(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 March 2006 (23.03.2006)

PCT

(10) International Publication Number
WO 2006/031486 A2

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/US2005/031586

(22) International Filing Date:
2 September 2005 (02.09.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/607,154 3 September 2004 (03.09.2004) US

(71) Applicant *(for all designated States except US)*: **THE REGENTS OF THE UNIVERSITY OF CALIFORNIA** [US/US]; 1111 Franklin Street, 12th Floor, Oakland, CA 94607 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **BENNETT, Michael J.** [US/US]; 1275 Wildwing Lane, Vallejo, CA 94591 (US). **BELL, Gregory R.** [US/US]; 1346 Gilman Street, Berkeley, CA 94706 (US).

(74) Agent: **KUSHA, Babak**; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, CA 94111, (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

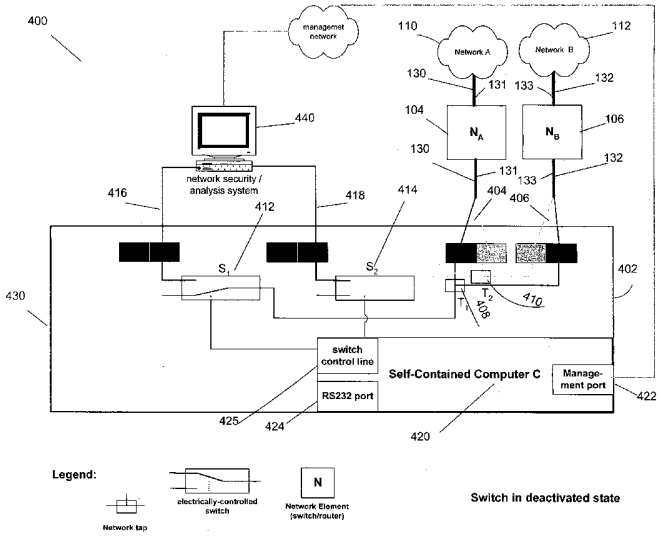
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** A SYSTEM FOR SECURE ACCESS TO, AND ACTIVATION OF, A NETWORK TAP



(57) **Abstract:** An apparatus and method for securely tapping a computer network is disclosed. The secure network tap permits remote activation and deactivation of its tapping functionality, encryption of the control channel, and production of encrypted log files containing records of access to the underlying data stream. Depending on the embodiment, the secure network tap may also provide fail-safe behavior in response to local link-state changes, and it may include functionality for capturing, archiving and encrypting the tapped traffic.

WO 2006/031486 A2

A SYSTEM FOR SECURE ACCESS TO, AND ACTIVATION OF, A NETWORK TAP

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application No. 60/607,154 filed September 3, 2004, the disclosure of which is hereby incorporated by reference herein in its entirety for all purposes.

STATEMENT AS TO RIGHTS TO INVENTIONS MADE UNDER FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

[0002] This invention was made with U.S. Government support under Contract Number DE-AC02-05CH11231 between the U.S. Department of Energy and The Regents of the University of California for the management and operation of the Lawrence Berkeley National Laboratory. The U.S. Government has certain rights in this invention.

BACKGROUND OF THE INVENTION

[0003] The present invention relates to a network tap, and more particularly to devices and methods that securely access and selectively activate a switchable network tap.

[0004] Network taps are used to monitor the data traversing a particular network medium, such as an optical fiber, a coaxial cable, or an unshielded twisted-pair copper cable. In many ways, network taps are analogous to wire taps in the world of analog telephony. Network taps are used for a variety of purposes, including intrusion detection, traffic accounting, traffic analysis, and troubleshooting.

[0005] Various techniques for tapping data networks are known, and several vendors provide commercially available taps based on these known techniques. At a high level of abstraction, these known techniques are similar in the sense that they permit a network monitoring system to passively receive a copy of the data traversing a network link, without injecting information into, or otherwise perturbing, the data flow itself.

[0006] Fig. 1 is a logical diagram 100 of a unidirectional network tap 102. Data originating from network element N_A 104 and destined for network element N_B 106 traverses the network medium. Network element N_A 104 (or network element N_B 106) is for example a switch, a router, a firewall, a server or other such element coupled with Network A 110 (or Network B 112). Tap T_1 120 splits or copies the stream of information so that two or more network elements (here, N_B 106 and monitoring system M 108) receive the identical data stream. Regardless of the technique for accomplishing such splitting or copying, the integrity of the data stream is maintained; that is no person or device making use of the tap 102 can transmit information into either path. In optical networks, fiber-optic splitters divide an incoming light stream into two or more output streams, according to a specified split ratio. In copper-based Ethernet networks, it is normally necessary to regenerate the incoming signals for all monitoring interfaces, and to assure that network traffic flow is uninterrupted in the event of a loss of power to the tap. (*e.g., see* A. Fischer, "Network Taps Enable Passive Monitoring," *Network World Fusion* (10/28/02)). Network element M 108 may perform a wide range of functions, including intrusion detection, traffic accounting, traffic analysis, and troubleshooting. Network element N_A 104 communicates using a bidirectional link 130, 131 with Network A 110. Likewise, network element N_B 106 communicates using a bidirectional link 132, 133 with Network B 112. Bidirectional links 130,131 and 132,133 are split at the interface 140 (serving N_A) and 141 (serving N_B) to enable individual unidirectional communication links 160, 150 between Network A 110 and Network B, 112. It should be noted that communication link 150 includes a transmit link (darker shaded box) and a receive link (lighter shaded box), and, likewise, communication link 160 includes a transmit link (lighter shaded box) and a receive link (darker shaded box) such that, for example, T_1 taps data flow between the transmit link of 160 (from N_A) and the receive link of 150 (to N_B).

[0007] Because most modern data communication systems rely on bidirectional communication, network taps are normally packaged and sold in pairs. What is commonly called a network tap is a pair of unidirectional taps which jointly permit the monitoring of a single bidirectional communication circuit. Fig. 2 is a logical diagram 200 of a bidirectional network tap 202, and it demonstrates that a bidirectional tap includes a pair of unidirectional taps. Tap T_1 120 is used to tap data from Network A 110 to Network B 112, and Tap T_2 122 is used to tap data from Network B 112 to Network A 110.

[0008] Currently-available network taps have a number of limitations and liabilities. One limitation is that they do not permit an operator (or remote system) to enable or disable the tapping functionality. In other words, current taps are always on. Once integrated into the network infrastructure, they are designed to pass copies of network data to monitoring interfaces at all times.

[0009] Unfortunately, such a design is undesirable in many situations. In a typical business environment, for example, a conventional tap may permit unauthorized access to sensitive data. Fig. 3 shows a simplified diagram 300 of a medium-sized enterprise network. In Fig. 3, conventional taps T_1 302 and T_2 304 are installed for debugging purposes. Because such taps do not incorporate security controls, it is relatively easy for unauthorized personnel with physical access to the room containing the taps, or with login access to the monitoring system, to capture all traffic traversing either link. In the process, such personnel may be able to intercept sensitive or proprietary information including medical records, electronic mail, passwords, and corporate documents. In addition, conventional taps are increasingly likely to provide access to private telephone conversations, and given the growing popularity of Voice Over IP (VOIP) technology, leading to potentially more adverse consequences. There is, therefore, a need for a network tap that does not suffer from the above shortcomings.

BRIEF SUMMARY OF THE INVENTION

[0010] The present invention is directed towards secure network taps. The secure network taps in accordance with the embodiments of the present invention include a self-contained computer system, as well as functionality for enabling and disabling the tapped output; for remote management; for authentication, authorization, and accounting; for optional fail-safe behavior in the event of link-state change; and for encryption of records related to access history. In addition, in one embodiment, the secured network tap includes functionality for capturing and archiving some or all of the tapped traffic, either with or without external monitoring access. In the latter case, the secure tap can be a black box that collects network data without diverting it through external interfaces to a monitoring system.

[0011] The secure network taps in accordance with the embodiments of the present invention are designed for environments in which access to the data traversing the

network medium needs to be carefully restricted, either because the underlying information is sensitive, or as the result of legal or business requirements, such as, for example, for compliance with the requirements of The Health Insurance Portability and Accountability Act of 1996 (HIPAA). The need for the secure network tap of the present invention is likely to grow substantially as network intrusion detection systems become more common, as privacy regulations become more complex and restrictive, and as Voice over IP technology becomes more popular.

[0012] The embodiments of the present invention provide devices and methods for securely tapping a computer network. The secure network tap permits remote activation and deactivation of its tapping functionality, encryption of the control channel, and production of encrypted log files containing records of access to the underlying data stream. Depending on the specific embodiments, the secure network tap can also provide fail-safe behavior in response to local link-state changes, and it can include functionality for capturing, archiving and encrypting all tapped traffic.

[0013] For a further understanding of the nature and advantages of the invention, reference should be made to the following description taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] Fig. 1 is a logical diagram of a known unidirectional network tap.

[0015] Fig. 2 is a logical diagram of a known bidirectional (*i.e.*, full-duplex) network tap.

[0016] Fig. 3 is a logical diagram of simple corporate network shown with conventional network taps.

[0017] Fig. 4 is an exemplary diagram of a secure network tap in accordance with one embodiment of the present invention, showing the logical relationship between the components, with the switches in their deactivated state.

[0018] Fig. 5 is an exemplary diagram of the secure network tap of Fig. 4, showing the physical relationship between the components, with the switches in their deactivated state.

[0019] Fig. 6 is an exemplary diagram of the secure network tap of Fig. 4, showing the physical relationship between components, with switches in their activated state.

[0020] Fig. 7 is a logical diagram of secure network tap, showing the link-state detection functionality.

[0021] Fig. 8 is an exemplary logical diagram of a secure network tap in accordance with a second embodiment of the present invention showing an on-board data-capture mechanism.

DETAILED DESCRIPTION OF THE INVENTION

[0022] As described below, the secure network tap in accordance with the embodiments of the present invention may be implemented with several optional features. Fig. 4 shows an exemplary diagram 400 of a secure network tap 402 in accordance with one embodiment of the present invention, showing the logical relationship between the components. In the embodiment shown in Fig. 4, the secure network tap 402 includes the following elements, namely: two network interfaces 404, 406 for connection to a network segment to be monitored; two unidirectional network taps 408, 410; two electrically-controlled switches 412, 414 for activating and deactivating the tapping function; two network interfaces 416, 418 through which tapped data may pass to an external monitoring system; a self-contained computer system 420; software which manages secure access, authentication, authorization, accounting, logging, and policy configuration; a network interface which permits remote connections 422; an optional local communication interface (e.g., a serial, a parallel or a USB interface) which permits local connections 424; and a tamper-evident sealed enclosure 430. Such an enclosure is an enclosure coated with or marked with a tamper-evident tape, label, decal or so on.

[0023] FIG. 4 shows an illustration of the logical relationship between the above components, with the switches in their deactivated state. The secure network tap 402 is placed on a network segment, in series with network elements N_A 104 and N_B, 106 which may be routers, switches, servers, firewalls, or other devices. Because the secure network tap

402 interrupts the segment joining these two network elements, it has access to data streams in both directions ($N_A \rightarrow N_B$, $N_B \rightarrow N_A$). Unidirectional tap T_1 408 splits or copies (*i.e.*, depending on the underlying network medium and the tapping technology used) traffic in the $N_B \rightarrow N_A$ direction, while unidirectional tap T_2 410 splits or copies traffic in the $N_A \rightarrow N_B$ direction. Electronically-controlled switches S_1, 412 and S_2, 414 permit the output of T_1 408 and T_2 410 (respectively) to be presented to external interfaces 416, 418, where a monitoring system 440 may be connected. In this embodiment, switches S_1, 412 and S_2, 414 are open by default; in other words, tapped traffic is not available to the external monitoring system 440 until a remote user or system has authenticated and activated the tapping function.

[0024] As is shown in Fig. 4, an integral feature of the secure network tap is the inclusion of a self-contained computer system C, 420, which has various subcomponents characteristic of a single board computer ("SBC"). These subcomponents may include, but are not limited to, one or more CPUs, volatile and non-volatile memory, disk drives, and input/output interfaces 422, 424, for example, for Ethernet, USB, serial , or parallel communication.

[0025] Self-contained computer system C, 420, permits an operator or a remote system to access the secure network tap through an input/output interface 422 (for example, an Ethernet port), to authenticate against a local or remote database, and to issue commands. Preferably, such access is conducted using an encrypted protocol such as SSH, SSL, or IPsec. The set of commands available to the operator or remote system varies depending on the embodiment, with all embodiments supporting the ability to control switches S_1 412 and S_2 414; that is, to permit network traffic captured by unidirectional taps T_1 408 and T_2 410 to be available at external interfaces 416, 418.

[0026] Fig. 5 is an exemplary diagram 500 showing the physical (in contrast to the logical) relationship between the components of Fig. 4. For purposes of illustration, the network medium being monitored in Fig. 5 can be a 1000BaseSX Ethernet, as specified by the IEEE standard 802.3z. Because a 1000BaseSX Ethernet runs over multimode fiber-optic cable, many components in this embodiment are optical components. The secure network tap 402 is placed in series with network elements N_A 104 and N_B 106, which may be routers, switches, servers, firewalls, or other devices. By virtue of this topology, the secure network tap 402 has access to data streams in both directions ($N_A \rightarrow N_B$, $N_B \rightarrow N_A$). Unidirectional taps T_1 408 and T_2 410 contain fiber-optic splitters. Each splitter divides one

of the incoming light streams and passes a portion of light to the downstream network element, and another portion of light to fiber-optic switch S_1 412 and S_2 414. Switches S_1 412 and S_2 414 permit the output of T_1 408 and T_2 410 to be available to external interfaces 416, 418, where a monitoring system 440 may be connected.

[0027] Switches S_1 412 and S_2 414 are open by default, in this embodiment. In other words, they pass no light to the external interfaces 416, 418. Self-contained computer system C, 420 has the ability to control the state of fiber-optic switches S_1 412 and S_2 414, and therefore to permit or interrupt the flow of data to the monitoring system 440 (which is external to the secure network tap, in this embodiment). Electrically-controlled fiber-optic switches are available from several vendors and may be implemented using a variety of underlying technologies, including Micro Electro-Mechanical Systems ("MEMS"). However, the technical implementation of switches S_1 412 and S_2 414 is not critical to their functional role within this embodiment of the secure network tap.

[0028] The nature of the link between computer system C, 420, and switches S_1 412 and S_2 414 depends on the implementation of S_1 412 and S_2 414, as well as the input/output (I/O) interfaces available on computer C, 420. For example, if S_1 412, S_2 414, and C, 420, all support RS232, the connection may be direct. If not, a signal converter 426 can be used. In Fig. 5, a two-channel RS232 to 5V TTL converter is used to connect computer system C, 420, to switches S_1 412 and S_2 414.

[0029] Computer system C, 420, is configured so that human operators or external systems can connect to it using a secure protocol, authenticate against a user database, which can be locally-stored, and issue commands or alter the configuration of the secure network tap. Preferably, access to computer system C, 420, should be conducted using an encrypted protocol such as SSH, SSL, or IPsec. In the embodiment shown in Figs. 4-5, human operators connect to computer C, 420, from a remote system by means of the SSH protocol and pre-shared keys.

[0030] After connecting and authenticating, a human operator can issue commands or change the configuration of the secure network tap. If the operator issues the command to activate the device's tapping function, for example, computer system C, 420, communicates with fiber-optic switches S_1 412 and S_2 414 in order to close them, so that light from optical taps T_1 408 and T_2 410 flows to the external monitoring interfaces 416,

418. The external monitoring system 440 can capture and analyze traffic flowing bidirectionally between network elements N_A 104 and N_B 106. Fig. 6 shows a diagram 600 illustrating the physical relationship between the components of the secure network tap when the tapping function is activated or engaged.

[0031] The computer system C, 420, stores software in memory and/or a hard drive and/or other storage medium and executes software routine(s) that are configured to manage tasks related to: remote access, including authentication, authorization and accounting; activation and deactivation of the tapping function; and the encryption and storage of all records related to the first two functions. In certain embodiments, computer system C, 420 has additional functions, which are discussed below. It should be noted that the encryption and storage of records can be used, because records pertaining to the access history and activation state of the secure network tap may be subject to digital chain-of-custody requirements (*e.g.*, *see* Chet Hosmer, "Proving the Integrity of Digital Evidence with Time," *International Journal of Digital Evidence,* Spring 2002, Volume 1, Issue 1).

[0032] In the embodiment shown in Figs. 4-6, the method for encrypting and storing records is a configurable option. For example, the user is permitted to choose among the following, namely, (a) the records are stored on a local, encrypted file system, accessible only by means of a private key which is not stored on the secure network tap itself, (b) the records are stored (and optionally, encrypted) on a removable file system, such as a flash card, accessible only by means of a private key, or (c) the records are stored on a remote file system (for example, over an NFS mount), and optionally encrypted during transmission and storage. Many other methods for encrypting and storing records can be envisioned by those skilled in the art.

ALTERNATIVE EMBODIMENTS

[0033] Although Figs. 5-6 illustrate an embodiment of the secure network tap designed for monitoring traffic on 1000BaseSX Ethernet links, this design can be adapted and extended for any networking standard that employs optical fiber, coaxial cable, or twisted-pair cable as a transmission medium, including varieties of non-wireless Ethernet, as well as Asynchronous Transfer Mode ("ATM") (*i.e.*, broadband switching and transmission technology), Frame Relay, Integrated Services Data Network ("ISDN"), Sonnet, and

Multiprotocol Label Switching ("MPLS"). To modify the network tap in accordance with the embodiments of the present invention, for use with other networking standards, the interfaces, taps, and switches require modifications. For example, for copper-based Ethernet, unidirectional taps T_1 and T_2 are replaced by Ethernet regenerators, which copy rather than split the incoming signal. It should also be noted that data may be replicated by means other than taps or regenerators. For instance, one embodiment of the secure network tap can utilize a switching fabric and port mirroring technology in order to copy incoming data to a monitoring interface. The alternative embodiments (*i.e.*, those tailored for specific layer-1 and layer-2 networking standards, and those integrating alternative means for copying or splitting incoming data) share the same basic functionality as the embodiments described above.

[0034] Moreover, an embodiment of the secure network tap suitable of the present invention can be constructed for use on a shared network medium such as IEEE 802.11a, 802.11b, or 802.11g (*i.e.*, wireless Ethernet). In such an embodiment, taps T_1 and T_2 are replaced by a single wireless network interface. Although a specialized device is normally not required for monitoring a wireless Ethernet, such an embodiment can be useful in at least two situations, namely when the wireless traffic is encrypted, and when Voice over IP (VOIP) is deployed wirelessly.

[0035] In addition to the alternative embodiments described above, the basic functionality of the secure network tap can be extended with various additional features, which may be incorporated (either singly or in combination) into any embodiment. These additional features include: link-state change detection; integrated data capture; integration and miniaturization of components; integration into other networking equipment; and an on-board matrix switch. Each of these features is described below in further detail.

Link-state change detection

[0036] Although the embodiments of the secure network tap as shown in Figs. 4-6 provide substantial security-related benefits when compared to an ordinary network tap, any unauthorized person with physical access might be able to alter the cabling which connects the secure network tap to the network being monitored, or to the associated monitoring system, or both. Such a person might then be able to intercept sensitive or proprietary information.

[0037] In order to defeat such attempts at tampering, the secure network tap may incorporate a link-state change detection functionality depicted by the link-state detector 702 shown in Fig. 7. This functionality permits the secure network tap to detect a link-state change on any of its network interfaces, whether those interfaces are used for pass-through, monitoring, or management. In such an embodiment, the on-board computer system 420 disables the tapping function as a fail-safe measure, when it detects any network link-state change. Both events (the detection of link-state change and the deactivation of tapping) are logged. The tapping function cannot be re-activated until an authorized person or system connects to the secure network tap, authenticates, and issues the appropriate command.

[0038] Fig. 7 is a logical diagram 700 of a secure network tap, with a link-state detector 702. When a cable attached to any interface (404, 406, 416, 418, or 422) is disconnected at either end, information about the link-state change is transmitted to computer system C, 420, which then deactivates the tapping function by opening switches S_1 412 and S_2 414.

[0039] The mechanism for assuring that link-state changes cause deactivation of the tapping function will vary according to the network medium being tapped. Several methods are described below, two for optical and one for copper-based Ethernet. However other methods for achieving the same functionality can be envisioned by those skilled in the art.

[0040] In the case of optical Ethernet such as 1000BaseSX, the following set of techniques may be employed: 1) Network interfaces can be contained and packaged inside the tamper-evident enclosure housing the secure network tap itself, with associated 2-strand fiber-optic patch cables protruding through small holes in the enclosure, each terminated by a pair of connectors. This design assures that physical disconnection can only occur at the remote end of each cable. 2) The fiber connectors on the remote end of each cable are modified so that it is impossible to remove or insert one fiber in the pair (*i.e.*, the transmit fiber) from the remote interface without simultaneously removing or inserting the other fiber in the pair (*i.e.*, the receive fiber). It should be noted that such a modification is unnecessary in the case of SFP connectors, which already incorporate the feature; but it is necessary in the case of SC and ST connectors. 3) The fiber-optic splitters should preferably be three-way splitters (in contrast to the two-way splitters T_1 and T_2 illustrated in Fig. 5), with the third light-path sent to a link-state detector. 4) Light from the receive fiber of interfaces serving

the monitoring system is also sent to the link-state detector. 5) The link-state detector sends an alert to the self-contained computer system in the event of any link-state change; or, alternatively, the link-state detector can interface directly with switches S_1 412 and S_2 414.

[0041] As an alternative to the measures described above, the link-state detection system can use specially-modified fiber-optic patch cables (or an assembly of such cables) to provide an electrical, optical or mechanical signal to the secure network tap in the event that any connector or connector element is disconnected from a network interface. This second method of state-change detection has the advantage of simplifying the design of the secure network tap.

[0042] In the case of copper-based Ethernet, the implementation of the link-state detection is different. In place of fiber optic splitters, Ethernet regenerators are used, which fulfill an analogous function. The regenerator(s) can directly detect link-state changes on the receive pair of monitoring and pass-through interfaces, using commercially available parts. Link-state change on the management interface is detected directly by the self-contained computer system.

[0043] Regardless of the method used to implement link-state change detection, the feature makes it substantially more difficult for an unauthorized person to tamper with the network cabling connected to the secure network tap without disabling the tapping function entirely.

On-board data capture for black box operation

[0044] In the embodiments of the secure network tap described above and shown in Figs. 4-7, the external interfaces 416, 418 are connected to a monitoring system for the purpose of intrusion detection, traffic accounting, traffic analysis, or troubleshooting.

[0045] In an alternative embodiment, the secure network tap can incorporate the functionality of this external monitoring system internally. This feature is implemented, by the self-contained computer system C, 420, which has the necessary components to implement the intrusion detection, traffic accounting, traffic analysis, or troubleshooting functions.

[0046] Fig. 8 illustrates a logical diagram 800 of the secure network tap with on-board data capture functionality. In this embodiment, tapped data flows from T_1 408 and

T_2 410 through switches 412, 414 to a pair of internal network interfaces 416A, 418A on computer system C, 420, when the tapping function is activated. Computer system C, 420, in this embodiment has the additional function of capturing, archiving and storing the tapped traffic; or optionally, a sub-set of all tapped traffic. The methods for capturing, archiving and storing tapped traffic on computer system C, 420, are numerous, and will depend on many factors, including the computer system's operating system. In one embodiment, computer C, 420, runs Linux, and the utility tcpdump is used to filter and capture the tapped data stream, which is saved on an encrypted file system. However, many other methods and techniques for accomplishing the same function can be envisioned by those skilled in the art.

[0047] It should be noted that the secure network tap depicted in Fig. 8 lacks external monitoring interfaces (though it retains an external management interface). In this black box embodiment, the way an operator or remote system examines the tapped data stream is by authenticating and connecting to computer system C, 420, first. As a result, computer system C, 420, maintains a record of access to the tapped data itself.

[0048] In some applications, however, it may be desirable for an embodiment of the secure network tap with on-board data collection to retain external monitoring interfaces. For example, the on-board computer system can be configured to capture one subset of tapped traffic, while an external monitoring system captured a different subset of tapped traffic.

Integration and miniaturization of components

[0049] While Figs. 4 through 8 show all taps (T_1 and T_2), switches (S_1 and S_2), and the computer system (C) as discrete components, it should be realized that these elements can be integrated and combined on a single printed circuit board, or a small number of integrated circuits, or a single integrated circuit.

Integration into other networking equipment

[0050] Although the secure network tap in accordance with the embodiments of the present invention has been described in terms of a stand-alone implementation, its functionality can be integrated into a larger, more complex network component such as a switch, router, access server, firewall, or intrusion detection system.

On-board matrix switch

[0051] The descriptions of the secure network tap in accordance with the embodiments of the present invention have been focused on the need to monitor network traffic on a single network link. In practice, however, it is likely that an organization may want to monitor traffic on a number of different links, and selectively switch among them, as necessary. For this purpose, a commercially available matrix switch can be integrated in the enclosure of the secure network tap. This matrix switch can permit a single link among multiple links to be selected for monitoring. Control and configuration of the integrated matrix switch can be among the features available to operators or remote systems that have logged into and authenticated on the secure network tap. Alternatively, multiple secure tap devices can be integrated into a matrix switch or other device. In this manner, in addition to, or in place of, integrating the secure tap together with other equipment, multiple secure taps can be ganged together and then can be integrating with other network devices.

[0052] As will be understood by those skilled in the art, the present invention may be embodied in other specific forms without departing from the essential characteristics thereof. For example, the secure network tap of the present invention can be adapted and extended for any networking standard that employs optical fiber, coaxial cable, or twisted-pair cable as a transmission medium, including all varieties of wireless and non-wireless Ethernet, as well as ATM, Frame Relay, ISDN, Sonnet, and MPLS. In addition, the tapped data can be passed to an external or internal monitoring system. Additionally, the novel aspects of the secure network tap in accordance with the embodiments of the present invention may be implemented individually or in combination with one another. These other embodiments are intended to be included within the scope of the present invention, which is set forth in the following claims.

WHAT IS CLAIMED IS:

1. A network tap for accessing data streams between a first and a second network element, comprising:

two network interfaces for connection to a network segment to be monitored between the first and the second network elements;

two unidirectional network taps to perform a tapping function, coupled with the two network interfaces, the first of the two unidirectional network taps tapping the data stream from the first network element to the second network element and the second of the two unidirectional taps tapping the data stream from the second network element to the first network element;

two electrically-controlled switches each coupled with each of the two unidirectional network taps, for selectively activating the tapping function of the data streams;

two monitoring system network interfaces each coupled with each of the two switches through which tapped data passes to a monitoring system;

a self-contained computer system coupled with the two electrically-controlled switches, the self-contained computer system configured for executing a computer program, the computer program having instructions for causing the self-contained computer system to

provide remote access, including authentication, authorization and accounting, to a monitoring system,

selectively activate the two electrically-controlled switches,

encrypt and store records related to the remote access and the selective activation of the two electrically-controlled switches;

a management port network interface coupled with the self-contained computer system, configured for remote connections; and

a tamper-evident enclosure for housing the two network interfaces, the two unidirectional network taps, the two electrically-controlled switches, the two monitoring

system network interfaces, the self-contained computer system, and the management port network interface.

2. The network tap of claim 1 further comprising a local communication interface coupled with the self-contained computer system, configured for local connections.

3. The network tap of claim 2 wherein the local communication interface comprises an interface selected from a group consisting of a serial port, a parallel port, and a USB port.

4. The network tap of claim 1 wherein the network elements are selected from the group consisting of routers, switches, servers, firewalls, and combinations thereof.

5 The network tap of claim 1 wherein the monitoring system is an external monitoring system.

6. The network tap of claim 1 wherein the monitoring system is an internal monitoring system.

7. The network tap of claim 6 wherein the internal monitoring system is a part of the self-contained computer system.

8. The network tap of claim 1 wherein the tapping function is configured to tap data streams from a network based on networking standards consisting of 1000BaseSX Ethernet links, any networking standard that employs optical fiber, coaxial cable, twisted-pair cable, wireless, non-wireless Ethernet, Asynchronous Transfer Mode, Frame Relay, Integrated Services Data Network, Sonnet, Multiprotocol Label Switching, and combinations thereof.

9. The network tap of claim 1 wherein the two electrically-controlled switches are fail-safe switches such that in the absence of a signal from the self-contained computer to selectively activate the tapping function of the data streams, the switches are deactivated and the tapped data streams is not passed to the monitoring system.

10. The network tap of claim 1 further comprising a link-state detector coupled with the self-contained computer system, the link-state detector configured to cause

the self-contained computer system to disable the tapping function, when the link-state detector detects a network link-state change.

11. The network tap of claim 10 wherein the link-state detector is configured to detect an electrical, an optical, a mechanical, or a combination thereof change in the link-state.

12. The network tap of claim 10 wherein the link-state detector is configured to detect a network link-state change when there is a change in the link-state of any one of: the two network interfaces, the two unidirectional network taps, the two electrically-controlled switches, the two monitoring system network interfaces, the management port network interface, the serial interface, or combinations thereof.

13. The network tap of claim 10 wherein the detection of a link-state change and a deactivation of the tapping function are logged by the self-contained computer system.

14. The network tap of claim 10 wherein the tapping function is not re-activated until an authorized person or system connects to the secure network tap, authenticates, and issues an appropriate command to re-activate the secure network tap.

15. The network tap of claim 1 further comprising an integrated data capture system, wherein the self-contained computer system is configured to perform functions for capturing, archiving and storing at least a portion of the tapped data stream.

16. The network tap of claim 15 wherein the self-contained computer system is configured to allow an operator or remote system to examine the tapped data stream in response to the operator or remote system connecting to and being authenticated with the self-contained computer system.

17. The network tap of claim 16 wherein the self-contained computer system is configured to maintain a record of access to the tapped data.

18. The network tap of claim 1 wherein the two unidirectional network taps, the two electrically-controlled switches, and the self-contained computer system are integrated into a system selected from the group consisting of a single printed circuit board, a small number of integrated circuits, a single integrated circuit, and combinations thereof.

19. The network tap of claim 1 being integrated with and further comprising a network component selected from the group consisting of a switch, a router, an access server, a firewall, an intrusion detection system, and combinations thereof.

20. The network tap of claim 1 further comprising a

a matrix switch integrated in the enclosure of the secure network tap, wherein the matrix switch can permit a single link among multiple links to be selected for monitoring, and wherein the control and configuration of the integrated matrix switch are among the features available to operators or remote systems who are logged into and authenticated on the secure network tap.

21. The network tap of claim 1 wherein two unidirectional network taps are replaced by a wireless network interface, wherein the wireless network interface is operationally coupled with the two network interfaces and the two electrically-controlled switches.

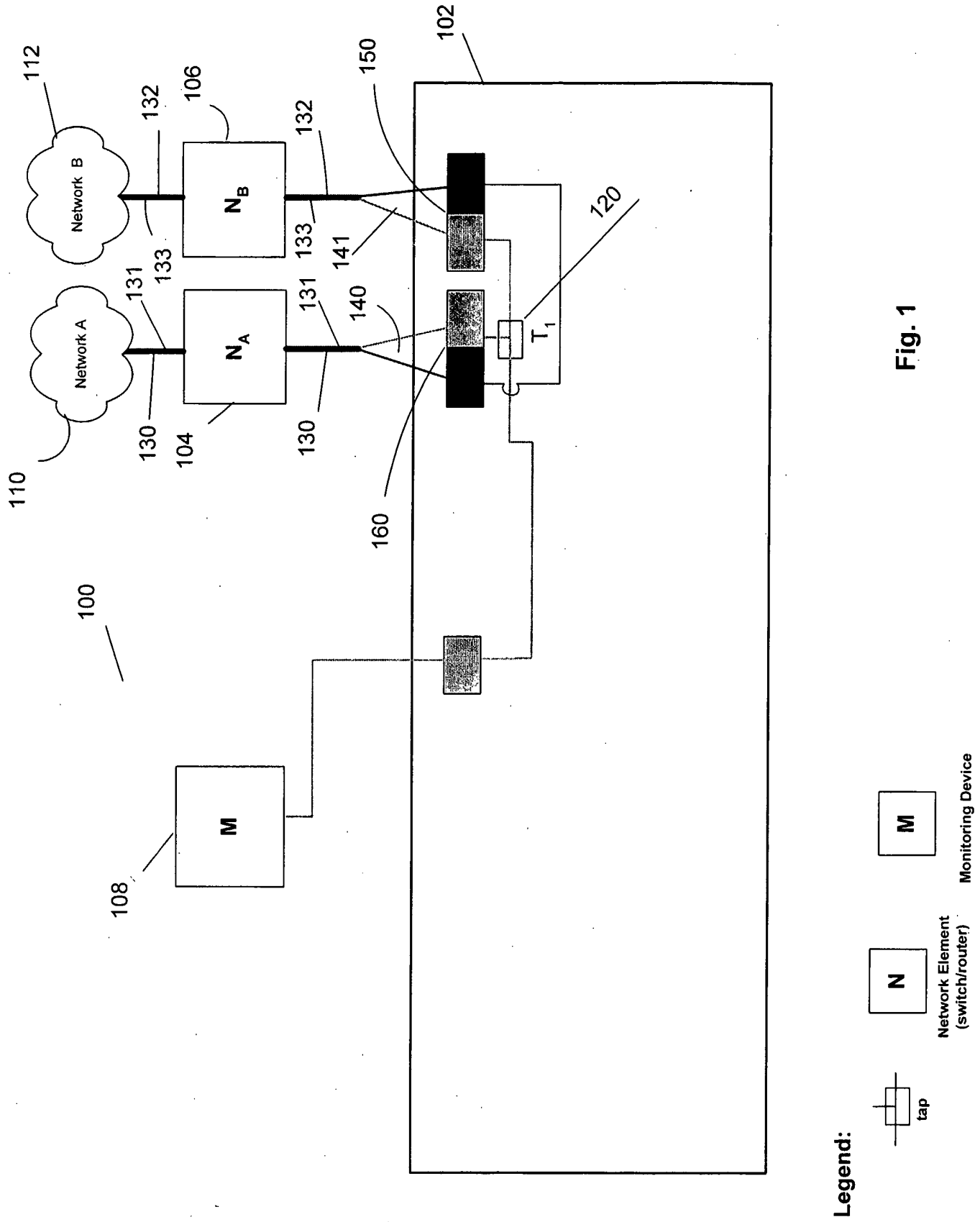

102
112
106
132
150
Network B
N_B
132
133
133
141
120
131
131
140
Network A
N_A
T_1
130
104
130
110
160
100
M
108
Legend:
tap
N
Network Element
(switch/router)
M
Monitoring Device

Fig. 1

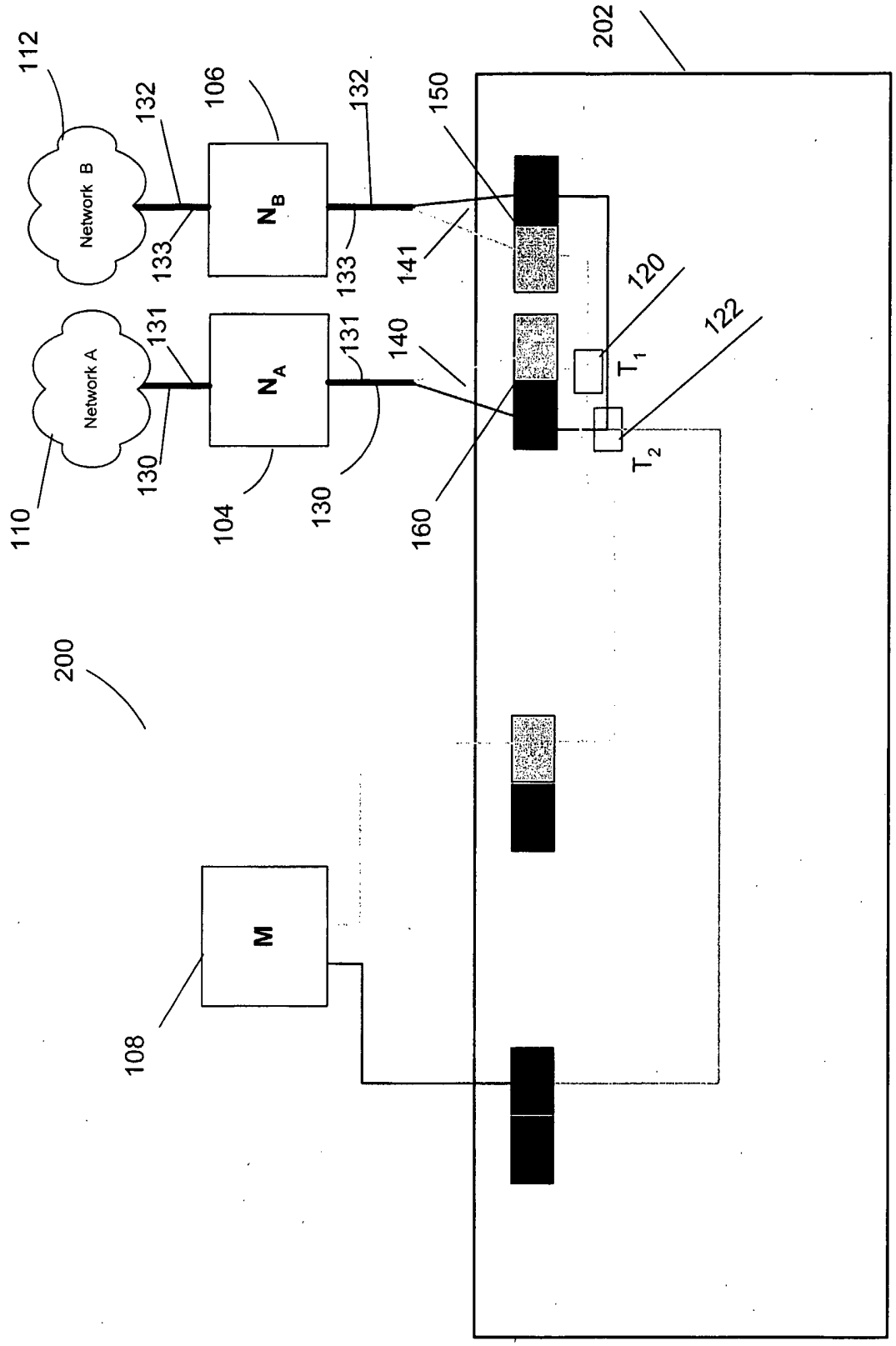

112
Network B
132
106
N_B
132
150
202
133
133
141
120
131
131
140
122
Network A
T_1
T_2
130
104
130
160
110
200
M
108
Legend:
tap
N
Network Element (switch/router)
M
Monitoring Device

Fig. 2

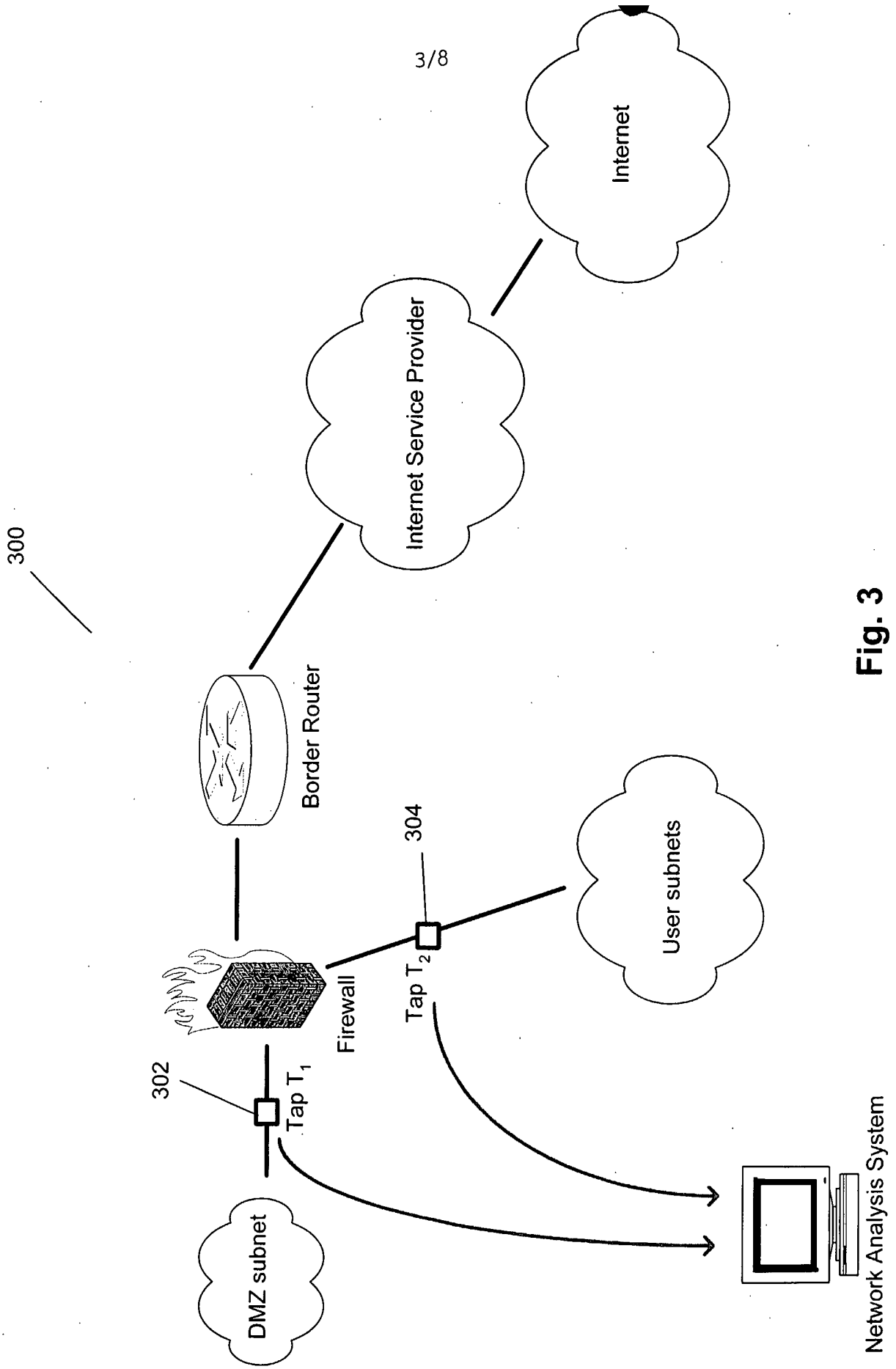

300
Internet
Internet Service Provider
Border Router
304
User subnets
Tap T_2
Firewall
302
Tap T_1
DMZ subnet
Network Analysis System

Fig. 3

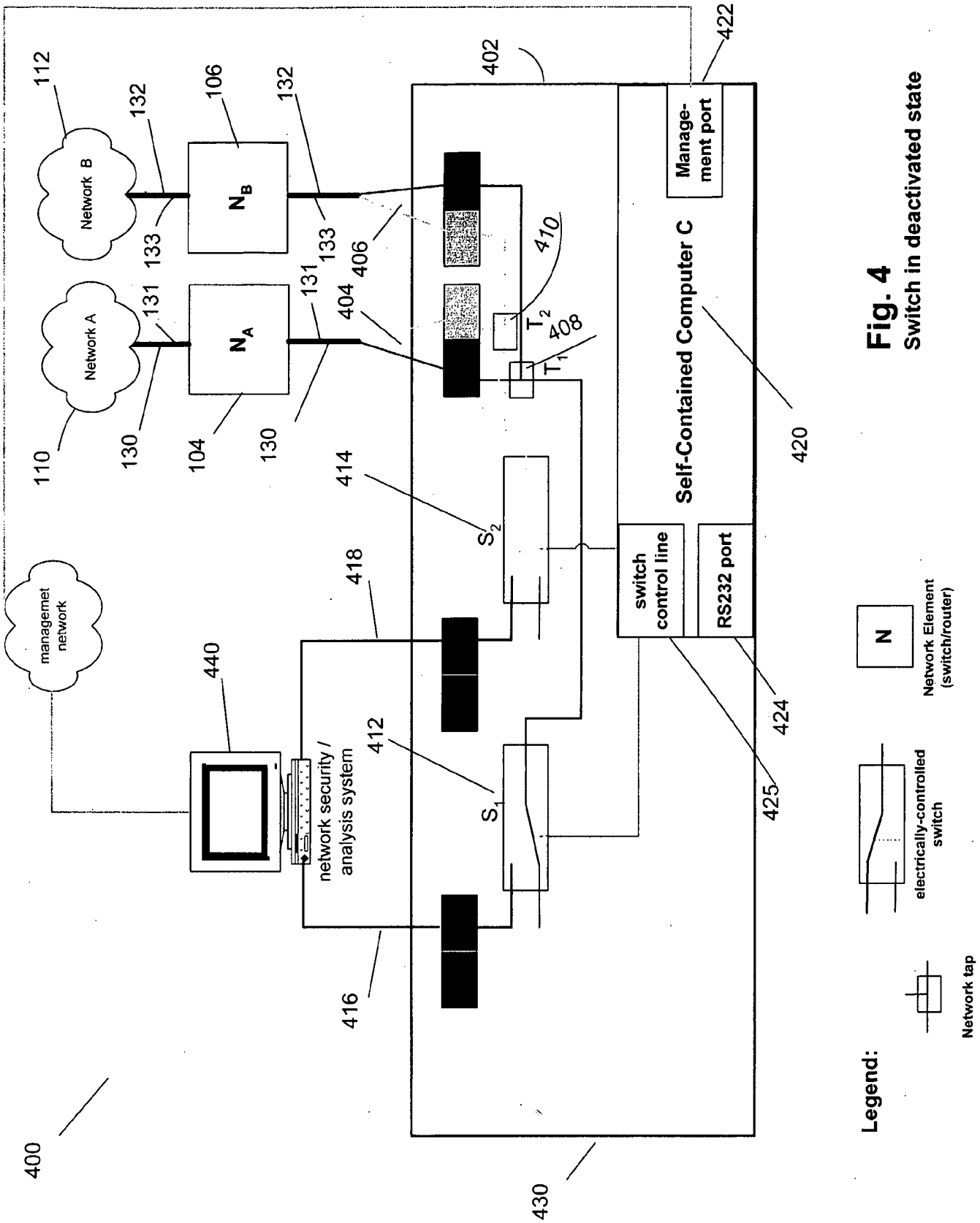


Fig. 4
Switch in deactivated state

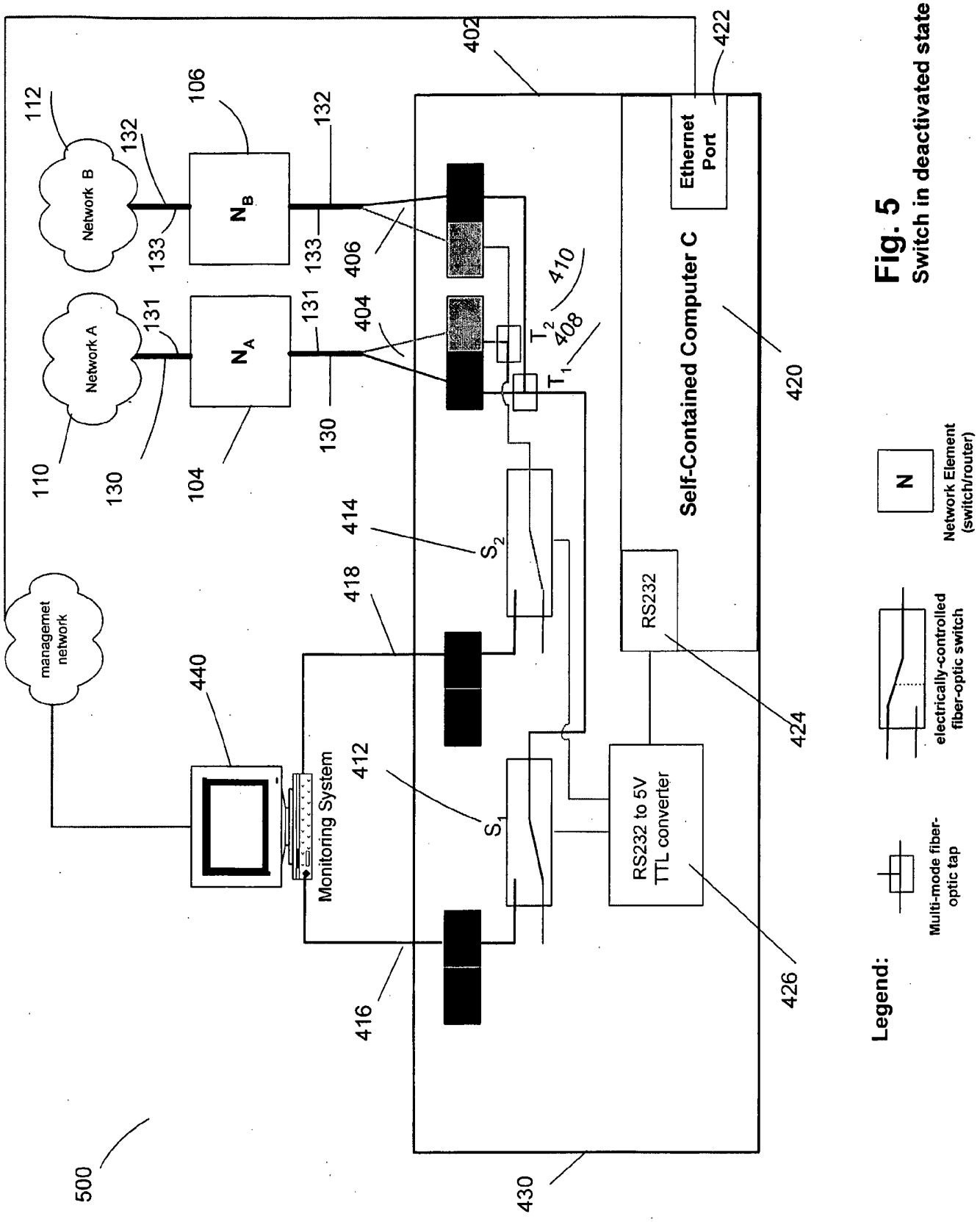


Fig. 5
Switch in deactivated state

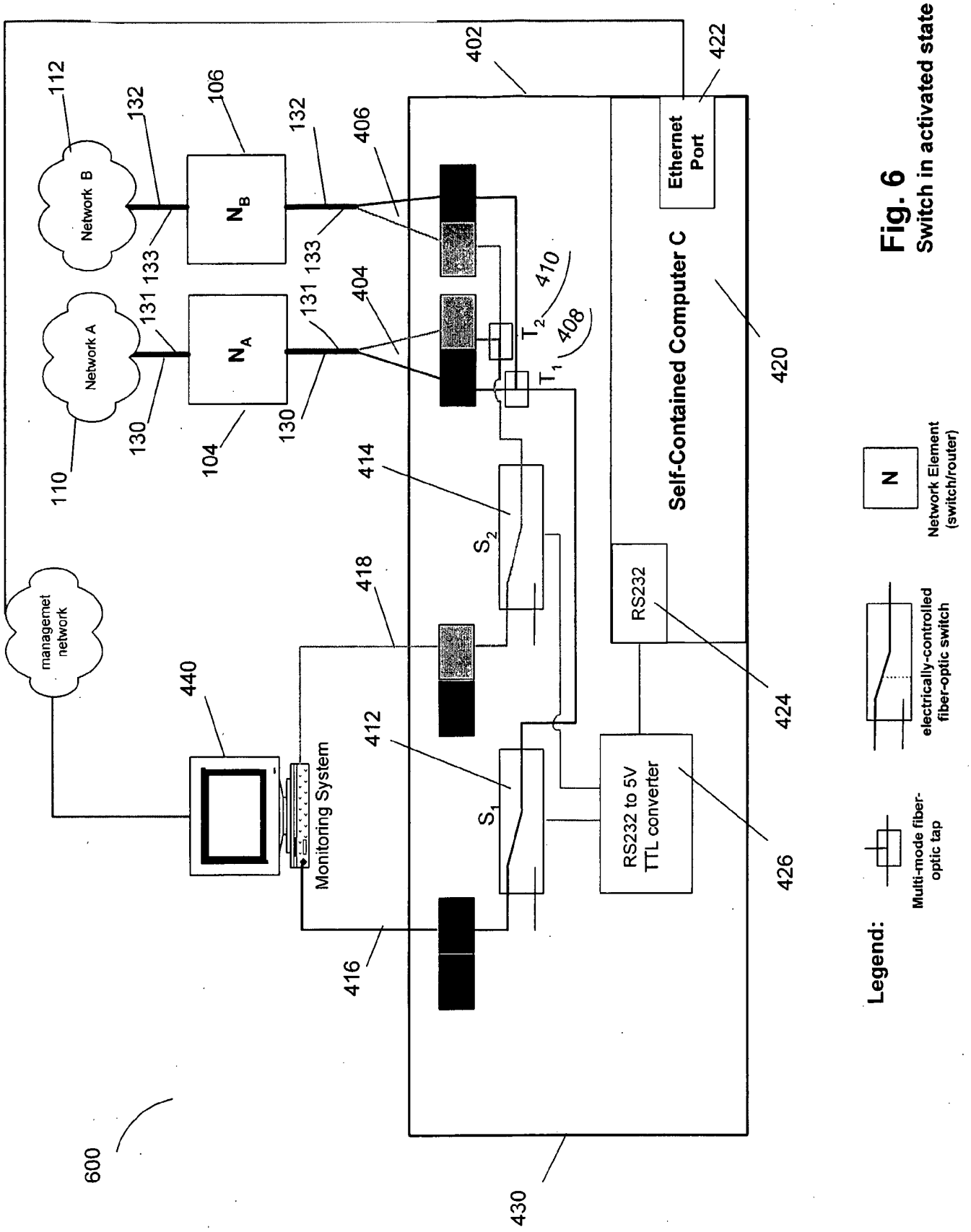


Fig. 6
Switch in activated state

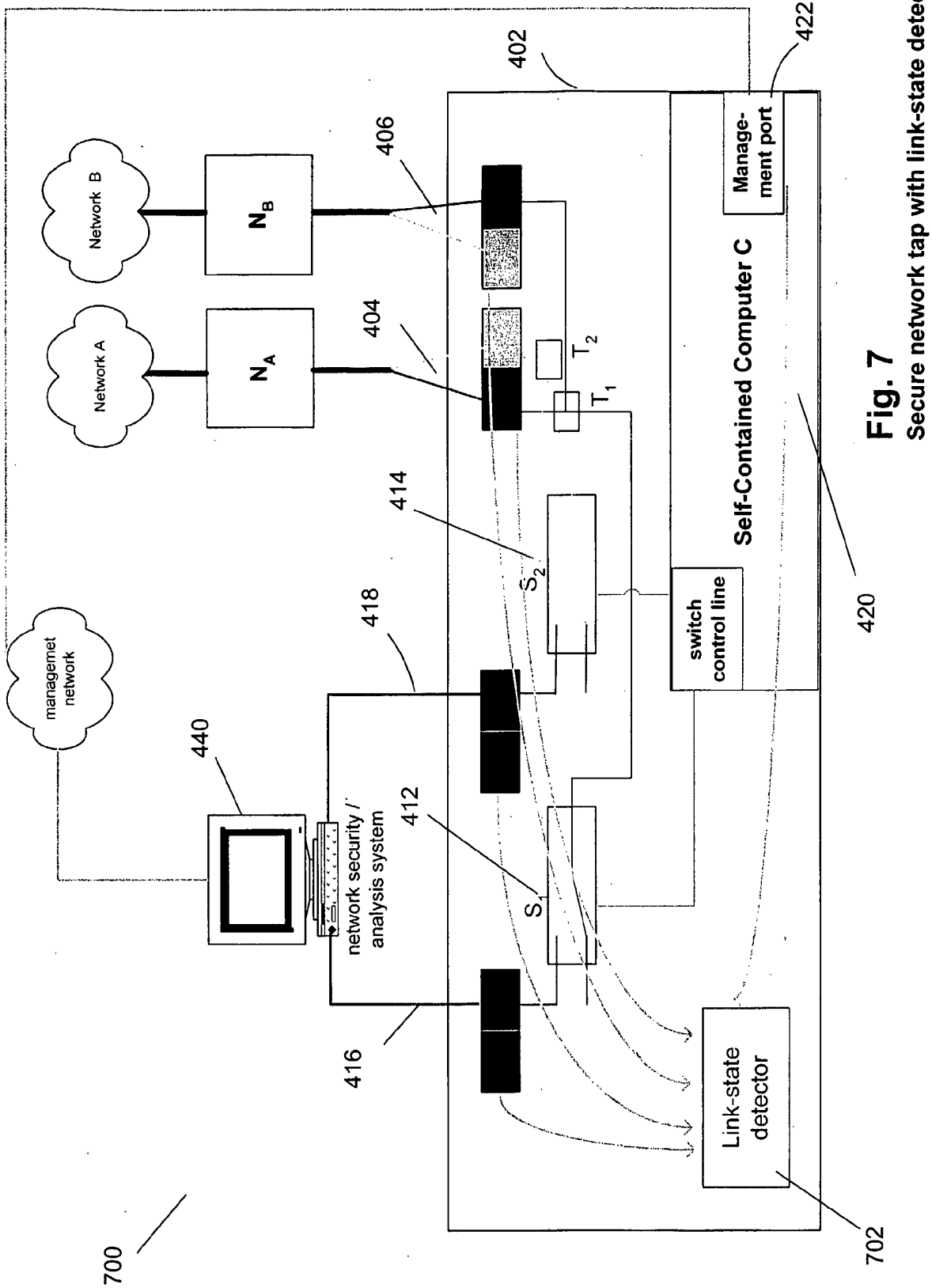


Fig. 7
Secure network tap with link-state detection

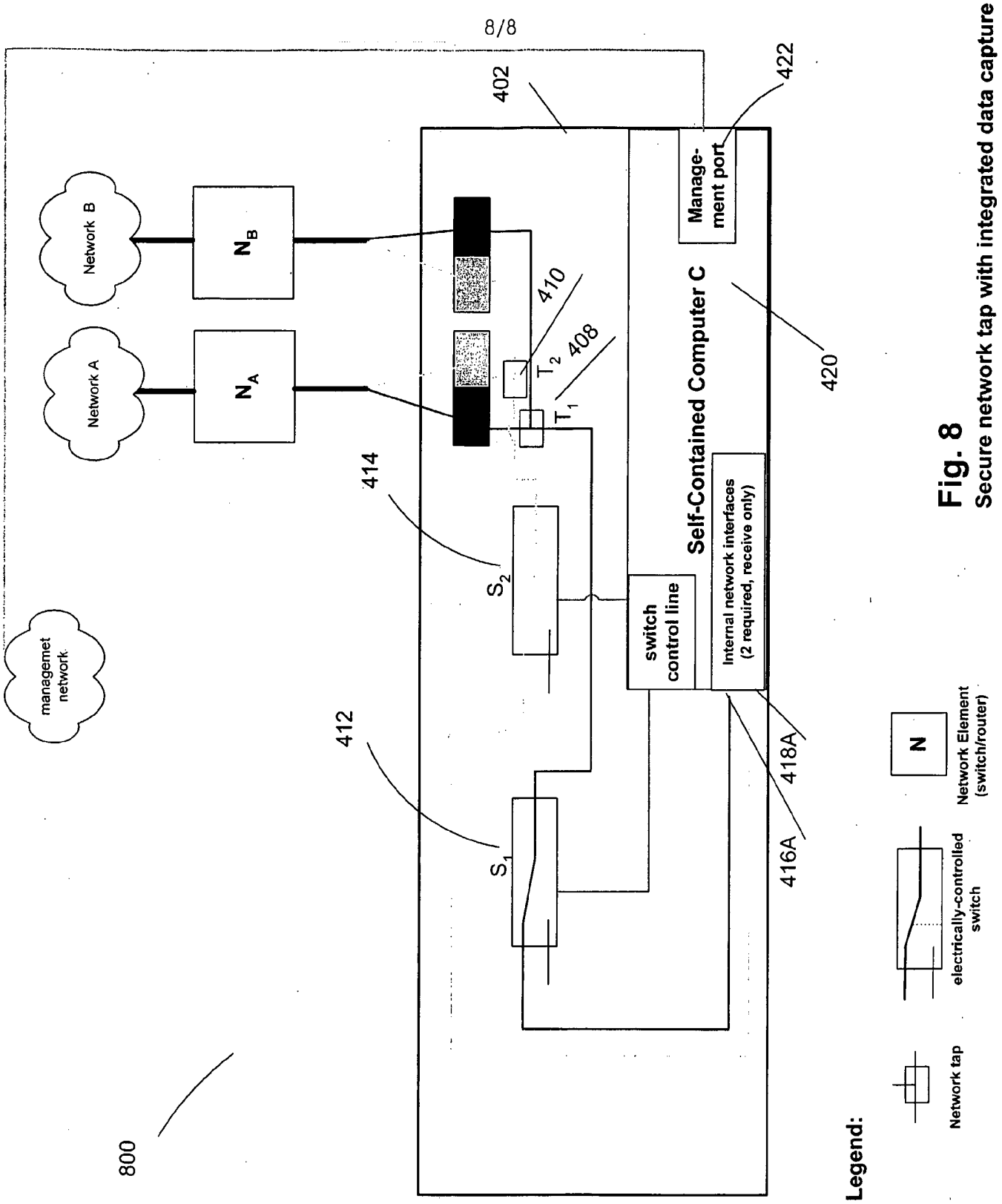


Fig. 8
Secure network tap with integrated data capture