management RJ45 at 100 Mbps Full Duplex.	Y
SS2210BT-BT/ SFP-S		Copper Input, SFP or Copper Output	10/100/ 1000 or 1 Gb Full Duplex		2	6	2 x 10/100/1000 Network Taps (RJ45). 4 RJ45 and 2 SFP Any-to-Any Monitoring Ports. Management RJ45 at 100 Mbps Full Duplex. Serial (rear) DB9F	Y
SS4210BT-SFP-S		Copper Input SFP Output	10/100/ 1000 or 1 Gb Full Duplex		4	2	4 x 10/100/1000 Network Taps (RJ45) and 2 SFP Any-to-Any Monitoring Ports.. Management port RJ45. Console port DB9.	Y

*Note: A Network (TAP) port shown on this page will tap one network link, 2 ports will tap 2 links, etc... Refer to product FASTstart guides for details on installation.
**Note: See datasheets for specific fiber, connector and split ratios available. Split ratios 50/50 and 70/30 are commonly used, other variations are available.