Network tap

A **network tap** is a hardware device which provides a way to access the data flowing across a computer network. In many cases, it is desirable for a third party to monitor the traffic between two points in the network. If the network between points A and B consists of a physical cable, a "network tap" may be the best way to accomplish this monitoring. The network tap has (at least) three ports: an **A** port, a **B** port, and a **monitor** port. A tap inserted between A and B passes all traffic through unimpeded, but also copies that same data to its monitor port, enabling a third party to listen.

Network taps are commonly used for network intrusion detection systems, VoIP recording, network probes, RMON probes, packet sniffers, and other monitoring and collection devices and software that require access to a network segment. Taps are used in security applications because they are non-obtrusive, are not detectable on the network (having no physical or logical address), can deal with full-duplex and non-shared networks, and will usually *pass through* traffic even if the tap stops working or loses power.

1 Terminology

The term **network tap** is analogous to phone tap or vampire tap. Some vendors have phrases for which **tap** is an acronym; however, those are most likely bacronyms.

The monitored traffic is sometimes referred to as the *pass-through* traffic, while the ports that are used for monitoring are the *monitor* ports. There may also be an aggregation port for full-duplex traffic, wherein the "A" traffic is aggregated with the "B" traffic, resulting in one stream of data /packets for monitoring the full-duplex communication. The packets must be aligned into a single stream using a time-of-arrival algorithm.

Vendors will tend to use terms in their marketing such as *breakout*, *passive*, *aggregating*, *regeneration*, *inline power*, and others. Common meanings will be discussed later. Unfortunately, vendors do not use such terms consistently. Before buying any product it is important to understand the available features, and check with vendors or read the product literature closely to figure out how marketing terms correspond to reality. All of the "vendor terms" are common within the industry and have real definitions and are valuable points of consideration when buying a tap device.

A distributed tap is a set of network taps which report to a centralized monitoring system or packet analyzer.

1.1 New filterable tap technology

A new type of tap, or network access point, is available. This new type of tap is called a "filterable" tap. It is especially valuable in the 10 Gigabit environment because 10-Gigabit test equipment is very expensive. Some taps, like those from several vendors, offer the ability to utilize less expensive and more widely available 1-Gigabit monitoring and analysis tools with these 10 Gigabit networks. When used in this fashion, some form of load-balancing or port-bonding is recommended to avoid packet loss to the monitoring tools.

A filterable tap, that provides advanced filtering, can selectively pass data, based on application, VLAN ID, or other parameters, to the 1-Gigabit port for deep analysis and monitoring, including IDS requirements.

Filtered access is also the best way to focus on business-critical traffic, or other specific areas of your network. At higher speeds, network traffic analysis cannot be performed using the older "capture and decode everything" philosophy. In this type of environment, focused access is the best way to enable traffic analysis, and often is the only way.

Any filterable tap you consider must have a simple user interface for easy setup and management. Furthermore, it must be able to collect the Layer 1 and Layer 2 data, while still allowing for auto saving, and easy access to data by graphing programs. Such a tap can be part of a strategy to monitor for essential metrics, such as frame errors and corrupted frames in IPv6.

2 Advantages and features

Older network technologies tended to be *shared*. Connecting a monitoring device to a *shared* network segment (i.e., piece of a network) was very easy—just connect the monitoring device as you would any other host, and enable promiscuous mode. Modern network technologies tend to be switched, meaning that devices are connected using point-to-point links. If a monitoring device is connected to such a network, it will only see its own traffic. The network tap allows the monitoring device to view the contents of a point-to-point link.

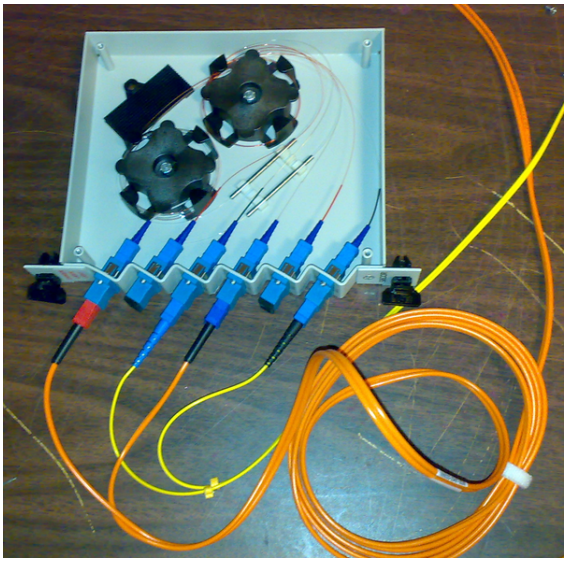
Modern network technologies are often full-duplex,

meaning that data can travel in both directions at the same time. If a network link allows 100 Mbit/s of data to flow in each direction at the same time, this means that the network really allows 200 Mbit/s of aggregate throughput. This can present a problem for monitoring technologies if they have only one monitor port. Therefore, network taps for full-duplex technologies usually have two monitor ports, one for each half of the connection. The listener must use channel bonding or link aggregation to merge the two connections into one aggregate interface to see both halves of the traffic. Other monitoring technologies do not deal well with the full-duplex problem.

Once a network tap is in place, the network can be monitored without interfering with the network itself. Other network monitoring solutions require in-band changes to network devices, which means that monitoring can impact the devices being monitored.

Once a tap is in place, a monitoring device can be connected to it as-needed without impacting the monitored network.

Some taps have multiple output ports, or multiple pairs of output ports for full-duplex, to allow more than one device to monitor the network at the tap point. These are often called *regeneration* taps.



A passive fiber optic tap.

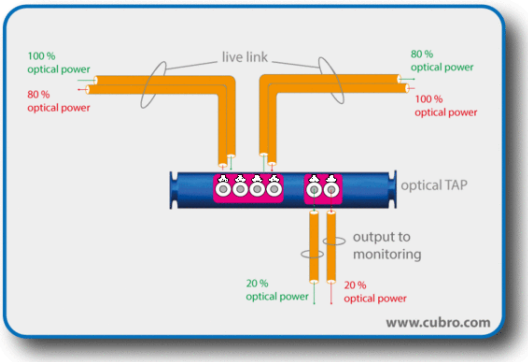
Some taps, particularly fiber taps, can use no power and no electronics at all for the *pass-through* and *monitor* portion of the network traffic. This means that the tap should never suffer any kind of electronics failure or power failure that results in a loss of network connectivity. One way this can work, for fiber-based network technologies, is that the tap divides the incoming light using a simple physical apparatus into two outputs, one for the *pass-through*, one for the *monitor*. This can be called a *passive* tap. Other taps use no power or electronics for the *pass-through*, but do use power and electronics for the *monitor* port. These can also be referred to as *passive*. Fiber taps are of limited use in some situations. For example, non-orthogonal photon fiber networks can not be tapped at all.[1]

Some taps operate at the physical layer of the OSI model rather than the data link layer. For example, they work with multi-mode fiber rather than 1000BASE-SX. This means that they can work with most data link network technologies that use that physical media, such as ATM and some forms of Ethernet. Network taps that act as simple optical splitters, sometimes called *passive taps* (although that term is not used consistently) can have this property.

Some network taps offer both duplication of network traffic for monitoring devices and SNMP services. Most major network tap manufacturers offer taps with remote management through Telnet, HTTP, or SNMP interfaces. Such network tap hybrids can be helpful to network managers who wish to view baseline performance statistics without diverting existing tools. Alternatively, SNMP alarms generated by managed taps can alert network managers to link conditions that merit examination by analyzers to intrusion detection systems.

Some taps get some of their power (i.e., for the *pass-through*) or all of their power (i.e., for both *pass-through* and *monitor*) from the network itself. These can be referred to as having *inline power*.

Some taps can also reproduce low-level network errors, such as short frames, bad CRC or corrupted data.



Funktion princip of an optical network tap

3 Disadvantages and problems

Because network taps require additional hardware, they are not as cheap as technologies that use capabilities that are built into the network. However, network taps are easier to manage and normally provide more data than some network devices.

Network taps can require channel bonding on monitoring devices to get around the problem with full-duplex discussed above. Vendors usually refer to this as aggregation

as well.

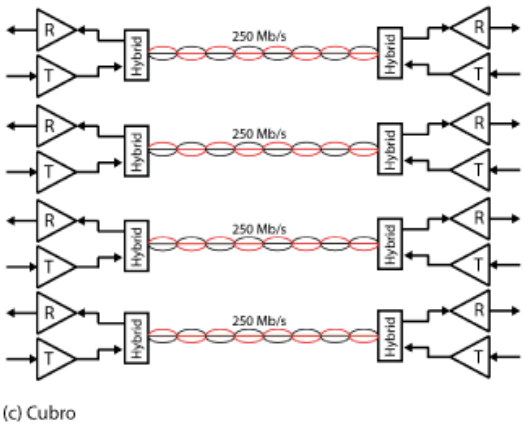
Putting a network tap into place will disrupt the network being monitored for a short time.[2] Even so, a short disruption is preferable to taking a network down multiple times to deploy a monitoring tool. Establishing good guidelines for the placement of network taps is recommended.

Monitoring large networks using network taps can require a lot of monitoring devices. High-end networking devices often allow ports to be enabled as mirror ports which is a software network tap. While any free port can be configured as a mirror port, software taps require configuration and place load on the network devices.

Even fully *passive* network taps introduce new points of failure into the network. There are several ways that taps can cause problems, and this should be considered when creating a tap architecture. Consider non-powered taps for optical-only environments or *throwing star network tap* for copper 100BT. This allows you to modify the intelligent aggregation taps that may be in use and avoids any complications when upgrading from 100 megabit to gigabit to 10 gigabit. Redundant power supplies are highly recommended.

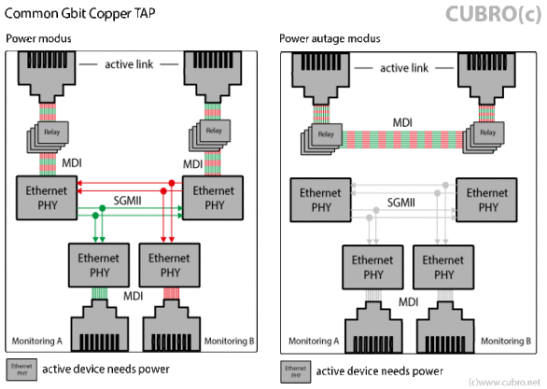
Fully *passive* is only possible on optical connections any bandwidth and on copper connections from type G703 (2Mbit) and Ethernet Base-T 10/100 Mbit. On Gigabit and 10 Gbit Base-T connections passive tapping is currently not possible.

4 Gigabit Base-T issues



Explains the physical connection on Gbit Ethernet

To transport 1 Gbit of traffic full duplex (1 Gbit in each direction simultaneously) a very complex signal is used to reach the desired performance and quality. In case of Gbit Ethernet the signal is called PAM 5 modulation, meaning that each cable pair transports 5 bits simultaneously in both directions. The PHY chips at each end of the cable have a very complex task at hand, because they must separate the two signals from each other. This is only possible because they know their own signal, so they can deduct their own send signals from the mixed signals on the line and then interpret the information sent by their link partners.



Schematic function of a Gbit Copper TAP

To tap a copper link as shown in the picture above it is not possible to just tap the middle of the wire because all you will see is a complex modulation of two signals. The only way to terminate the signal (as shown in the picture) is to use a PHY chip to separate the signal and then send the signal on to the link partner. This solution is working but causes some other problems.

1.) It is not passive any longer, so in the case of a failure the link can go down and the services on the link are interrupted. To minimize this problem each copper tap has a bypass switch (relays), which closes in a power down situation (as shown in the picture), to bring the link back up. Also this solution will not prevent that the link is down for a minimum of three seconds. These three seconds are a result of the autonegotiation behavior. This can not be changed because it is a vital function of the IEEE 802.3 standard as described in clause 28 and 40. Even this short interruption time could cause big problems in a network.

- a.) In some cases these links cannot be re-established without shutting down the services.
- b.) Rerouting functions in the network may take place
- c.) Streaming applications can collapse and cause more issues.

2.) Some layer 1 information is not transported over a copper tap (e.g. pause frames)

3.) The clock synchronization is affected. Sync-E over a standard Gbit copper tap is impossible and IEEE 1588 is affected, because of the additional delay a copper tap produces.

5 Comparison to other monitoring technologies

Various monitoring approaches can be used, depending on the network technology and the monitoring objective:

The simplest type of monitoring is logging in to an interesting device and running programs or commands that show performance statistics and other data. This is the cheapest way to monitor a network, and is highly appropriate for small networks. However, it does not scale well to large networks. It can also impact the network being monitored; see observer effect.

Another way to monitor devices is to use a remote management protocol such as SNMP to ask devices about their performance. This scales well, but is not necessarily appropriate for all types of monitoring. The inherent problems with SNMP are the polling effect. Many vendors have alleviated this by using intelligent polling schedulers, but this may still affect the performance of the device being monitored. It also opens up a host of potential security problems.

Another method to monitor networks is by enable promiscuous mode on the monitoring host, and connecting it to a shared segment. This works well with older LAN technologies such as 10BASE-T Ethernet, FDDI, and token ring. On such networks, any host can automatically see what all other hosts were doing by enabling promiscuous mode. However, modern switched network technologies such as those used on modern Ethernets provide, in effect, point-to-point links between pairs of devices, so it is hard for other devices to see traffic.

Another method to monitor networks is to use port mirroring (called "SPAN", for Switched Port Analyzer, by Cisco, and given other names by some other vendors) on routers and switches. This is a low-cost alternative to network taps, and solves many of the same problems. However, not all routers and switches support port mirroring and, on those that do, using port mirroring can affect the performance of the router or switch. These technologies may also be subject to the problem with full-duplex described elsewhere in this article, and there are often limits for the router or switch on how many pass-through sessions can be monitored, or how many monitor ports (generally two) can monitor a given session.

Countermeasures for network taps include encryption and alarm systems. Encryption can make the stolen data unintelligible to the thief. However, encryption can be an expensive solution, and there are also concerns about network bandwidth when it is used.

Another counter-measure is to deploy a fiber-optic sensor into the existing raceway, conduit or armored cable. In this scenario, anyone attempting to physically access the data (copper or fiber infrastructure) is detected by the alarm system. A small number of alarm systems manufacturers provide a simple way to monitor the optical fiber for physical intrusion disturbances. There is also a proven solution that utilizes existing dark (unused) fiber in a multi-strand cable for the purpose of creating an alarm system.

In the alarmed cable scenario, the sensing mechanism uses optical interferometry in which modally dispersive coherent light traveling through the multi-mode fiber mixes at the fiber's terminus, resulting in a characteristic pattern of light and dark splotches called speckle. The laser speckle is stable as long as the fiber remains immobile, but flickers when the fiber is vibrated. A fiber-optic sensor works by measuring the time dependence of this speckle pattern and applying digital signal processing to the Fast Fourier Transform (FFT) of the temporal data.

The U.S. government has been concerned about the tapping threat for many years, and it also has a concern about other forms of intentional or accidental physical intrusion. In the context of classified information Department of Defense (DOD) networks, Protected Distribution Systems (PDS) is a set of military instructions and guidelines for network physical protection. PDS is defined a system of carriers (raceways, conduits, ducts, etc.) that are used to distribute Military and National Security Information (NSI) between two or more controlled areas or from a controlled area through an area of lesser classification (i.e., outside the SCIF or other similar area). National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 7003, Protective Distribution Systems (PDS), provides guidance for the protection of SIPRNET wire line and optical fiber PDS to transmit unencrypted classified National Security Information (NSI).

6 See also

- Virtual TAP device

7 References

[1] Practical quantum key distribution over a 48-km optical fiber network Richard J. Hughes, George L. Morgan and C. Glen Peterson Physics Division Los Alamos National Laboratory, pdf

[2] "Sniffing Tutorial part 1 - Intercepting Network Traffic". NETRESEC Network Security Blog. 2011.

Make-a-Passive-Network-Tap

8 Text and image sources, contributors, and licenses

8.1 Text

- **Network tap** *Source:* https://en.wikipedia.org/wiki/Network_tap?oldid=685175456 *Contributors:* Charles Matthews, Itai, Kkron, Dupuy, PaulHanson, Guy Harris, Kelly Martin, Woohookitty, Krille, Btyner, Wavelength, Gaius Cornelius, Bovineone, Extraordinary, Kf4bdy, SmackBot, Mauls, Morty abzug, Jerome Charles Potts, Frap, DéRahier, JonHarder, Adamantios, Mcescher43, Willhb, Cydebot, Beta16, AndreasWittenstein, Barek, Malwiki, Nancyquill, Jim.henderson, Brothejr, Mariolina, AlastairIrvine, Tburket, Wikiisawesome, Spearsall, AlleborgoBot, Gsteidl, Editore99, N-lane, LaosLos, DumZiBoT, Fierrot, Ariconte, Addbot, MrOllie, Tassedethe, Legobot II, Oldcommguy, AnomieBOT, Materialscientist, Analphabot, TheLakeman, MarkmacVSS, MaximusMeridius00, AManWithNoPlan, Ssbat3, Helpsome, Helpful Pixie Bot, Ducatimonster, BattyBot, Andy huckridge, Faithchew, Tcardo2, Chrisliom and Anonymous: 57

8.2 Images

- **File:Base-T-Gbit-Physics.gif** *Source:* https://upload.wikimedia.org/wikipedia/commons/a/ad/Base-T-Gbit-Physics.gif *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* Chrisliom
- **File:Fiber_optic_tap.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/fc/Fiber_optic_tap.png *License:* GFDL *Contributors:* Own work *Original artist:* Roens
- **File:Gbit-Tap-schema.gif** *Source:* https://upload.wikimedia.org/wikipedia/commons/a/ac/Gbit-Tap-schema.gif *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* Cubro
- **File:Optical-tap-schema-wiki.gif** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/90/Optical-tap-schema-wiki.gif *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* Chrisliom
- **File:Question_book-new.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/9/99/Question_book-new.svg *License:* Cc-by-sa-3.0 *Contributors:*
  Created from scratch in Adobe Illustrator. Based on Image:Question book.png created by User:Equazcion *Original artist:* Tkgd2007

8.3 Content license

- Creative Commons Attribution-Share Alike 3.0