(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 1 826 986 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
20.01.2010 Bulletin 2010/03

(51) Int Cl.:
H04L 29/06 *(2006.01)* ***H04L 12/24*** *(2006.01)*

(21) Application number: **07106761.5**

(22) Date of filing: **21.01.2003**

(54) Management of passive network devices using covert connections

Verwaltung passiver Netzwerkgeräte über verdeckte Verbindungen

Gestion de dispositifs de réseau passifs à l'aide de connexions cachées

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT SE SI SK TR

(43) Date of publication of application:
29.08.2007 Bulletin 2007/35

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
03729531.8 / 1 586 185

(73) Proprietor: **IP-Tap UK**
Cambridge CB4 0WS (GB)

(72) Inventors:
- **Evrard, Philippe**
  B-1380, Lasne (BE)
- **Naveau, Olivier**
  B-1020, Laeken (BE)
- **Nasdrovisky, Stephane**
  B-1020, Laeken (BE)
- **Dubois, Olivier**
  Braine L'Alleud (BE)

(74) Representative: **Piotrowicz, Pawel Jan Andrzej et al**
Venner Shipley LLP
Byron House
Cambridge Business Park
Cowley Road
Cambridge CB4 0WZ (GB)

(56) References cited:
US-B1- 6 266 704

- **HWA-CHUN LIN ET AL: "Distributed network management by HTTP-based remote invocation" GLOBECOM 99, vol. 3, 5 December 1999 (1999-12-05), pages 1889-1893, XP010373743**
- **MARKUS KUHN: "Steganography" STEGANOGRAPHY MAILING LIST, [Online] 3 July 1995 (1995-07-03), pages 1-2, XP002242875 Retrieved from the Internet: URL:http: //www.jjtc.com/Steganography/steg list.htm> [retrieved on 2003-05-30]**

EP 1 826 986 B1

Description

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention is related to the field of data network security and, more particularly, to a system and method for covertly managing passive network devices from a remote location.

Description of the Related Art

[0002] The emergence of Internet commerce has forced large organizations to connect their internal networks to public networks, with the resulting increase in risk being inevitable. The security industry progressively provides the procedures, tools and countermeasures to respond to this increased risk. Security solutions may be broadly categorized as active or passive.

[0003] Network devices are active if they are required to set up a functional infrastructure and may include, among others, access control (firewalls), content filtering (anti-virus), and strong authentication (radius). Conversely, network devices which are not required to set up a functional infrastructure are passive and are typically used to build a second line of defense. Passive devices include, for example, intrusion detection and network scanning.

[0004] Two tools commonly used by organizations to obtain network security include the firewall as an active component, and intrusion detection as a passive component.

[0005] The firewall is an active component in that it affirmatively decides, for each inbound or outbound packet, whether the packet is to be accepted or dropped. The firewall is located at a key point of the network, meaning a point where all the traffic from/to the public network can be controlled. However, while the firewall is an important piece of network security, it remains vulnerable for at least three reasons. First, firewalls are not immune to network attacks hidden in legitimate packets; half-open connection attack, resulting from a protocol flow, or packet fragmentations are two better known examples. Second, firewalls, like other software implementations, are not immune to software bugs. Third, firewalls are administered by security administrators who can make mistakes or who may be inadequately trained to fulfill their function.

[0006] For at least these reasons, the firewall itself needs to be protected. Like any other protection device, a firewall cannot resist assault indefinitely and thus is vulnerable if an alert is not triggered within a defined period of time. Hence, intrusion detection systems are used to provide such alerts.

[0007] Intrusion-detection systems may be either host-based or network-based. Host-based intrusion detection systems are installed on servers and monitor important system resources like files, processes and system activity. Network-based intrusion-detection systems are connected to key points of the network and monitor traffic from/to public networks.

[0008] To protect themselves against potential intruders, some passive network devices need to remain hidden. This means that while they are physically connected to the network and able to tap any network traffic, they do not answer to any kind of request. Network-based intrusion detection systems are often invisible, meaning that the network interface card (NIC) on which they capture the network traffic has its communication stack disabled. Disabling the communication stack is the absolute protection guarantee against attacks coming from the network and should be a requirement for a passive device that must remain uncompromised.

[0009] Problems arise when hidden passive network devices need to be managed from a remote location. Most network-based devices need to be administered from or communicate with a management center. To do so, the device uses either forged packets that are pushed on the local network or an additional NIC connected to the internal network with standard IP-based traffic used to communicate with the management server. Both of these methods annihilate the protection guarantee offered by a passive device; in the first case, the management center could be compromised, in which case resulting effects are unpredictable and, in the second case, the internal network is a perfect backdoor.

[0010] Remote Management is eg. disclosed by "Distributed Network Management by HTTP-Based remote Invocation", Lin, Wang, Globecom '99.

[0011] Accordingly, a need exists for a method allowing passive network devices to be covertly managed from a remote location.

SUMMARY OF THE INVENTION

[0012] The invention is defined by the subject matter of the independent claims.

[0013] In view of the foregoing, one object of the present invention is to overcome the difficulties of managing passive network devices from a remote location without compromising the management center through the use of partner devices for passive network devices.

[0014] Another object of the present invention is to establish a standard IP-based conversation between two or more partner devices as a first communication channel that can then be used by passive network devices to create a second communication channel allowing such devices to communicate.

[0015] A further object of the invention is to establish a system in which a passive network device listens to network traffic intended for another recipient and extracts necessary management information from such traffic.

[0016] A still further object of the invention is to enable a passive network device to generate protocol data units (PDU's) imitating those sent by a cooperating node in

order to implement the reverse direction of management traffic.

[0017] Another object of the invention to is provide a system and method in which neither the management center nor the passive network devices are directly addressable on the network but instead require a third party in order to communicate with one another.

[0018] Yet another object of the invention is to establish a covert management channel between a management center and a passive network device using a standard communication channel established between two third parties.

[0019] In accordance with this and other objects, the present invention is directed to a system and method for covertly managing passive network devices from a local or remote management center. A standard IP-based conversation established over a data network between two or more partner devices occurs in a first communication channel. The passive network devices listen to the network traffic passing on the data network to which they are connected. While the traffic is not intended for the passive network devices, but rather is being passed between the partner and cooperating devices, the passive network devices are able to extract their management information from this traffic and, through generation of protocol data units (PDU's) imitating those sent by the intended nodes, implement the reverse direction of the management traffic. Using a communication channel set up between third parties to enable communication, neither the management center nor the passive network devices are directly addressable on the network, instead being "transparent" to the network. Traffic exchanges are signed and encrypted in order to provide standard authentication, privacy and integrity.

[0020] These together with other objects and advantages which will become subsequently apparent reside in the details of construction and operation as more fully hereinafter described and claimed, reference being had to the accompanying drawings forming a part hereof, wherein like numerals refer to like parts throughout.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021]

Figure 1 illustrates a typical network topology according to the prior art;

Figure 2 illustrates the two distinct communication channels in accordance with the present invention;

Figure 3 is a more detailed embodiment of a protocol stack for the second communication channel of Figure 2;

Figure 4 depicts the minimal set of primitives of the service interface for the second communication channel of Figure 3;

Figure 5 presents a time diagram of the service primitives of Figure 4;

Figure 6 illustrates the APDU layering and encapsulation within the communication stacks of the second communication channel according to the present invention;

Figure 7a presents the coupling between transmission and host layers (emission) within the communication stacks of the second communication channel according to the present invention; and

Figure 7b illustrates the coupling between transmission and host layers (reception) within the communication stacks of the second communication channel according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0022] In describing a preferred embodiment of the invention illustrated in the drawings, specific terminology will be resorted to for the sake of clarity. However, the invention is not intended to be limited to the specific terms so selected, and it is to be understood that each specific term includes all technical equivalents which operate in a similar manner to accomplish a similar purpose.

[0023] A typical network topology according to the prior art is depicted in Figure 1. The devices involved in the covert management method are all connected on the insecure network 13 through a local area network (LAN) 110, 111. As used herein, "device" is used to refer to a standard computer hardware arrangement running an operating system (OS) and a set of applications, and including a network interface card (NIC) required by the network connection. The insecure network 13 may be the Internet through which an intruder 12 gains access to the LANs 110, 111.

[0024] As shown, the devices may include a partner 10, a management center 11, a managed element 15 and a cooperating system 16. The managed element 15, to be remotely managed by the management center 11, includes passive network devices. The partner 10 and cooperating system 16 represent communication nodes on the network between which information is passed. These two devices establish an IP-based communication with one another. According to the transport and application pair that is selected for this particular communication, different scenarios are possible. For example, the partner 10 can send a stateless (UDP, ICMP) packet to the cooperating system 16; the partner 10 can establish a stateful (TCP) connection to the cooperating system 16; the cooperating system 16 can send a stateless (UDP, ICMP) packet to the partner 10; or the cooperating system 16 can establish a stateful (TCP) connection to partner 10.

[0025] The management center 11 and the managed element 15 are invisible in order to protect themselves from external attacks which could be performed by the potential intruder 12. This implies that the management center 11 and the managed element 15, respectively connected to LAN 110 and LAN 111, have their network interface card (NIC) set in promiscuous mode to capture

any traffic circulating on their respective networks. However, their data, network and transport layers have been configured in such a way that they do not give away any information, e.g., ARP response, broadcast, etc., that could reveal their presence. This having been said, there is no way, a priori, that the management center 11 and the managed element 15 can communicate management information to each other.

[0026] In order to address this problem, and according to a preferred embodiment of the present invention illustrated in Figure 2, a covert management channel, or second communication channel 325, is established between the management center 101 and the managed element 105 using a standard communication channel, or first communication channel 225, established between partner 100 and cooperating system 106. As noted earlier, the managed element 15, to be remotely managed by the management center 11, includes a passive network device. The partner 100 and cooperating system 106 represent communication nodes on the network between which information is passed. These two devices establish an IP-based communication with one another using the standard communication channel.

[0027] The standard communication channel represents the first communication channel 225 which is a standard IP peer-to-peer communication. Partner 100 and cooperating system 106 communicate through a set of intermediate systems. Two types of intermediate systems are illustrated in Figure 2, namely intermediate system 200 and intermediate system 201.

[0028] Partner 100 and cooperating system 106 run full communication stacks, numbered from 0 to 3. Typically, in a TCP/IP model, these layers could be mapped on 0: network interface card (NIC) layer 300 and device drivers; 1: network layer 301 (IP); 2: transport layer 302 (TCP, UDP or other like ICMP); and 3: application layer (HTTP, FTP) 303.

[0029] Intermediate system 200 runs a subset of the full stack, up to the transport layer 302, and typically includes networking equipment, like routers. Intermediate system 201 runs a still smaller subset of the communication stack, including the NIC layer 300, and may include backbone equipment.

[0030] According to the present invention, the second communication channel 325, utilized by the management center 101 and the managed element 105, is integrated with the first communication channel 225. Although the management center 101 and the managed element 105 do not have any possibility of communicating directly with one another as neither is directly addressable, they are able, by "eavesdropping" on the legitimate conversation between partner 100 and the cooperating system 101 over the first communication channel 225, to receive and transmit the management information they need to exchange.

[0031] An example will illustrate the operation of the dual communication channel according to the present invention. Suppose partner 100 is part of a network operation center (NOC). The objective of partner 100 is to monitor the state of a set of web servers, one of which is the cooperating system 106. The partner 100 issues a request, such as a SNMP-request, to the cooperating system 106 in order to obtain information. The management center 101 and the managed element 105 are aware of this legitimate request because they are connected on local area networks such as LAN 110 and LAN 111 and, having their NIC set in promiscuous mode, can "see" the request. Therefore, the management center 101 and the managed element 105 are aware that an answer from the cooperating system 106 is expected.

[0032] Independently of the request sent by partner 100, the management center 101 can fabricate a request (a "fabricated" request) whose source IP address is partner 100 and whose destination address is cooperating system 106, and can push this "fabricated" request onto the network. Such a "fabricated" request, so termed to distinguish it from the legitimate request already sent by the partner 100, includes a marker (MK) which indicated a relationship with the management center 101. As a legitimate packet, the "fabricated" request of management center 101 is routed to the cooperating system 106. The managed element 105, eavesdropping on the network, detects the marker (MK) of the management center 101 and, by trapping the packet, obtains the request.

[0033] In the other direction, independently of the answer supplied by the cooperating system 106, the managed element 105 can fabricate an answer (a "fabricated" answer) whose source IP address is the cooperating system 106 and whose destination address is the partner 100, and can push this "fabricated" answer onto the network. Such a "fabricated" answer, so termed to distinguish it from the legitimate answer sent by the cooperating system 106, includes a marker (MK) which indicates a relationship with the managed element 105. As a legitimate packet, the "fabricated" answer of the managed element 105 is routed back to the partner 100. The management center, eavesdropping on the network, recognizes the marker (MK) of the managed element 105 and, by trapping the packet, obtains the information it needs.

[0034] The marker (MK) is a means tht allows the management center 101 and the managed element 105 to filter out of the legitimate traffic of the first communication channel 225 the few network packets that will be used to transport the covert management information of the second communication channel 325. As an illustration, the partner 100 may synchronize the cooperating system 106 through the NTP protocol. In this case, the management center 101 and the managed element 105 will be configured to use this legitimate conversation to build the covert management channel and the marker (MK) will be a pattern that will retrieve all NTP network traffic (UDP port 123, TCP port 123). The traffic will be legitimate if it belongs to the first communication channel 225 and "fabricated" if it belongs to the second communication channel 325. As the volume of the network traffic of the first communication channel 225 can potentially be huge, the

marker (MK) must be tuned in such a way that it will deliver a low volume but constant traffic to the management center 101 and the managed element 105.

[0035] Because the management center 101 and the managed element 105 do not have their network and transport layers enabled, the application layer of the management center 101 and of the managed element 105 needs to emulate a communication stack both to send and receive network packets. Concerning the packet reception, such an embodiment may be implemented through a Berkeley Packet Filter (BPF). In this latest case, the marker (MK) defined to filter out the network packets at the destination of the managed element 105 can be any filter supported by BPF:IP addresses, destination ports, and defined pattern used in network packet payload. The marker (MK) is initialized at installation time.

[0036] Both communication channels have their independent communication stacks as shown in Figure 2. The first communication channel 225, used by the partner 100 and the cooperating system 106, is based on a standard TCP/IP model, using network, transport and application layers and functions. The second communication channel 325 has its independent communication stack, designated by five different communication layers: 0, A, B, C and D, and relies on the first communication channel network layer 301, and eventually transport layer 302, to transport the information it needs to communicate.

[0037] By nature, the present invention is intended to transfer small protocol data units (PDU's) between the management center 101 and the managed element 105 in a connectionless, datagram type of communication. Indeed, when the second communication channel relies on the first communication channel to serve as a vehicle for moving the PDU between peer entities, this can only be done through a single, or limited number of, datagram packets. Since a primary purpose of the invention, as implemented through the second communication channel, is to covertly manage, in a secure way, a set of passive network devices without compromising their integrity through the activation of a communication stack, the covert channel is initially intended to support control command. The underlying hardware and network type define the maximum size of a packet, including all headers, referred to as the maximum transfer unit (MTU). Typically, a packet size of a few hundred bytes is sufficient to implement the present invention.

[0038] A further recommendation of the present invention is to employ commonly used Internet protocols like NTP or HTTP to host the covert management traffic. This way, the covert management traffic is diluted into the normal traffic, the benefit thereof being that there is a high probability that the passive device will remain undetected, further of being uncompromised.

[0039] An embodiment of the protocol stack for the second communication channel, in accordance with the present invention, is shown in Figure 3. This stack or communication model, referred to conceptually as a service provider 400, includes a plurality of communication layers including a host layer A, a transmission layer B, a validation layer C, and a management service layer D. While the number and nature of the different layers may vary, adherence with certain design principles is recommended. As an example, for simplicity the number of layers should be kept as small as possible. Each layer should have its own functions and similar functions should be placed within the same layer; specific functions should not overlap across layers. Each layer should have a set of interfaces only with adjacent layers, and it should be possible to redesign a layer without affecting adjacent layers. Finally, the implementation of the same layer specification may vary according to the hardware, the device driver, and the operating system that are used.

[0040] In compliance with the design principles just summarized, the functions of the different communication layers shown in Figure 3 may be defined as follows.

[0041] The function of the management service layer D is to maintain a covert management general context between the management center 101 and the managed element 105 by maintaining a sequence number. The management service layer D also provides management service header information like version, source and destination address.

[0042] The function of the validation layer C is to provide authentication, integrity and privacy. Based on standard algorithms, the validation layer C calculates a message authentication code (MAC) and a packet key (PK), and encrypts/decrypts the payload received from the adjacent upper/lower layers.

[0043] The function of the transmission layer B is to provide functions to convert the encrypted payload from binary to ASCII and back, as well as generic functions to build the packet that needs to be sent to the peer host. The transmission layer B may also be divided into two adjacent sublayers, namely transmission and transport sublayers. A transport layer specification may be needed should the amount of data to be transferred between peer entities be large or should the quality of services be guaranteed.

[0044] The function of the host layer A is to provide an interface to the local host device driver and hardware to send and receive network packets. In most implementations, the host layer A runs in kernel space while the other communication layers run in user space. The host layer may be implemented using a Berkeley UNIX BPF filter.

[0045] A minimal implementation of the present invention is illustrated in Figure 4. In order for the management center 101 and the managed element 105 to communicate, the management center 101 runs an application process referred to as the management application 410 and the managed element 105 runs an application process referred to as the management agent 420. The service interface used by the management application 410 and the management agent 420 defines six primitives, namely the Command Send 411, the Response Receive 412, the Trap Receive 413, the Command Receive 421, the Response Send 422, and the Trap Send 423.

[0046] As in any communication model, there is a logical transmission between the peer layers of the communication stack but the physical communication occurs at the lowest level of the communication stack or service provider 400, i.e., at the host layer A.

[0047] The time sequence diagrams of Figure 5 present the sequence of events that take place in the order of their relative positions on the vertical time lines. The management application 410 sends a Command Send request 411 to the service provider 400 through the service interface. The service provider 400 transmits the Command Send request 411 to the management agent 420 which, in turn, prepares the Response Send 422 and submits it to the service provider 400 through the service interface. The management application 410 receives the Response Receive 412 from the service provider 400. Should the management agent 420 wish to communicate some unsolicited information to the management application 410, the agent 420 issues a Trap Send 423 to the service provider 400, which the management application 410 will receive through the Trap Receive 413 primitive.

[0048] Figure 6 gives a detailed view of how each communication layer transforms the Application Protocol Data Unit (APDU), when each communication layer fulfills its function.

[0049] The management service layer D receives an APDU and concatenates the management header to the APDU. The management header includes a timestamp (TS), the version (VER) of the management service layer, the source (SRC) and the destination addresses (DST), and a sequence number (SEQ).

[0050] The timestamp is essential to the management of passive network devices because, at a minimum, it is required to correlate events; it may also be used to compute a packet key. Therefore, any communication between the management center 101 and the managed element 105 is time-stamped.

[0051] The version of the management service layer is required to guarantee upward compatibility. It is preferred to represent the version in one byte. The four first bits are dedicated to the major version number and the four last bits to the minor version number.

[0052] Each passive network device, whether part of the management center 101 or the managed element 105, receives a unique address. More specifically, the address is a unique characteristic of the management service layer of a particular device, by analogy with an IP address which is the unique characteristic of the first communication channel 225. Addresses of both communication channels are assigned independently.

[0053] The assignment of IP addresses to the devices of the first communication channel 225 (namely, the partner 100 and the cooperating system 106) is a prerequisite of the second communication channel 325. This assignment complies with the standard Internet connectivity practices, meaning that two devices will be able to establish a standard TCP/IP conversation on the required ports, with whatever firewall, router, etc., reconfiguration (s) being implied.

[0054] The assignment of addresses to the passive devices of the second communication channel 325 cannot be completely defined in the present invention because it depends upon the management model of the passive devices. Generally, the unique address can be initialized in one of two ways. Should the managed element 105 be an appliance that is completely pre-installed and configured by a single vendor, the vendor, who is in control of the full address range, will pre-configure the unique address. In some instances, the vendor can also pre-configure the unique address of the management center(s) 101. Should the managed element 105 be an appliance delivered by several vendors, however, the unique address will typically be initialized at configuration time and delivered by the authority that has the full address range under its control. The initialization of the passive device will have to take these two scenarios into account.

[0055] The sequence number is a global counter maintained by the management service layer of the management center 101 and of the managed element 105. As earlier stated, a primary purpose of this invention is to communicate small control commands/responses. Therefore, the sequence number is primarily used to track and check whether commands, responses or traps have been lost.

[0056] The present invention proposes a communication model where commands, responses and traps will inevitably be lost since there is no possible guarantee on the Quality of Service (QoS), which is a characteristic of the first communication channel. Therefore, the management service layer is responsible for repeating the commands until it receives an acknowledgment. An acknowledgment of a Command Send 411 consists of a Response Receive 412. An acknowledgment of a Trap Send 423 cannot be fully specified in the present invention because it depends on the nature of the passive device. It can include a Command Send 411, a reconfiguration of an active device, or a manual intervention of an operator on the passive device, whose effect is to reset the Trap Send 423 condition. The management service layer D passes the management header and the APDU to the validation layer C.

[0057] The validation layer C offers complementary functions, depending upon whether it is sending or receiving a packet. If it sends a packet, it appends a Message Authentication Code (MAC), computes a packet key and encrypts the packet. If it receives a packet, it computes a packet key, decrypts the message using the MAC, and checks validity.

[0058] It is the responsibility of the supplier of the passive network devices to define the encryption schemes that will be supported by such devices. Due to the characteristics of the second communication channel, manual IPSEC is a basic requirement.

[0059] The validation layer C passes an encrypted

buffer in binary format to the transmission layer B. Like the validation layer C, the transmission layer B offers complementary functions, depending upon whether it is sending or receiving a packet. If a packet is being sent, the transmission layer B first transforms the binary buffer into an ASCII machine-independent format. It then builds a network packet that contains the ASCII buffer and that is in a suitable format for the host layer A; this transformation is detailed in Figure 7a. The network packet is passed to the host layer A. If the transmission layer B receives a network packet from the host layer A, the transmission layer first extracts the ASCII payload from the network packet, converts the ASCII buffer into a binary buffer and transfers it to the validation layer, as detailed in Figure 7b. The host layer does not perform any data transformation. Equipped with an emitter 20 and a receptor 30, the host layer A provides an interface between the other communication layers of the service provider 400 and the local device driver and hardware.

[0060] Figure 7a presents in greater detail how the transmission and host layers integrate to send a PDU to a passive network device. An example will be used for illustration. If the transmission layer receives a packet to be transferred, the transmission layer transforms the binary buffer into ASCII and copies this PDU into the transmit queue where the PDU awaits transmission.

[0061] Figure 7b presents in greater detail how the transmission and host layers integrate to receive a PDU from the passive network device. The receptor 30 of the host layer A constantly monitors the network 50 and filters out packets that match a set of predefined patterns that define the marker (MK); the patterns may be stored in a pattern file 35. When the receptor 30 of the host layer filters out a packet, it sends it to the PDU factory 40 of the transmission layer B. The PDU factory 40 decides if the packet is an emission signal or a received PDU. In the first case, if the transmit queue is not empty, the PDU factory 40 builds a network packet and sends it to the emitter 20 of the host layer A. In the second case, the received PDU is passed to the ASCII to binary generic function, transformed into BIN and inserted into the reception queue, where it is then passed to the validation layer C.

[0062] The foregoing descriptions and drawings should be considered as illustrative only of the principles of the invention. The invention may be configured in a variety of shapes and sizes and is not limited by the dimensions of the preferred embodiment. Numerous applications of the present invention will readily occur to those skilled in the art. Therefore, it is not desired to limit the invention to the specific examples disclosed or the exact construction and operation shown and described. Rather, all suitable modifications and equivalents may be resorted to, falling within the scope of the invention.

Claims

1. A management center (101) for managing a passive network device from a remote location over a distributed computer network, said management center configured to listen to data traffic on a data network and to be transparent to said data network, said management center configured to generate a fabricated request and to push said fabricated request onto said data network, said fabricated request having a source address corresponding with a partner device (100) and a destination address corresponding with a cooperating device (106) such that said fabricated request is routable to said cooperating device on said data network as a legitimate packet, said fabricated request further having a marker indicating a relationship with said management center, said management center further configured to eavesdrop on said data network, to recognize a marker on a fabricated answer generated and pushed onto said data network by a managed element (105), said fabricated answer having a source address corresponding with said cooperating device and a destination address corresponding with said partner device, said fabricated answer further having a marker indicating a relationship with a managed element, and to trap the fabricated answer packets to thereby indirectly exchange information with the managed element over said data network.

2. A management center according to claim 1, wherein said management center includes a service provider (400) having a host layer, a transmission layer, a validation layer and a management service layer.

3. A management center according to claim 2, wherein said management service layer is configured to concatenate a management header to a received data unit, said header including at least one of a timestamp, a source address and a destination address.

4. A management center according to claim 2 or 3, wherein management center is configured to run an application process to communicate with the managed element over a service interface which defines a plurality of primitives (411, 412, 413, 421, 422, 423).

5. A managed element (105) for being managed by a management centre (101) from a remote location over a distributed computer network, said managed element configured to listen to data traffic on a data network and to being transparent to said data network, said managed element configured to eavesdrop on said data network, to recognize a marker on a fabricated request generated and pushed onto said data network by a management center (101), said fabricated request having a source address corre-

sponding with a partner device and a destination address corresponding with a cooperating device, said fabricated request further having a marker indicating a relationship with said management center, and to trap the fabricated request, said managed element further configured to generate a fabricated answer and to push said fabricated answer onto said data network, said fabricated answer having a source address corresponding with a cooperating device and a destination address corresponding with a partner device such that said fabricated answer is routable to said partner device on said data network as a legitimate packet, said fabricated answer further having a marker indicating a relationship with said managed element to thereby indirectly exchange information with the management center over said data network.

6. A managed element according to claim 5, wherein said managed element includes a service provider having a host layer, a transmission layer, a validation layer and a management service layer.

7. A managed element according to claim 6, wherein said management service layer is configured to concatenate a management header to a received data unit, said header including at least one of a timestamp, a source address and a destination address.

8. A managed element according to claim 6 or 7, wherein managed element is configured to run an application process to communicate with the management center over a service interface which defines a plurality of primitives.

9. A managed element according to any one of claims 5 to 8, wherein said managed element is a passive network device.

10. A method for managing a passive network device from a remote location over a distributed computer network, the method comprising:

listening to data traffic on a communication channel between a partner device and a cooperating device on a data network and being transparent to the data network;
generating a fabricated request addressed to said cooperating device and having a source address of said partner device, said fabricated request also having a marker indicating a relationship with a management center;
detecting a marker on a fabricated answer generated and pushed onto said data network by a managed element (105), said fabricated answer having a source address corresponding with said cooperating device and a destination address corresponding with said partner device, said fabricated answer further having a marker indicating a relationship with a managed element; and
trapping said fabricated answer.

11. A method according to claim 10, further comprising:

intercepting unsolicited information addressed to one of said partner device and said cooperating device through a trap receive primitive.

12. A method for managing a passive network device from a remote location over a distributed computer network, the method comprising:

listening to data traffic on a communication channel between a partner device and a cooperating device on a data network and being transparent to the data network;
detecting a marker on a fabricated request generated and pushed onto said data network by a management center (101), said fabricated request having a source address corresponding with said partner device and a destination address corresponding with said cooperating device, said fabricated request further having a marker indicating a relationship with a management center;
trapping said fabricated request; and
generating a fabricated answer to said fabricated request, said fabricated answer addressed to said partner device and having a source address of said cooperating device, said fabricated answer also having a marker indicating a relationship with said managed element.

13. A method according to claim 12, further comprising:

intercepting a command send primitive from said management center; and
pushing a response onto the network with a response send primitive which for trapping by said management center.

14. A method according to claim 12 or 13, further comprising:

conveying unsolicited information to said management center by conveying data addressed to one of said partner device and said cooperating device using a trap send primitive.

15. A method according to any one of claims 10 to 14, further comprising, when sending a packet:

concatenating a header to a data unit, said header including at least one of a timestamp, a destination address, and a source address;

forwarding the header and data unit to a validation layer;
appending an authentication code to and encrypting said packet;
passing the encrypted packet in binary format to a transmission layer;
transforming said binary format into ASCII and building a network packet suitable for a host layer;
passing the network packet to said host layer; and
inserting said network packet into a transmit queue.

16. A method according to any one of claims 10 to 15, further comprising, when receiving a packet:

monitoring the network for a packet matching a predefined pattern;
filtering out an appropriate packet;
forwarding the packet to a transmission layer;
inserting, in response to determining that the packet is a data unit, the data unit into a reception queue;
converting the data unit into binary format;
forwarding the binary data unit to said validation layer; and
computing a packet key and decrypting the data unit.

17. A computer program which, when executed by a computer, causes the computer to perform a method according to anyone of claims 10 to 16.

Patentansprüche

1. Managementzentrum (101) zum Managen einer passiven Netzwerkvorrichtung von einem entfernten Ort über ein verteiltes Computernetzwerk, wobei das Managementzentrum dazu konfiguriert ist, Datenverkehr in einem Datennetzwerk abzuhören und für das Datennetzwerk transparent zu sein, wobei das Managementzentrum dazu konfiguriert ist, eine fabrizierte Anforderung zu erzeugen und die fabrizierte Anforderung in das Datennetzwerk zu schieben, wobei die fabrizierte Anforderung eine einer Partnervorrichtung (100) entsprechende Quelladresse und eine einer kooperierenden Vorrichtung (106) entsprechende Zieladresse aufweist, so dass die fabrizierte Anforderung im Datennetzwerk als legitimes Paket an die kooperierende Vorrichtung geleitet werden kann, wobei die fabrizierte Anforderung ferner eine Markierung aufweist, die eine Beziehung zum Managementzentrum angibt, wobei das Managementzentrum ferner dazu konfiguriert ist, im Datennetzwerk zu lauschen, um eine Markierung in einer fabrizierten Antwort zu erkennen, die von einem gemanagten Element (105) erzeugt und in das Datennetzwerk geschoben wurde, wobei die fabrizierte Antwort eine der kooperierenden Vorrichtung entsprechende Quelladresse und eine der Partnervorrichtung entsprechende Zieladresse aufweist, wobei die fabrizierte Antwort ferner eine Markierung aufweist, die eine Beziehung zu einem gemanagten Element angibt, und um die Pakete fabrizierter Antworten einzufangen, um dadurch über das Datennetzwerk indirekt Informationen mit dem gemanagten Element auszutauschen.

2. Managementzentrum nach Anspruch 1, wobei das Managementzentrum einen Serviceprovider (400) mit einer Host-Schicht, einer Übertragungsschicht, einer Validierungsschicht und einer Managementdienstschicht aufweist.

3. Managementzentrum nach Anspruch 2, wobei die Managementdienstschicht dazu konfiguriert ist, einen Managementkopfabschnitt mit einer empfangenen Dateneinheit zu verknüpfen, wobei der Kopfabschnitt zumindest einen Zeitstempel und/oder eine Quelladresse und/oder eine Zieladresse aufweist.

4. Managementzentrum nach Anspruch 2 oder 3, wobei das Managementzentrum dazu konfiguriert ist, einen Anwendungsprozeß auszuführen, um mit dem gemanagten Element über ein Dienstinterface zu kommunizieren, das eine Mehrzahl von Grundelementen (411, 412, 413, 421, 422, 423) definiert.

5. Gemanagtes Element (105) zum Managen durch ein Managementzentrum (101) von einem entfernten Ort über ein verteiltes Computernetzwerk, wobei das gemanagte Element dazu konfiguriert ist, Datenverkehr in einem Datennetzwerk abzuhören und für das Datennetzwerk transparent zu sein, wobei das gemanagte Element dazu konfiguriert ist, im Datennetzwerk zu lauschen, um eine Markierung in einer fabrizierten Anforderung zu erkennen, die von einem Managementzentrum (101) erzeugt und in das Datennetzwerk geschoben wurde, wobei die fabrizierte Anforderung eine einer Partnervorrichtung entsprechende Quelladresse und eine einer kooperierenden Vorrichtung entsprechende Zieladresse aufweist, wobei die fabrizierte Anforderung ferner eine Markierung aufweist, die eine Beziehung zum Managementzentrum angibt, und zum Einfangen der fabrizierten Anforderung, wobei das gemanagte Element ferner dazu konfiguriert ist, eine fabrizierte Antwort zu erzeugen und die fabrizierte Antwort in das Datennetzwerk zu schieben, wobei die fabrizierte Antwort eine einer kooperierenden Vorrichtung entsprechende Quelladresse und eine einer Partnervorrichtung entsprechende Zieladresse aufweist, so dass die fabrizierte Antwort im Datennetzwerk als legitimes Paket an die Partnervorrichtung geleitet

werden kann, wobei die fabrizierte Antwort ferner eine Markierung aufweist, die eine Beziehung zum gemanagten Element angibt, um dadurch über das Datennetzwerk indirekt Informationen mit dem Managementzentrum auszutauschen.

6. Gemanagtes Element nach Anspruch 5, wobei das gemanagte Element einen Serviceprovider mit einer Host-Schicht, einer Übertragungsschicht, einer Validierungsschicht und einer Managementdienstschicht aufweist.

7. Gemanagtes Element nach Anspruch 6, wobei die Managementdienstschicht dazu konfiguriert ist, einen Managementkopfabschnitt mit einer empfangenen Dateneinheit zu verknüpfen, wobei der Kopfabschnitt zumindest einen Zeitstempel und/oder eine Quelladresse und/oder eine Zieladresse aufweist.

8. Gemanagtes Element nach Anspruch 6 oder 7, wobei das gemanagte Element dazu konfiguriert ist, einen Anwendungsprozeß auszuführen, um mit dem Managementzentrum über ein Dienstinterface zu kommunizieren, das eine Mehrzahl von Grundelementen definiert.

9. Gemanagtes Element nach einem der Ansprüche 5 bis 8, wobei das gemanagte Element eine passive Netzwerkvorrichtung ist.

10. Verfahren zum Managen einer passiven Netzwerkvorrichtung von einem entfernten Ort über ein verteiltes Computernetzwerk, wobei das Verfahren umfaßt:

Abhören von Datenverkehr auf einem Kommunikationskanal zwischen einer Partnervorrichtung und einer kooperierenden Vorrichtung in einem Datennetzwerk, und Transparentsein für das Datennetzwerk;
Erzeugen einer fabrizierten Anforderung, die an die kooperierende Vorrichtung adressiert ist und eine Quelladresse der Partnervorrichtung aufweist, wobei die fabrizierte Anforderung weiterhin eine Markierung aufweist, die eine Beziehung zum Managementzentrum angibt;
Detektieren einer Markierung in einer fabrizierten Antwort, die von einem gemanagten Element (105) erzeugt und in das Datennetzwerk geschoben wurde, wobei die fabrizierte Antwort eine der kooperierenden Vorrichtung entsprechende Quelladresse und eine der Partnervorrichtung entsprechende Zieladresse aufweist, wobei die fabrizierte Antwort ferner eine Markierung aufweist, die eine Beziehung zu einem gemanagten Element angibt; und
Einfangen der fabrizierten Antwort.

11. Verfahren nach Anspruch 10, ferner umfassend:

Abfangen nicht angeforderter Informationen, die an die Partnervorrichtung und/oder die kooperierende Vorrichtung adressiert sind, durch ein Einfang-Empfangen-Grundelement.

12. Verfahren zum Managen einer passiven Netzwerkvorrichtung von einem entfernten Ort über ein verteiltes Computernetzwerk, wobei das Verfahren umfaßt:

Abhören von Datenverkehr auf einem Kommunikationskanal zwischen einer Partnervorrichtung und einer kooperierenden Vorrichtung in einem Datennetzwerk, und Transparentsein für das Datennetzwerk;
Detektieren einer Markierung in einer fabrizierten Anforderung, die von einem Managementzentrum (101) erzeugt und in das Datennetzwerk geschoben wurde, wobei die fabrizierte Anforderung eine der Partnervorrichtung entsprechende Quelladresse und eine der kooperierenden Vorrichtung entsprechende Zieladresse aufweist, wobei die fabrizierte Anforderung ferner eine Markierung aufweist, die eine Beziehung zu einem Managementzentrum angibt;
Einfangen der fabrizierten Anforderung; und
Erzeugen einer fabrizierten Antwort auf die fabrizierte Anforderung, wobei die fabrizierte Antwort an die Partnervorrichtung adressiert ist und eine Quelladresse der kooperierenden Vorrichtung aufweist, wobei die fabrizierte Antwort weiterhin eine Markierung aufweist, die eine Beziehung zum gemanagten Element angibt.

13. Verfahren nach Anspruch 12, ferner umfassend:

Abfangen eines Befehl-Senden-Grundelements vom Managementzentrum; und
Schieben einer Antwort in das Netzwerk mittels eines Antwort-Senden-Grundelements zum Einfangen durch das Managementzentrum.

14. Verfahren nach Anspruch 12 oder 13, ferner umfassend:

Übermitteln nicht angeforderter Informationen an das Managementzentrum durch Übermitteln von Daten, die an die Partnervorrichtung und/oder die kooperierende Vorrichtung adressiert sind, unter Verwendung eines Einfang-Senden-Grundelements.

15. Verfahren nach einem der Ansprüche 10 bis 14, beim Senden eines Pakets ferner umfassend:

Verknüpfung eines Kopfabschnitts mit einer Dateneinheit, wobei der Kopfabschnitt zumindest einen Zeitstempel und/oder eine Zieladresse und/oder eine Quelladresse aufweist;
Weiterleiten des Kopfabschnitts und der Dateneinheit an eine Validierungsschicht;
Anhängen eines Authentifizierungscodes an ein Paket und verschlüsseln des Pakets;
Übermitteln des verschlüsselten Pakets im Binärformat an eine Übertragungsschicht;
Umwandeln des binären Formats in ASCII und Erstellen eines für eine Host-Schicht geeigneten Netzwerkpakets;
Übermitteln des Netzwerkpakets an die Host-Schicht; und
Einfügen des Netzwerkpakets in eine Übertragungsschlange.

16. Verfahren nach einem der Ansprüche 10 bis 15, beim Empfangen eines Pakets ferner umfassend:

Überwachen des Netzwerks hinsichtlich eines Pakets, das mit einem vordefinierten Muster übereinstimmt;
Herausfiltern eines geeigneten Pakets;
Weiterleiten des Pakets an eine Übertragungsschicht;
Einfügen der Dateneinheit in eine Empfangsschlange in Reaktion auf die Feststellung, dass das Paket eine Dateneinheit ist;
Konvertieren der Daten in das binäre Format;
Weiterleiten der binären Dateneinheit an die Validierungsschicht; und
Berechnen eines Paketschlüssels und Entschlüsseln der Dateneinheit.

17. Computerprogramm, das, wenn es auf einem Computer ausgeführt wird, bewirkt, dass der Computer ein Verfahren nach einem der Ansprüche 10 bis 16 ausführt.

Revendications

1. Centre de gestion (101) pour gérer un dispositif de réseau passif à partir d'un emplacement à distance sur un réseau informatique réparti, ledit centre de gestion étant configuré pour écouter le trafic de données sur un réseau de données et pour être transparent audit réseau de données, ledit centre de gestion étant configuré pour générer une demande fabriquée et pour pousser ladite demande fabriquée sur ledit réseau de données, ladite demande fabriquée comportant une adresse de source correspondant à un dispositif partenaire (100) et une adresse de destination correspondant à un dispositif coopérant (106) de sorte que ladite demande fabriquée puisse être acheminée vers ledit dispositif coopérant sur ledit réseau de données en tant que paquet légitime, ladite demande fabriquée comportant en outre un marqueur indiquant une relation avec ledit centre de gestion, ledit centre de gestion étant en outre configuré pour effectuer une écoute sur ledit réseau de données, pour reconnaître un marqueur sur une réponse fabriquée générée et poussée sur ledit réseau de données par un élément géré (105), ladite réponse fabriquée comportant une adresse de source correspondant audit dispositif coopérant et une adresse de destination correspondant audit dispositif partenaire, ladite réponse fabriquée comportant en outre un marqueur indiquant une relation avec un élément géré, et pour piéger les paquets de réponse fabriqués pour, de ce fait, échanger indirectement des informations avec l'élément géré sur ledit réseau de données.

2. Centre de gestion selon la revendication 1, dans lequel ledit centre de gestion comprend un fournisseur de service (400) comportant une couche hôte, une couche de transmission, une couche de validation et une couche de service de gestion.

3. Centre de gestion selon la revendication 2, dans lequel ladite couche de service de gestion est configurée pour concaténer un en-tête de gestion avec une unité de données reçue, ledit en-tête comprenant au moins un horodatage, une adresse de source et une adresse de destination.

4. Centre de gestion selon la revendication 2 ou 3, dans lequel le centre de gestion est configuré pour exécuter un processus d'application pour communiquer avec l'élément géré sur une interface de service qui définit une pluralité de primitives (411, 412, 413, 421, 422, 423).

5. Elément géré (105) destiné à être géré par un centre de gestion (101) à partir d'un emplacement à distance sur un réseau informatique réparti, ledit élément géré étant configuré pour écouter le trafic de données sur un réseau de données et pour être transparent audit réseau de données, ledit élément géré étant configuré pour effectuer une écoute sur ledit réseau de données, pour reconnaître un marqueur sur une demande fabriquée générée et poussée sur ledit réseau de données par un centre de gestion (101), ladite demande fabriquée comportant une adresse de source correspondant à un dispositif partenaire et une adresse de destination correspondant à un dispositif coopérant, ladite demande fabriquée comportant en outre un marqueur indiquant une relation avec ledit centre de gestion, et pour piéger la demande fabriquée, ledit élément géré étant en outre configuré pour générer une réponse fabriquée et pour pousser ladite réponse fabriquée sur ledit réseau de données, ladite réponse fabriquée com-

portant une adresse de source correspondant à un dispositif coopérant et une adresse de destination correspondant à un dispositif partenaire de sorte que ladite réponse fabriquée puisse être acheminée vers ledit dispositif partenaire sur ledit réseau de données en tant que paquet légitime, ladite réponse fabriquée comportant en outre un marqueur indiquant une relation avec ledit élément géré pour, de ce fait, échanger indirectement des informations avec le centre de gestion sur ledit réseau de données.

6. Elément géré selon la revendication 5, dans lequel ledit élément géré comprend un fournisseur de service comportant une couche hôte, une couche de transmission, une couche de validation et une couche de service de gestion.

7. Elément géré selon la revendication 6, dans lequel ladite couche de service de gestion est configurée pour concaténer un en-tête de gestion avec une unité de données reçue, ledit en-tête comprenant au moins un horodatage, une adresse de source et une adresse de destination.

8. Elément géré selon la revendication 6 ou 7, dans lequel l'élément géré est configuré pour exécuter un processus d'application pour communiquer avec le centre de gestion sur une interface de service qui définit une pluralité de primitives.

9. Elément géré selon l'une quelconque des revendications 5 à 8, dans lequel ledit élément géré est un dispositif de réseau passif.

10. Procédé pour gérer un dispositif de réseau passif à partir d'un emplacement à distance sur un réseau informatique réparti, le procédé consistant à :

écouter le trafic de données sur un canal de communication entre un dispositif partenaire et un dispositif coopérant sur un réseau de données et transparent au réseau de données ;
générer une demande fabriquée adressée audit dispositif coopérant et comportant une adresse de source dudit dispositif partenaire, ladite demande fabriquée comportant également un marqueur indiquant une relation avec un centre de gestion ;
détecter un marqueur sur une réponse fabriquée générée et poussée sur ledit réseau de données par un élément géré (105), ladite réponse fabriquée comportant une adresse de source correspondant audit dispositif coopérant et une adresse de destination correspondant audit dispositif partenaire, ladite réponse fabriquée comportant en outre un marqueur indiquant une relation avec un élément géré ; et
piéger ladite réponse fabriquée.

11. Procédé selon la revendication 10, consistant en outre à :

intercepter des informations non sollicitées adressées à l'un dudit dispositif partenaire et dudit dispositif coopérant par l'intermédiaire d'une primitive de réception de piège.

12. Procédé pour gérer un dispositif de réseau passif à partir d'un emplacement à distance sur un réseau informatique réparti, le procédé consistant à :

écouter le trafic de données sur un canal de communication entre un dispositif partenaire et un dispositif coopérant sur un réseau de données et transparent au réseau de données ;
détecter un marqueur sur une demande fabriquée générée et poussée sur ledit réseau de données par un centre de gestion (101), ladite demande fabriquée comportant une adresse de source correspondant audit dispositif partenaire et une adresse de destination correspondant audit dispositif coopérant, ladite demande fabriquée comportant en outre un marqueur indiquant une relation avec un centre de gestion ;
piéger ladite demande fabriquée ; et
générer une réponse fabriquée à ladite demande fabriquée, ladite réponse fabriquée étant adressée audit dispositif partenaire et comportant une adresse de source dudit dispositif coopérant, ladite réponse fabriquée comportant également un marqueur indiquant une relation avec ledit élément géré.

13. Procédé selon la revendication 12, consistant en outre à :

intercepter une primitive d'envoi de commande provenant dudit centre de gestion ; et
pousser une réponse sur le réseau avec une primitive d'envoi de réponse qui est destinée à être piégée par ledit centre de gestion.

14. Procédé selon la revendication 12 ou 13, consistant en outre à :

transporter des informations non sollicitées vers ledit centre de gestion en transportant des données adressées à l'un dudit dispositif partenaire et dudit dispositif coopérant en utilisant une primitive d'envoi de piège.

15. Procédé selon l'une quelconque des revendications 10 à 14, consistant en outre, lors de l'envoi d'un paquet, à :

concaténer un en-tête avec une unité de données, ledit en-tête comprenant au moins l'un

d'un horodatage, d'une adresse de destination et d'une adresse de source ;
acheminer l'en-tête et l'unité de données vers une couche de validation ;
joindre un code d'authentification audit paquet et chiffrer ledit paquet ;
transférer le paquet chiffré au format binaire à une couche de transmission ;
transformer ledit format binaire en ASCII et construire un paquet de réseau approprié pour une couche hôte ;
transférer le paquet de réseau à ladite couche hôte ; et
insérer ledit paquet de réseau dans une file d'attente de transmission.

16. Procédé selon l'une quelconque des revendications 10 à 15, consistant en outre, lors de la réception d'un paquet, à :

surveiller le réseau quant à un paquet correspondant à un motif prédéterminé ;
retirer par filtrage un paquet approprié ;
acheminer le paquet vers une couche de transmission ;
insérer, en réponse à la détermination du fait que le paquet est une unité de données, l'unité de données dans une file d'attente de réception ;
convertir l'unité de données au format binaire ;
acheminer l'unité de données binaire vers ladite couche de validation ; et
calculer une clé de paquet et déchiffrer l'unité de données.

17. Programme d'ordinateur qui, lorsqu'il est exécuté par un ordinateur, amène l'ordinateur à effectuer un procédé selon l'une quelconque des revendications 10 à 16.

FIG. 1
(PRIOR ART)

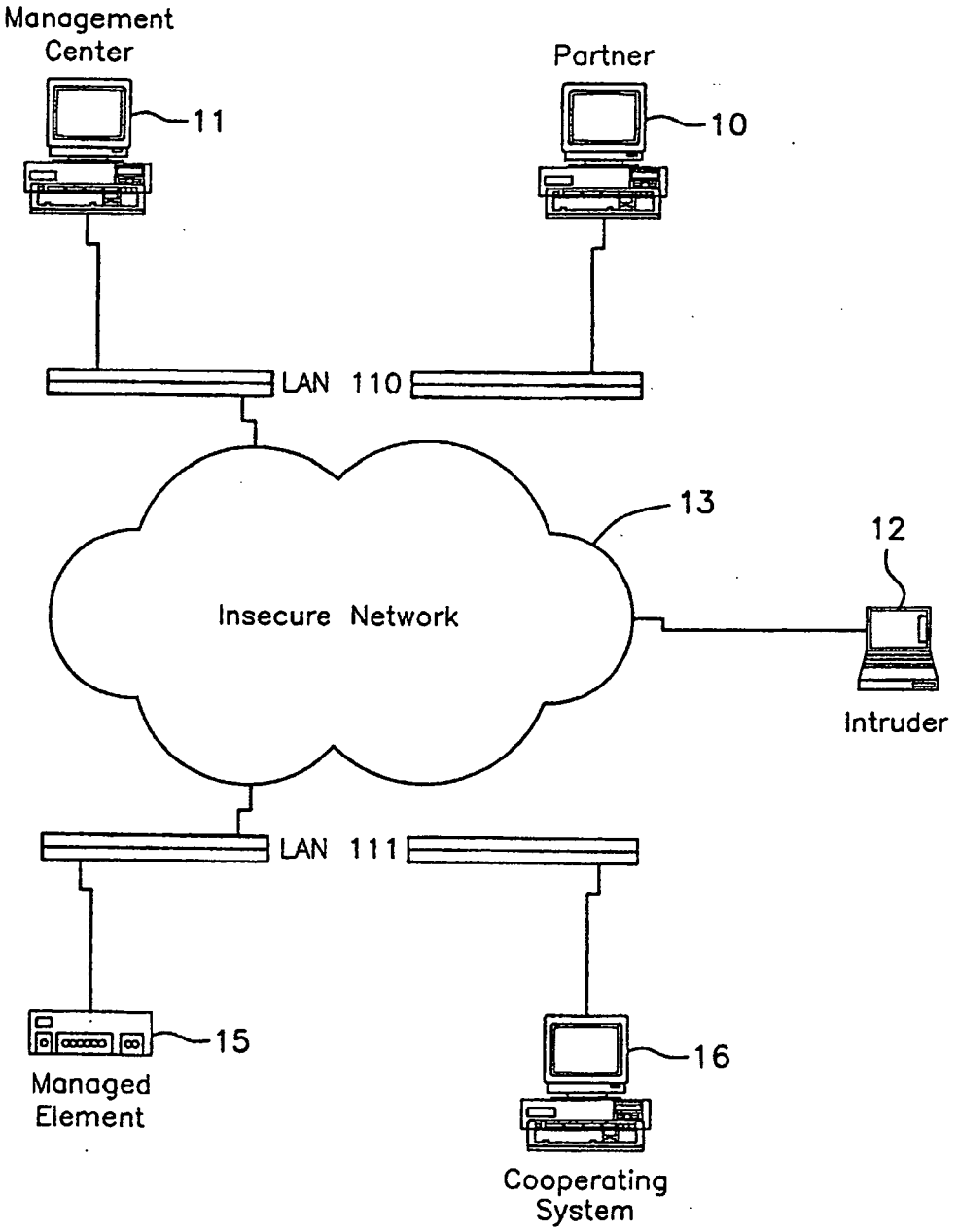


FIG. 2

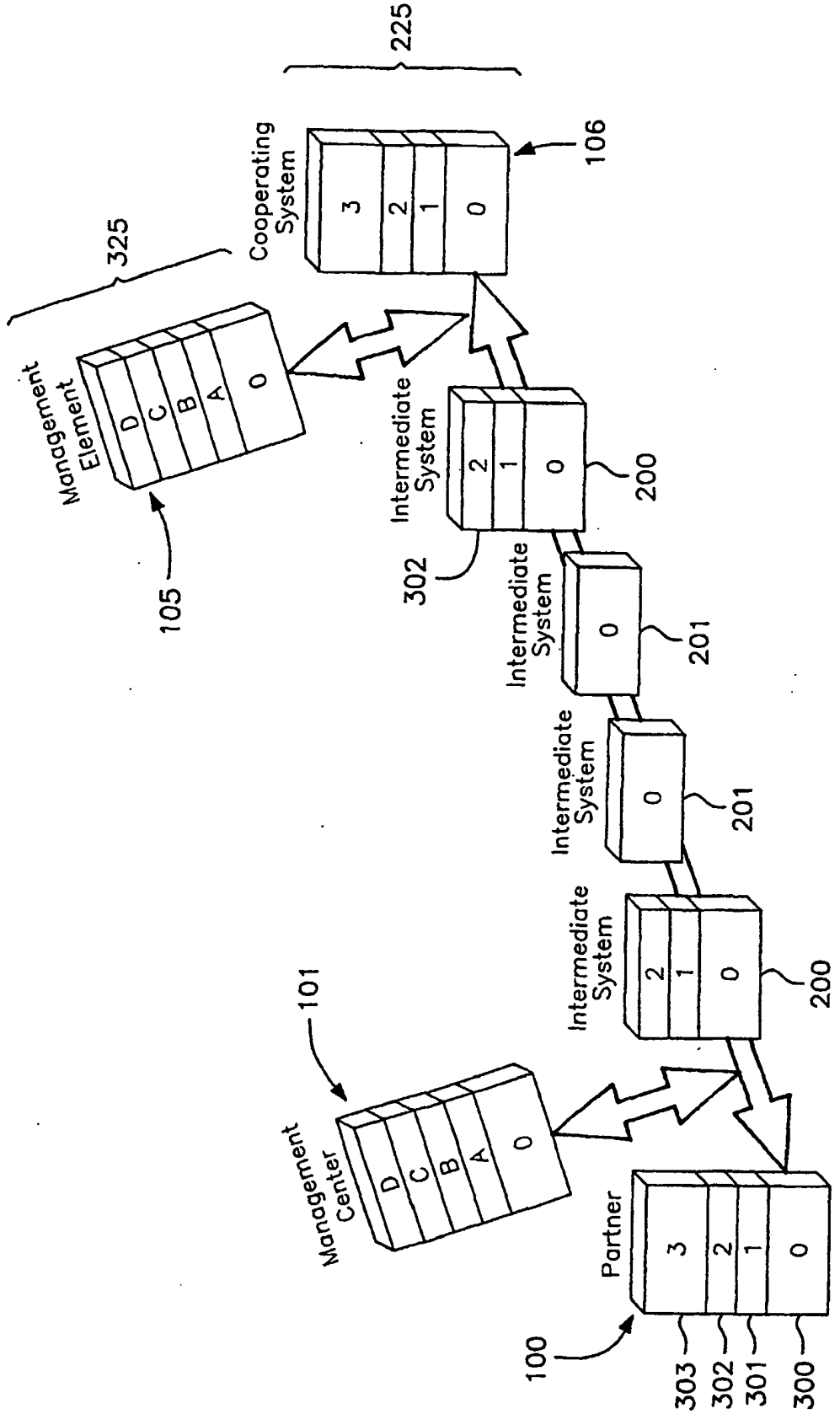

225
325
Cooperating System
3
2
1
0
106
Management Element
D
C
B
A
0
105
Intermediate System
2
1
0
200
302
Intermediate System
0
201
Intermediate System
0
201
Intermediate System
2
1
0
200
101
Management Center
D
C
B
A
0
Partner
3
2
1
0
100
303
302
301
300

FIG. 3

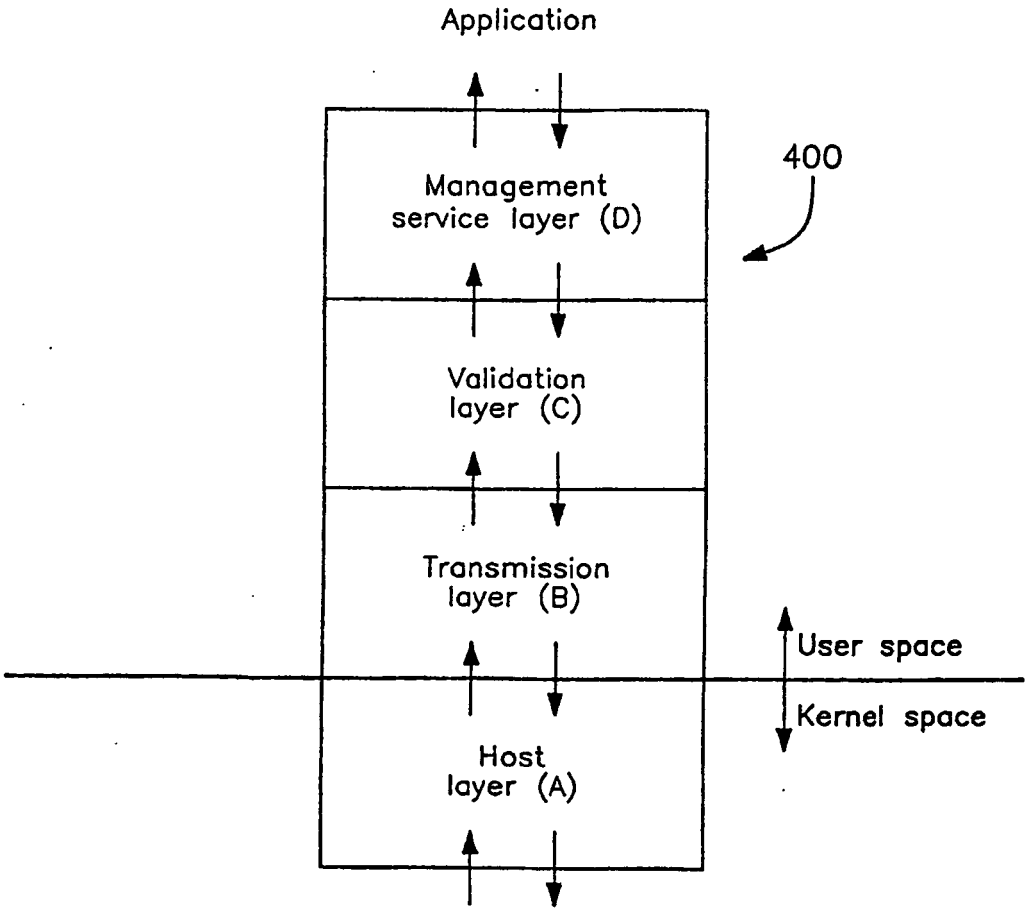

Application
400
Management service layer (D)
Validation layer (C)
Transmission layer (B)
User space
Kernel space
Host layer (A)

FIG. 4

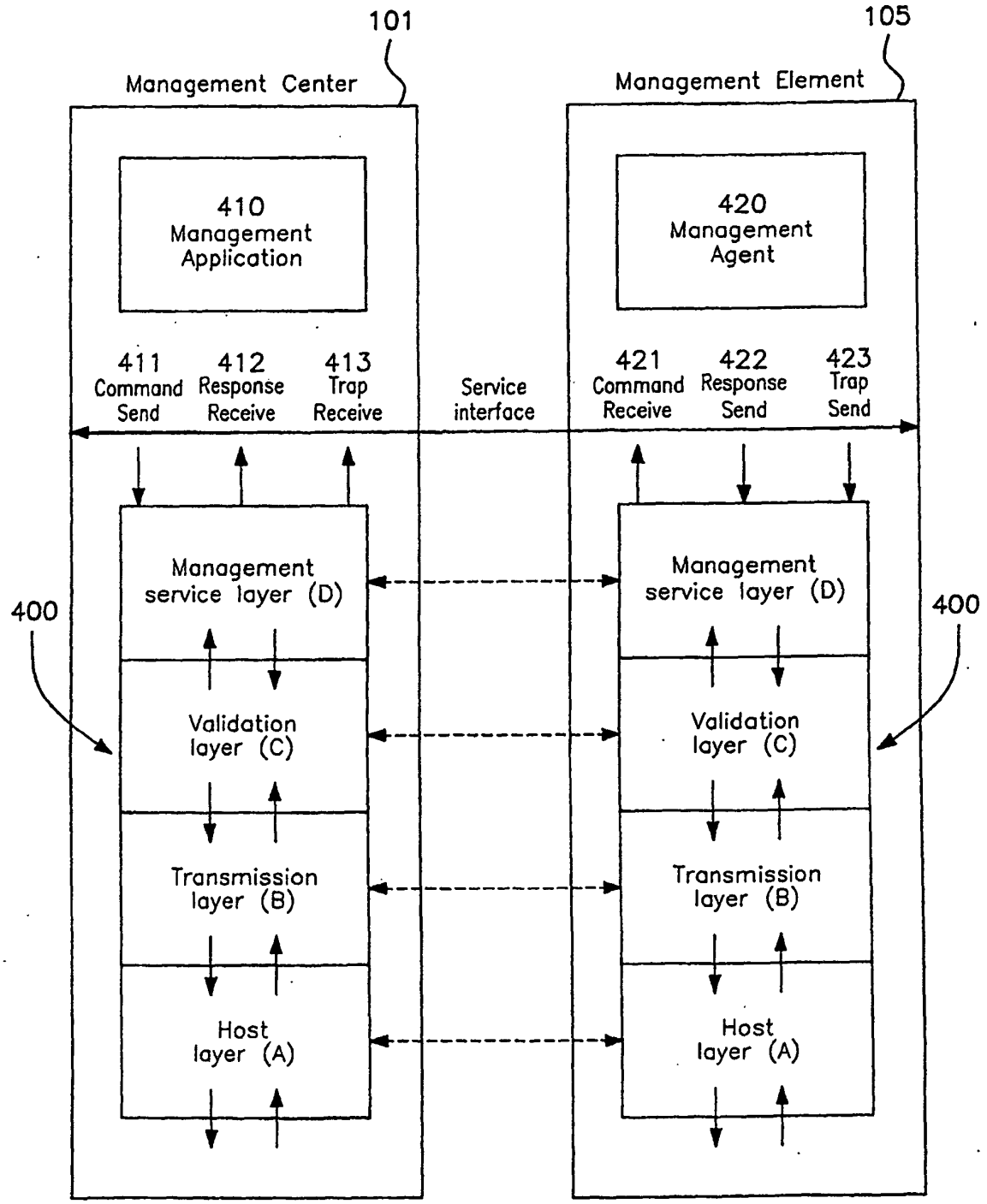

101
105
Management Center
Management Element
410
Management
Application
420
Management
Agent
411
Command
Send
412
Response
Receive
413
Trap
Receive
Service
interface
421
Command
Receive
422
Response
Send
423
Trap
Send
400
400
Management
service layer (D)
Management
service layer (D)
Validation
layer (C)
Validation
layer (C)
Transmission
layer (B)
Transmission
layer (B)
Host
layer (A)
Host
layer (A)

FIG. 5

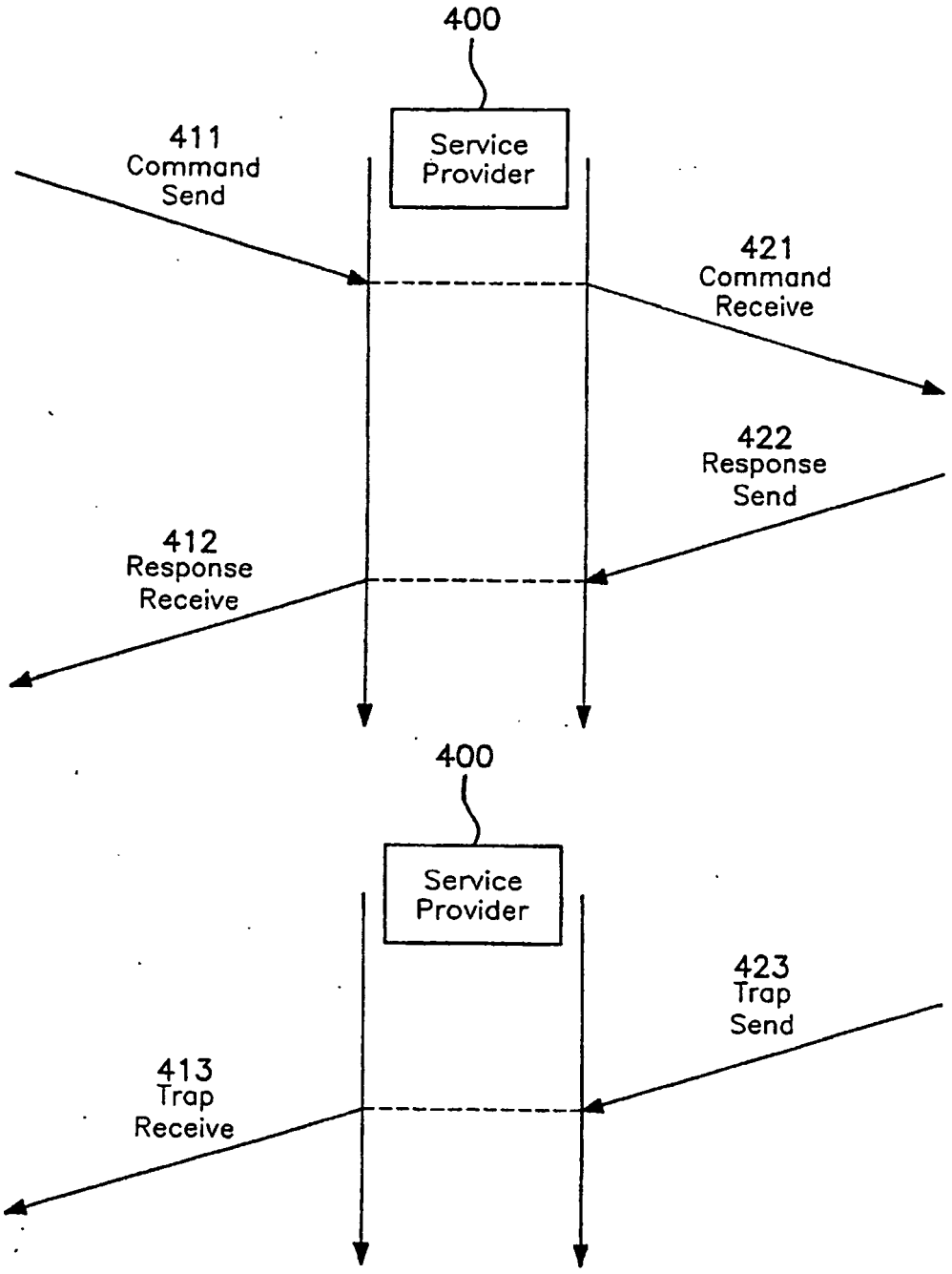

400
Service Provider
411 Command Send
421 Command Receive
422 Response Send
412 Response Receive
400
Service Provider
423 Trap Send
413 Trap Receive

FIG. 6

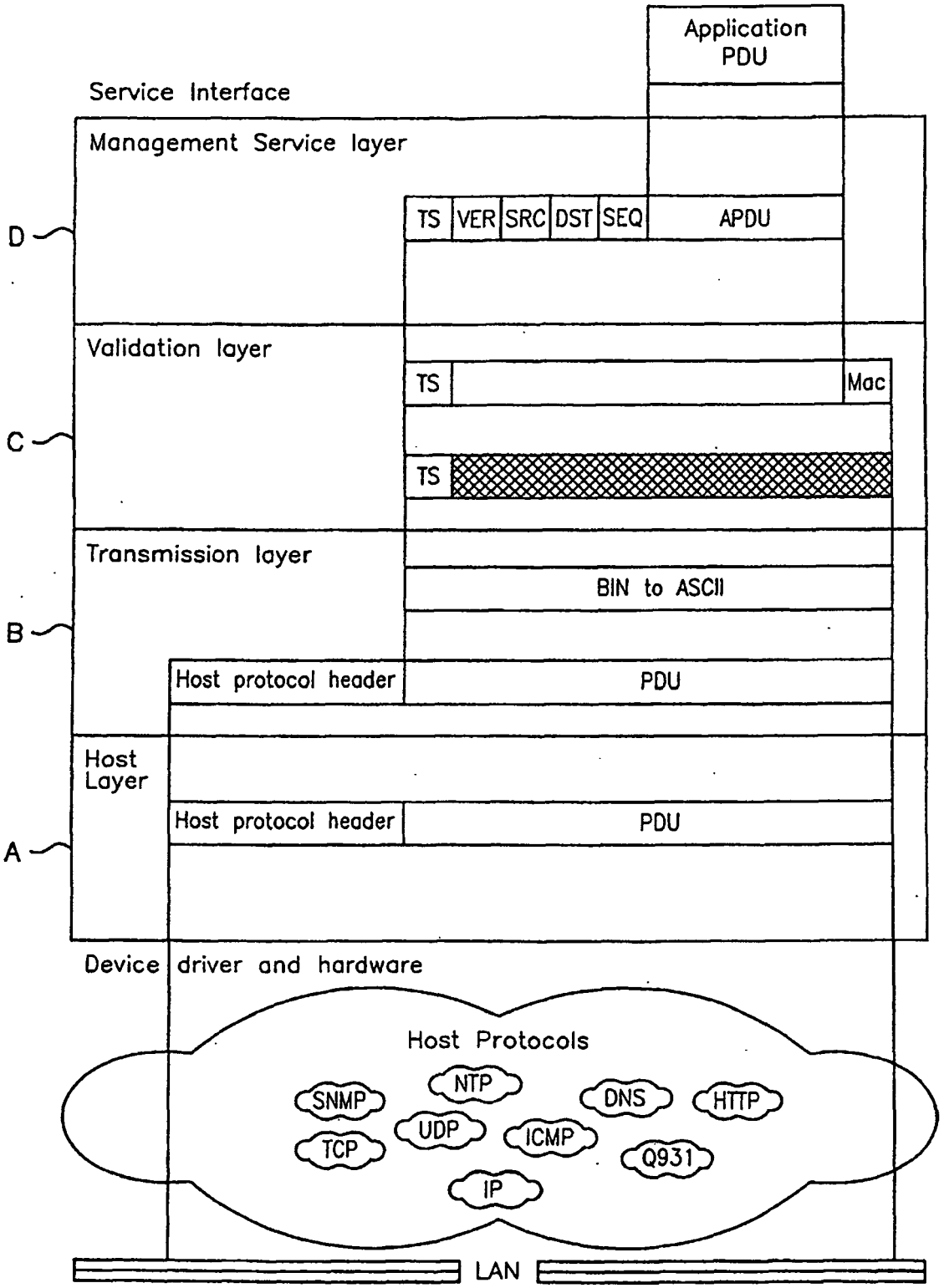

Application PDU
Service Interface
Management Service layer
TS
VER
SRC
DST
SEQ
APDU
D
Validation layer
TS
Mac
C
TS
Transmission layer
BIN to ASCII
B
Host protocol header
PDU
Host Layer
Host protocol header
PDU
A
Device driver and hardware
Host Protocols
SNMP
NTP
DNS
HTTP
UDP
TCP
ICMP
Q931
IP
LAN

FIG. 7A

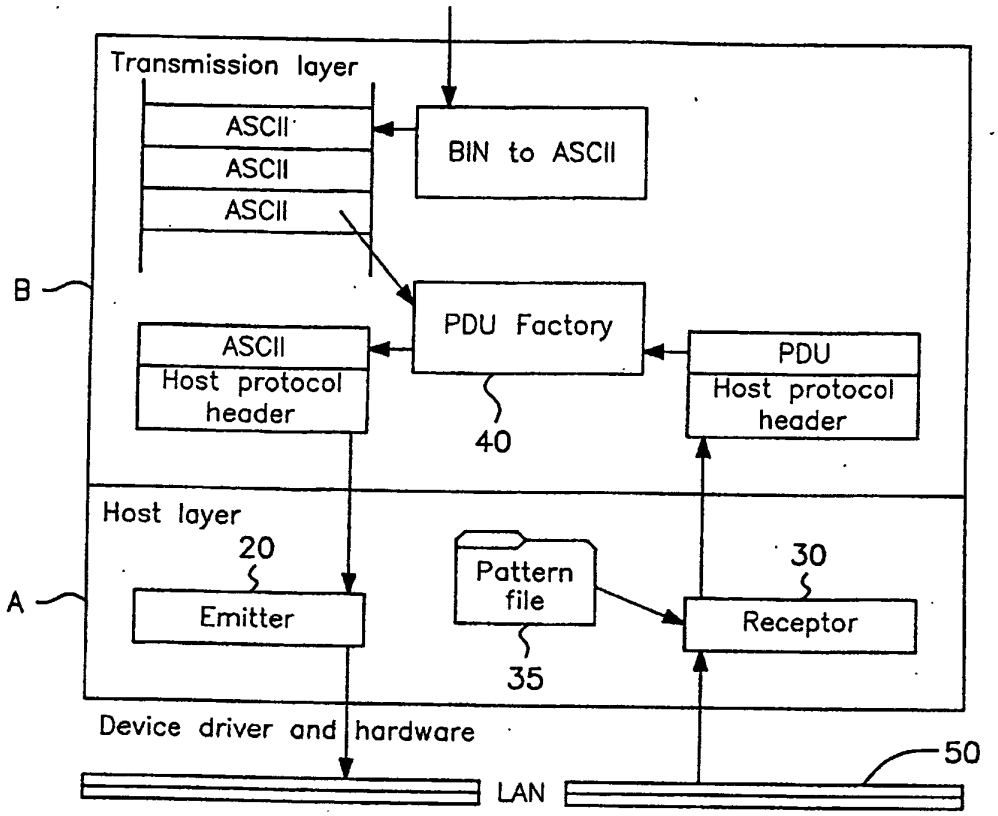
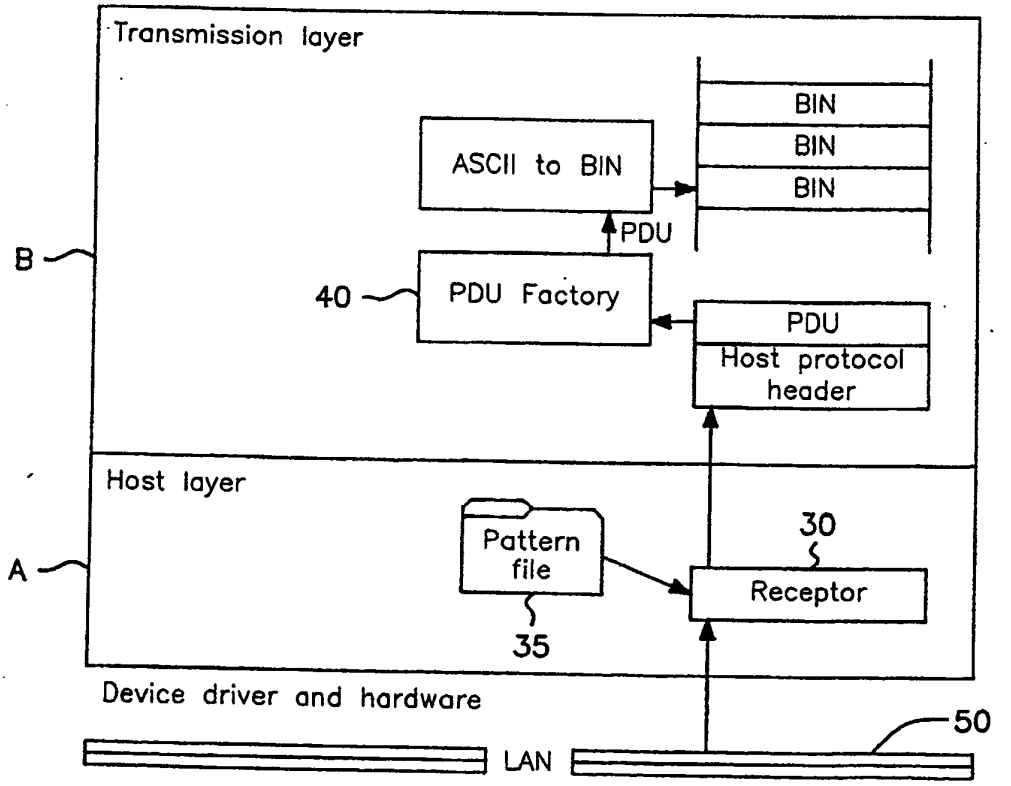

Transmission layer
ASCII
ASCII
ASCII
BIN to ASCII
B
PDU Factory
ASCII
Host protocol header
PDU
Host protocol header
40
Host layer
20
30
A
Emitter
Pattern file
Receptor
35
Device driver and hardware
50
LAN

FIG. 7B


Transmission layer
BIN
BIN
BIN
ASCII to BIN
PDU
B
40
PDU Factory
PDU
Host protocol header
Host layer
30
Pattern file
A
Receptor
35
Device driver and hardware
50
LAN