METHOD AND SYSTEM FOR MONITORING DATA COMMUNICATION

System Diagram:

- System Manager
- Management Bus
- HIGH SPEED BACKPLANE
- SHELF CONTROLLER
- PACKET SWITCH CARD
- AGW CARD

Abstract: Methods and systems for monitoring data communication are disclosed. One such method includes accessing a network platform via a user interface and communicating a command to the network platform via the user interface, where the command indicates a category of data to monitor. The method further includes identifying data packets in the network platform that correspond with the category of data to monitor and communicating the identified packets from the network platform to a collection agent.
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.
METHOD AND SYSTEM FOR MONITORING DATA COMMUNICATION

CROSS REFERENCE TO RELATED APPLICATIONS

This application is related to commonly assigned, co-pending U.S. Patent Applications Serial No. 11/003,546, filed on December 3, 2004 and entitled “Method and System for Decryption of Encrypted Packets”; Serial No. 11/003,841, also filed on December 3, 2004 and entitled “Method and System for Providing Packet Data Services”; and Serial No. 11/066,789, filed on February 24, 2005 and entitled “Method and System For Load Balancing in a Network Platform”; all to the same inventors as the instant application. The disclosures of U.S. Patent Application Nos. 11/003,546, 11/003,841 and 11/066,789 are incorporated herein by reference in their entirety.

BACKGROUND

I. Field

This disclosure is related to data communications and, more specifically, to monitoring data communication sessions.

II. Description of Related Art

The use of technology for accessing the Internet, the World Wide Web and/or other types of packet data networks (e.g., business or private networks) continues to increase at a rapid rate. The advent of wireless mobile devices, such as wireless phones, wireless personal digital assistants (PDAs) and wireless network enabled notebook computers, provides users of such devices with the ability to access data networks from any location where radio coverage facilitating such access is available. Such access may be provided using protocols such as the Mobile Internet Protocol (Mobile IP). Mobile IP functions may be implemented
in accordance with the Code Division Multiple Access (CDMA) 2000 standard, which is described in further detail in the Telecommunications Industry Association ("TIA") standards IS-95A and IS-95B, which are both incorporated herein by reference in their entirety. CDMA is also described in the International Telecommunications Union ("ITU") IMT-2000 series of standards, which are all incorporated herein by reference in their entirety. CDMA is further described in the TIA IS-2000 series of standards, which are all incorporated herein by reference in their entirety. The IS-2000 series of standards are commonly referred to as CDMA2000.

The rapid growth in the use of such techniques for accessing data networks has motivated the development of network systems that provide such data services with ever-increasing bandwidth. Additionally, rising infrastructure and operating costs associated with implementing and maintaining such networks (e.g., Mobile IP networks) has motivated the development of network devices and systems/platforms that may be employed in multiple applications and/or provide multiple functions concurrently. For example, the same network platform may provide both packet data serving node (PDSN) functions and/or home agent (HA) functions in a Mobile IP network. PDSN and HA services are described in detail in the CDMA2000 standards and will not be described in detail here. In mobile IP networks, it is common to use multiple devices and/or platforms for providing such services with the processing of communication sessions (calls) being distributed among the multiple devices and/or platforms. Additionally, with the development of higher bandwidth systems and increases in data network capabilities, there has been an associated increase in the quality of service expectations of users of these networks.

In order to provide users of such data networks (e.g., mobile IP networks) with an acceptable quality of service, service providers (and, in certain situations, users) of such data services use a number of techniques to increase the efficiency of the network devices and
platforms providing such services, so as to more effectively use the available bandwidth in providing their customers access to, for example, the Word Wide Web, the Internet and/or private networks.

One such technique is monitoring and analysis of data (collectively “data monitoring”), such as packet data, which is processed and communicated by the platforms of the communication network. Such monitor data may be used for a number of purposes. For example, communication monitor data may be used to test network platforms, to validate the operation of data networks and to troubleshoot communication problems in data networks. By viewing data communications that are processed in a network platform using such monitor data, network administrators, network engineers, or network users can gain valuable insight into the flow of data in such networks. Based on such data monitoring, changes to the configuration of a data network (and the network platforms included in the network) may be made in order resolve communication problems, correct the function of a network platform or to simply have data communication be accomplished more efficiently in the network.

Current approaches for data monitoring include using a menu driven interface that is implemented by a network platform. Using this interface, system administrators (or users of the system) can issue commands that indicate particular categories of data to monitor. For example, data communication associated with a particular data “call” (e.g., a data communication session associated with a specific user device) may be monitored. Alternatively, data communication between the network platform and another network platform or data communication of a specific communication protocol may be monitored. Of course, other types of data monitoring may be performed.

Using current approaches, in response to the command indicating a category of data to be monitored, the network platform (e.g., using an application card/packet-processing card) “taps” the appropriate communication session(s) in accordance with the command. Data
packets (or copies of those packets) that match a category of data being monitored (e.g., data packets associated with a particular call or protocol type) are then decoded to convert them from a transport protocol (e.g., Internet Protocol) format to a textual format, such as an American Standard Code for Information Interchange (ASCII) format. The textual (ASCII) format of the data packets is displayed via the user interface so that they may be readily analyzed by the system administrator and/or user.

Such approaches, however, have certain drawbacks. For example, the conversion of data packets from a transport protocol format to a textual format requires the use of string operations. Such operations are processor and memory intensive and, therefore, can adversely impact the performance of the network platform’s ability to provide data services to users of the network.

Another drawback of such approaches is that their functionality is generally limited so as not to consume too many resources (memory and/or processing resources) on the packet-processing cards. This limited functionality, however, results in such techniques not providing consistent decoding of packets. For example, because in certain communication protocols, packets have different formats depending on the direction they are traveling (e.g., Point-to-Point Protocol) and functionality limitations of current data monitoring approaches, decoding of such packets may differ according to the direction a given packet is traveling. For example, in one direction, packets may be decoded to a desired textual format, while packets traveling in the other direction are simply displayed in a hexadecimal form (e.g., transport protocol format) via the user interface. Based on the foregoing, alternative approaches for monitoring data communications in network platforms are desirable.

The foregoing examples of the related art and limitations related therewith are intended to be illustrative and not exclusive. Other limitations of the related art will become
apparent to those of skill in the art upon a reading of the specification and a study of the drawings.
SUMMARY

The following embodiments and aspects thereof are described and illustrated in conjunction with systems, tools and methods which are given by way of example and meant to be illustrative, not limiting in scope. In various embodiments, one or more of the above-described problems have been reduced or eliminated, while other embodiments are directed to other improvements.

An example method for monitoring data communications includes accessing a network platform via a user interface, such as a command line interface. The network platform (and user interface) may be accessed using, for example, a telnet or secure shell session. The method also includes communicating a command to a first packet-processing card of the network platform via the user interface. The command includes instructions for the network platform to perform a specific function related to monitoring data communications in the network platform. For example, the command may instruct the network platform to capture all data packets corresponding with a communication session associated with a specific user device (e.g., mobile station). In certain embodiments, the captured packets (e.g., portions of and/or copies of the packets) are then sent to a collection agent for storage and/or analysis.

After receiving the command, the first packet-processing card distributes the command to (i) a second packet-processing card in the network platform and; (ii) a packet-switch card in the network platform. The specific function indicated in the command is then performed using the first packet-processing card, the second packet-processing card or the packet-switch card, depending, at least, on the particular function indicated in the monitor command and the configuration of the network platform.

An example system for monitoring data communication includes a network platform for providing at least one of packet data serving node services and home agent services. In
operation, the network platform receives a command that instructs the network platform to perform a specific function related to monitoring data communication in the network platform. Such commands include, but are not limited to, commands that instruct the network platform to monitor (e.g., capture) (i) data packets corresponding with data communication of a specific protocol type, (ii) data packets corresponding with data communication associated with a specific other network platform, and (iii) data packets corresponding with data communication associated with a specific user device.

The example system also includes a collection agent coupled with the network platform. Depending on the particular embodiment, the collection agent may be implemented in a separate physical entity from the network platform or, alternatively, may be implemented as a separate functional entity in the network platform. The collection agent may include a packet storage module and a packet analyzer. The collection agent, in operation, receives packets from the network platform that are associated with one or more monitoring sessions (initiated by commands such as those described above) that are active on the network platform. The collection agent stores the received packets in a predetermined format that corresponds with the packet analyzer. The collection agent also applies the packet analyzer to the received packets to convert the stored packets to a textual format for analysis by a user. Application of the packet analyzer to the stored packets may be initiated, for example, in response to receiving one or more packets from the network platform or, alternatively, may be initiated by a user or in some other manner.
BRIEF DESCRIPTION OF THE DRAWINGS

Example embodiments are illustrated in referenced figures of the drawings. It is intended that the embodiments and figures disclosed herein are to be considered illustrative rather than restrictive.

Figure 1 is a diagram illustrating a communication network;

Figures 2A and 2B are two diagrams illustrating a backplane-based network platform for providing packet data serving node and/or home agent services in a data network;

Figure 3 is a block diagram illustrating a packet-processing card (e.g., wireless application card) of the platform shown in Figures 2A and 2B;

Figure 4 is a block diagram illustrating a packet-switch card of the platform shown in Figures 2A and 2B;

Figure 5 is a block diagram illustrating a collection agent that may be implemented in the network of Figure 1;

Figure 6 is a diagram illustrating example monitor commands;

Figure 7 is a diagram illustrating an example format of a captured packet as communicated to a collection agent;

Figure 8 is a flowchart illustrating a method for monitoring data communication; and

Figure 9 is a flowchart illustrating another method for monitoring data communication.
DETAILED DESCRIPTION

Embodiments of systems and methods for monitoring data communication are discussed generally in the context of wireless communication systems and packet data networks. However, it will be appreciated that these embodiments are illustrative and not limiting. Such techniques may be implemented in any number of types of communication systems, such as wired local area networks, and wired wide area networks, among any other type of appropriate data and/or communication networks. As in most telecommunication and data applications, it will also be appreciated that many of the elements of the various embodiments described herein are functional entities that may be implemented as hardware, firmware and/or software, or using any other appropriate technique. Additionally, many of the elements described in this disclosure may be implemented as discrete components or in conjunction with other components, in any suitable combination and location.

Organization of the Disclosure

This disclosure is organized as follows. First, a data network in which systems and methods for monitoring data communication may be implemented is described with reference to Figure 1. The network of Figure 1 includes a wireless data network that implements the Mobile IP protocol in accordance with the CDMA2000 standard. Second, a network platform with which the monitoring techniques described herein may be implemented is described with reference to Figures 2 – 4. The network platform of Figures 2 – 4 may be used in the system of Figure 1 to provide, for example, packet data serving node and/or home agent services in the data network. Third, a collection agent that is used in conjunction with the network platform of Figures 2 – 4 to implement data communication monitoring is described with reference to Figure 5. Fourth, example commands for initiating data monitoring will be described with respect to Figure 6. Fifth, an example packet format for
packets identified in a monitor session (captured packets) and communicated to a collection agent will be described with respect to Figure 7. Sixth, example embodiments of methods for monitoring data communication are described with reference to Figures 8 and 9.

**Data Communications Network**

Figure 1 shows a data communication network 100 that is used for packet data communication. In network 100, a mobile station 110 is a wireless device, such as a wireless phone, a wireless personal digital assistant (PDA), a wireless enabled computer, or any other appropriate device that may be used in conjunction with a wireless communication network for data communications.

The mobile station 110 communicates with a radio network over an air interface 115. The radio network includes a base transceiver station (BTS) 120 that directly communicates with the client station 110 over the air interface 115 using radio frequency signals. The mobile station 110 may communicate with the BTS 120 using a variety of different protocols. For example, such communication may be accomplished using the CDMA2000 standard. Other wireless protocols may also be used. For example, the mobile station 110 and the BTS 120 may communicate using Wideband CDMA (WCDMA), Time Division-Synchronous CDMA (TD-SCDMA), Advanced Mobile Phone Service (AMPS), Digital AMPS (D-AMPS), Universal Mobile Telecommunications System (UMTS), Global System for Mobile Communication (GSM), IS-136, Time Division Multiple Access (TDMA), IEEE 802.11, Bluetooth (e.g., 802.15.1), MMDS, DECT, integrated digital enhanced network (IDEN), general packet radio service (GPRS) or other protocols.

The BTS 120 is coupled with a base station controller (BSC) 125. The BSC 125 is further coupled with a Radio Access Network/Packet Control Function Device 130, which in turn is coupled with a packet-data-serving node (PDSN) 135. The PDSN 135 then connects
to a packet data network 140, such as the public Internet. These components and their operation are all described in further detail in the CDMA standards and will not be described in detail here for the purpose of brevity and clarity.

Using this connectivity, the mobile station 110 is then able to communicate with devices on the packet data network 140, as well as devices coupled with the packet network 140, such as a home agent (HA) 145, a Web server 155 and a private network 150, as some examples. The Web server 155 provides the mobile station 110 access to the World Wide Web.

The data network 100 shown in Figure 1 also includes a first collection agent 136 that is coupled with the PDSN 135 and a second collection agent 146 that is coupled with the HA 145. As was discussed above, the collection agents 136 and 146 may be implemented as separate physical entities from the PDSN 135 and the HA 145 or, alternatively, may be implemented as separate functional entities in the same physical platform(s) that implement the PDSN 135 and the HA 146. The collection agents 136 and 146 operate in conjunction with, respectively, the PDSN 136 and the HA 146 to implement data monitoring functions that overcome at least some of the drawbacks of current approaches described above. When processed by the PDSN 135 and the HA 145, data packets are examined to identify data packets that match specific criteria (e.g., criteria that are defined in one or monitor commands). The matching packets (e.g., copies of the packets or copies of portions of the packets) are sent to the respective collection agent 136 or 146. The process of identifying matching packets in the PDSN 135 and/or the HA 145 may be termed a monitor session or an active monitor session.

Decoding of the matching packets is then performed (e.g., real time or “offline”) using the collection agent or another device. In such an approach, application cards (packet-processing cards) of the PDSN 135 and the HA 146 do not implement packet decoding
functions. Therefore, such an approach reduces the performance impact on network platforms (e.g., the PDSN 135 and the HA 145) that results from the decoding packets for data monitoring sessions using prior approaches. Furthermore, because packet decoding is done by an entity other than the packet-processing cards, a more complex packet analyzer than those used in current approaches may be used without adversely impacting network performance. In such an approach, the shortcoming of inconsistent packet decoding due to, for example, the direction of travel of a packet may also be overcome by using a packet analyzer with increased functionality.

The data network of Figure 1 also includes a Remote Authentication Dial-In User Service (RADIUS) server 147 that is coupled with the HA 145. As is known, the RADIUS server 147 authenticates users, authorizes access to private networks and collects information for the purposes of accounting and billing (such as user access time and charges). RADIUS servers and their role in data networks implementing the Mobile IP and CDMA standards are described in more detail in the TIA IS-835-C standard.

Data communications in the data network 100 may be accomplished using communication tunnels. A communication tunnel is established in response to a call setup request. Such a communication tunnel may be established in accordance with the IS-835-C standard. Of course, other communication protocols are possible for establishing a communication tunnel. Briefly, for systems using the IS-835-C standard, a communication tunnel is setup by a mobile device sending a registration request (e.g., and A11 request to a PDSN). This request is processed by the PDSN and/or HA and if accepted, a generic routing encapsulation (GRE) tunnel is setup for the call. An A11 registration reply is then sent to the mobile device from the PDSN. The PDSN then negotiates point-to-point protocol (PPP) parameters with the mobile device via the GRE tunnel prior to setting up the complete call context. GRE tunnels may also be used to communicate captured packets from the PDSN.
135 to the collection agent 136 and from the HA 145 to the collection agent 146. Alternatively, any number of other types of communication tunnels may be used. For example, an Internet-Protocol-in-Internet-Protocol tunnel or a Universal Datagram Protocol tunnel may be used, as two examples.

Network services are provided by the various platforms of the network 100, such as the PDSN 135, the HA 145 and the Web Server 155, for example. However, for purposes of this disclosure, network platforms and methods for providing network services and monitoring data communication will be discussed generally in the context of the PDSN 135 and the HA 145. Of course, other types of network services, such as VPN services, may be provided in similar fashion as the embodiments disclosed herein.

**Backplane-based Network Platform**

Figures 2 – 4 illustrate a backplane-based network platform 200 that is used to provide PDSN and/or HA services and to implement (in conjunction with a collection agent) data monitoring services in a Mobile IP compliant data communication network, such as in the network 100 shown in Figure 1. The platform 200 may be used to implement the PDSN 135 of Figure 1 and/or the HA 145 of Figure 1. Due to its backplane-based design, the platform 200 is also able to provide both PDSN and HA services simultaneously. In such an application, PDSN services are provided using a first IP address while HA services are provided using a second IP address.

1. **Overview**

Backplane-based systems/platforms that may be used in a data network, such as network 100 of Figure 1, to provide network data services and to implement data monitoring
functions, typically include a high-speed backplane for communicating packet data and/or other data (such as monitor commands) from one packet-processing card to another in the same platform. It will be appreciated that data (e.g., monitor commands) may also be communicated in other ways in such a network platform, such as over a system management bus, for example.

One example of such a backplane-based network device is the Total Control 2000 (TC2K) available from UTStarcom, Inc., 1275 Harbor Bay Parkway, Alameda, California 94502. The backplane-based design of the TC2K system allows for all packet data traffic communicated to/from the system to be aggregated onto a single IP address. Specifically, the TC2K backplane-based system includes multiple wireless application processing cards (packet-processing cards) coupled, via a high speed-backplane, with a packet-switch card.

The packet-switch card performs packet routing and forwarding functions in the TC2K system. Because the packet-switch card is capable of routing packets to the individual wireless applications cards, the TC2K system is able to aggregate all of the data traffic for the system onto a single network address (e.g., an IP address in this example) or a reduced number of IP addresses, depending on the particular implementation. Therefore, all of the application cards in the TC2K system may operate using the same IP address, or a number of IP addresses that is less that the total number of wireless application (packet-processing) cards in the system. The packet-switch card routes packets to individual wireless application cards for processing based on the content of each packet.

For example, packets may be routed based on a communication session identifier (e.g., the source IP address of the packet) that is included in a header of each packet. After determining the communication session identifier from a specific packet, the packet-switch card determines the wireless application card responsible for processing packets associated with that specific communication session. The packet-switch card, by comparing the
communication system identifier from the packet to a table associating communication
session identifiers and wireless application cards, can make this determination, for example.

Also, improvements in data networking hardware (e.g., routers, servers, etc.) have
lead to corresponding increases in the data bandwidth that is available over a single network
collection. Data bandwidths of 1 gigabit per second on a single cable (1 gigabit = 1x10^9
bits) are currently readily available, with data bandwidths of 10 gigabits per second also
becoming more readily available. Such increases in the data bandwidth available on a single
network connection allow systems (such as the TC2K) implementing a single-IP address (or
fewer IP addresses than the total number of application cards in the system) to employ a
single network cable per IP address and still have even greater data bandwidth than previous
systems.

It may be desirable, however, to employ two network cables per IP address for
hardware redundancy and increased system reliability. For example, if an application card
that is operating as a network interface card (NIC) for the provision of PDSN services were to
fail, a second application card coupled with the redundant network cable could be activated in
its place, thus preventing a loss of network services.

A backplane based system (e.g., a TC2K system) may implement multiple network
services in the same platform (e.g., PDSN and HA functions), where each function is
provided using respective single network addresses. Such an approach allows for multiple
(e.g., redundant) devices, such as packet-processing cards capable of implementing PDSN
and HA functions, to be associated with each network address. In such an implementation,
should one device fail, another (redundant) device can nearly seamlessly take its place and
continue to provide network services without any perceptible service interruption from the
user's perspective.
In such backplane based systems, data communication processing is done in a distributed fashion. For example, communications session associated with the same IP address are often processed by separate packet-processing cards in the same network platform. Implementing data monitoring in such a system is also accomplished in a distributed fashion. For instance, a monitor command for initiating a monitor session may be communicated to one of the packet-processing cards in a backplane-based system. The packet-processing card that receives the monitor command then distributes that command to the other packet-processing cards and/or the packet-switch card in the network platform. Thus, when a monitor session is requested, the distribution of the monitor command ensures that packets matching criteria included in the command will be captured regardless of which packet-processing card (or packet-switch card) is responsible for processing those packets.

2. Architecture

Figures 2A and 2B illustrate two different representations of a backplane-based network platform/system 200. Figure 2A illustrates an exemplary chassis arrangement for a backplane-based network platform 200 for providing PDSN and/or HA services. The platform 200 is substantially similar to the UTStarcom TC2K wireless network platform. For purposes of this discussion, systems and methods for data monitoring will be generally discussed in the context of the TC2K system (e.g., the architecture illustrated in Figures 2A and 2B). Of course, other system architectures are possible.

The platform 200 includes a shelf controller card 210. While the platform 200 is illustrated with a single shelf controller 210, it will be appreciated that additional shelf controller cards may be implemented in the platform 200. For example, the UTStarcom TC2K platform includes two shelf controllers. The shelf controller provides hardware management for the platform 200 and provides low-speed Ethernet connectivity (e.g., 100
Mbps) between the components of the platform 200. For example, the shelf controller recognizes when a card (e.g., packet-switch card or packet-processing card) is inserted or removed from the platform 200 and, accordingly, applies or removes power from the respective card slots. This functionality allows for the packet-processing and packet-switch cards to be "hot-swapped" (e.g., removed and replaced while the system is in operation).

The platform 200 also includes a system manager card 230. As with the shelf controller card 210, the platform 200 is illustrated with a single system manager card 230. However, additional system manager cards may be included in the platform 200, such as for redundancy purposes. The system manager card 230 is coupled with a system management bus (not shown in Figure 2A) and provides for configuring the components of the platform 200. For example, the system manager card 230 is used to establish the type of service or services the platform 200 is to provide. Using the system manager 230, the platform 200 is configured to provide HA services, PDSN services or both. In the UTStarcom TC2K platform, system management is accomplished over a 100 Mbps data bus (the system management bus) using the Simple Network Management Protocol (which is described in detail in the IETF's RFC 1157), as well as UTStarcom defined proprietary communication mechanisms. RFC 1157 is incorporated by reference herein in its entirety.

The system manager card 230 may also implement a user interface, e.g., a command line interface (CLI), for receiving monitor commands. A user and or system administrator may access the user interface via a telnet or secure shell session. Such sessions are known and will not be described in detail here. Once connected with the system manager card 230, a user can "attach" to a specific packet-processing card of the system and communicate a monitor command to that packet-processing card over the system management bus.

The platform 200 also includes a packet-switch card 220. As with the shelf controller 210 and the system manager card 230, the platform 200 is shown with a single packet-switch
card 200 for purposes of illustration. It will be appreciated that additional, redundant packet-switch cards may be included in the platform 200. The TC2K system typically includes two packet-switch cards.

The packet-switch card 220 operates as a distribution point for data packets in the platform 200. Packets that are received by the packet-switch card 220 are routed or forwarded to a destination (e.g., for processing or egress from the platform 200). For packets being processed in the platform 200, the packet-switch card 220 will examine each packet and communicate the individual packets to a respective access gateway (AGW) card of a plurality of AGW cards 240, 245 and 250 (packet-processing devices/cards or wireless application processing cards) based on this examination. As indicated by the dotted lines in Figure 2A, the platform 200 may contain additional AGW cards. The AGW card to which a particular packet is routed depends on the type of packet and/or information contained in the packet headers, such as information contained in one or more of the Layer 2 to Layer 7 headers of Internet Protocol packets.

If any data monitoring sessions are active in the platform 200, the packet-switch card 220 also examines data packets it receives to determine if the packets match any of the criteria that has been specified for the active monitoring sessions. This determination may also be made based on an examination of the packets' headers. If a packet matching any of the monitoring session criteria is found, the packet-switch 220 captures the matching packet (e.g., copies the packet, or a portion of the packet) and communicates the captured packet to a collection agent, such as via a GRE tunnel established between the platform 200 and the collection agent.

Figure 2B illustrates the platform 200 in a block diagram. As shown in Figure 2B, the platform 200 includes a high-speed backplane 270 and a system management bus 280 (alternatively system control bus). The packet-switch card 220 and the AGW cards 240, 245
and 250 are coupled with the backplane 270. The combination of the packet-switch card 220 and the high-speed backplane 270 are referred to as a Media Data Bus (MDB) in the TC2K platform. The MDB is capable of handling gigabit Ethernet communication between the packet-switch card 220 and the AGW cards 240 – 250. Packets being processed by the platform 200 are communicated via the MDB.

In Figure 2B, the shelf controller card 210 and the system manager card 230 are coupled with the system management bus 280 (which may also be termed a system control bus), while the system management bus 280 is in turn coupled with each of the AGW cards 240 – 250. As was discussed above, shelf controller card 210 implements hardware management functions for the platform 200 and provides low-speed Ethernet connectivity (e.g., 100 Mbps) between the components of the platform 200. As was also discussed above, the system manager 230, via the management bus 280, configures the platform 200 in accordance with the services the platform is to provide. Monitor commands may be distributed in the platform 200 via the system management bus 280 or, alternatively, via the MDB.

3. Access Gateway Card (Packet-processing Card)

Figure 3 illustrates the AGW Card 240 of the platform 200 in further detail. As shown in Figure 3, the AGW card 240 is coupled with the high-speed backplane 270 and the system management bus 280, as has been previously discussed. The AGW card 240 includes a Layer 2 (L2) Ethernet switch 300 that is coupled with the high-speed backplane 270. The L2 switch 300 receives packet data communicated to the AGW card 240 from the packet-switch card 220 (via the backplane 270). Additionally, the L2 switch 300 communicates packet data that is being sent from the AGW card 240 to the packet-switch card 220 onto the high-speed backplane 270. This communication is accomplished in accordance with any
number of various data communication protocols, such as the Ethernet standard, for example. When the AGW card 240 is configured to communicate data between the network and the packet-switch card, it may be said to be functioning as a NIC.

As was discussed above, processing of data packets in the platform 200 is accomplished in a distributed fashion. For example, the packet-switch 220 sends data packets to the AGW cards of the platform 200 that are dedicated to providing certain network services. For example, the packet-switch card 220 sends packets for PDSN processing to the AGW cards in the platform 200 that are designated to perform PDSN processing.

The packet-switch card 220 determines the AGW card of the platform 200 that is responsible for processing each packet. For example, the packet-switch card 220 may examine the headers of a data packet and determine that the packet is part of a communication session (e.g., based on the source IP address of the packet) for which the platform 200 is providing PDSN services. Based on the communication session identifier (e.g., the source IP address), the packet-switch card 220 forwards the packet to the AGW card that is responsible for providing PDSN services for that particular communication session. As an example, the packet-switch card 220 may modify the Ethernet header of the packet (e.g., by inserting an MPLS header) to indicate that the AGW card 240 is the intended destination of the packet and then forward the packet to the AGW card 240.

Once a packet is received at the AGW card 240, the L2 switch 300 examines the Ethernet header of the packet and determines that the AGW card 240 is the destination. The L2 switch 300 of the AGW card 240 then sends the data packet to the controller 310, which processes the packet (e.g., performing Point-to-Point Protocol processing, as described in the IETF's RFCs 1661, 1662 or Generic Route Encapsulation Protocol processing, such as described in the IETF's RFC 2784) to produce a processed packet.
If one or monitor sessions are active on the AGW card 240, information in the packet (e.g., the packet's headers) is also examined to determine if it matches any criteria of the active monitoring sessions. If the packet matches any of the criteria, a copy of the packet (or a portion of the packet) is made to be sent to a collection agent, such as via a GRE tunnel.

The controller 310 then sends the processed packet to the L2 switch 300 to be communicated to the packet-switch card 220 via the backplane 270. AGW cards that are used for providing network services (e.g., PDSN services, HA services, or any number of other data services) are said to be operating as NACs.

The AGW card 240 further includes an Ethernet port 330. The Ethernet port 330 may be coupled with an external network cable to allow the AGW card 240 to provide for data ingress and egress from the platform 200, such as to/from other network platforms and/or to a collection agent. In this situation, the AGW card 240 would be said to be functioning as a line card (NIC) and may not provide any packet processing or data monitoring services in the platform 200. In this situation, the L2 switch 300 effectively shunts the Ethernet port 330 with the high-speed backplane 270. As was noted above, all of the AGW cards (packet-processing cards) in the platform 200 may operate using a single-IP (network) address, with each AGW card being responsible for processing data packets associated with a specific, respective communication session or sessions.

The AGW card 240 additionally includes a packet buffer 340 that is coupled with the controller 310. The packet buffer 340 is used to buffer data packets at the AGW card 240 in the event those packets arrive at the AGW card 240 out of order. Data packets may arrive out of order for any number of reasons, such as a result of network congestion or distributed processing within the platform 200. In the event such out of order arrival occurs, the buffer 340 holds the packets until a contiguous sequence of packets is present. The controller 310 then reorders the packets and processes them in sequence.
It will be appreciated that the AGW cards (e.g., the AGW card 240) of the platform 200 may operate in a number of fashions. Specifically, the AGW cards may operate as a NIC only, operate as a NAC only, or may operate as both a NIC and a NAC in the same system. Specifically, a data packet may be received from a data network by the AGW card 240. That packet is then sent to the packet-switch card 220. The packet-switch card 220 may then send the packet back to the AGW card 240 for PDSN or HA processing and comparison with active monitoring session criteria. The AGW card 240 then sends the processed packet back to the packet-switch card 220. The packet-switch card 220 may then send the packet back to the AGW card 240 for egress from the platform 200 (e.g. for communication to a destination via the network). In this situation, the AGW card 240 is operating as both a NIC and a NAC in providing network services.

The AGW card 240 may also operate so as to provide a data output port for communicating captured packets to a collection agent. In such an approach, the AGW card 240 would operate so as to communicate captured packets for any active monitor sessions in the platform 200 to the collection agent, e.g., via a tunnel. In this situation, the AGW card 240 may or may not provide network data services in the platform 200, depending on the particular application.

4. Packet-switch card

Figure 4 illustrates the packet-switch card 220 of the platform 200 in further detail. As is shown in Figure 4, the packet-switch card 220 is coupled with the high-speed backplane 270 via a switch fabric 400. As has been previously described, the packet-switch card 220 communicates packet data with (to and from) the AGW cards of the platform 200 via the MDB (which includes the packet-switch card 220 and the backplane 270). The switch fabric 400 may be implemented using one or more L2 switch components arranged in any suitable
fashion in the packet-switch card. The switch fabric 400 communicates, via the MDB, to receive and transmit packet data in the platform 200.

The packet-switch card 220 further includes a programmable controller 420. The controller 420 may take the form of any appropriate instruction-processing device such as, but not limited to, a microcontroller, a microprocessor or a network processor. The controller 420 makes routing and forwarding decisions for data packets received by the packet-switch card 220.

The packet-switch card 220 additionally includes a network interface 430 (e.g., an Ethernet port or optical data port) that may serve as a packet data ingress/egress point for the platform 200. Alternatively, data ingress/egress for the platform 200 is accomplished through one or more of the AGW cards that are operating as NICs, as was discussed above. In either situation, for the system 200, data packets entering the platform 200 are routed to the packet-switch card 220. Once a data packet is received by the packet-switch card 220, the packet is examined by the controller 420, which determines which AGW card of the platform 200 to route the packet to for processing.

When a data packet is received at the packet-switch card 220, the packet-switch card 220 examines the data packet's headers (e.g. using the controller 420) to determine, for example, an identifier for a communication session with which the data packet is associated. The controller 420 then determines which AGW card of the platform 200 is responsible for processing packets for the determined communication session. This determination may be made by consulting a table that associates communication sessions that the platform 200 is servicing with the respective AGW cards responsible for processing those sessions. Such a table may be stored and maintained in the controller 420, for example. Alternatively, a list of the communication sessions and their associated AGW cards may be stored in a separate component in the packet-switch card 220, such as in a memory device (not shown) coupled
with the controller 420. It will be appreciated that other information in the data packet’s headers may be used to determine which AGW card is responsible for processing the packet.

If one or monitor sessions are active on the packet-switch card 220, the packet is also examined to determine if it matches any of the criteria of the active monitoring sessions. If the packet matches any of the criteria, a copy of the packet (or a portion of the packet) is made and sent to a collection agent via, for example, a GRE tunnel.

After determining which AGW card is responsible for processing the data packet, comparing the packet to active monitoring session criteria and capturing the packet, if appropriate, the packet-switch card 220 forwards the data packet to the responsible AGW card for processing (e.g., HA or PDSN processing) after which the AGW card returns the packet to the packet-switch card 220. Additional packet processing may then be performed in a similar fashion.

Once the processing of the packet is complete, the packet-switch card 220 receives a completed packet. Based on an examination of the headers of the completed packet, the packet-switch card 220 determines that processing of the packet is complete and strips out any remaining MPLS headers and/or labels that were inserted during processing. The packet-switch card 220 then modifies the Ethernet header appropriately and routes the completed packet to the destination address indicated in the headers (e.g., via the packet-switch card 220’s network interface or via an AGW card operating as a NIC, depending on the particular embodiment). Also, depending on the criteria of any active monitoring sessions, the processed packet may be captured and sent to a collection agent.

**Collection Agent**

Referring now to Figure 5, a block diagram illustrating a collection agent 500 that may be implemented as the collection agents 136 and 146 in Figure 1 is shown. The
collection agent 500 includes a first communication interface 510 that provides connectivity with a PDSN and/or HA. The communication interface 510 is used to receive captured packets from the PDSN and/or HA for data monitoring sessions being executed on the PDSN and/or HA. The communication interface 510 may implement one or communication tunnels for receiving packets from the PDSN and/or HA, where each tunnel corresponds with a respective data monitoring session. By implementing separate tunnels (e.g., GRE tunnels) for each active monitoring session, the collection agent can easily identify the monitoring session with which a specific captured packet is associated by determining its tunnel identifier from a header (e.g., GRE header) included with the captured packet.

In the collection agent 500, a packet storage module 520 is used to store (save) captured packets. Captured packets are processed by the packet storage module 520 (e.g., removing headers associated with communication of the packet from the PDSN or HA to the collection agent) and the captured packets are stored, such as on a hard disk drive or optical data storage device, in a predetermined format. The predetermined format is typically a format that is compatible with a packet analyzer application 530 that is also included in the collection agent 500. Any number of formats may be used to store the captured packets and the particular format will depend on the particular packet analyzer 530 that is used. As one example, packets may be stored in Berkeley Packet Capture (PCAP) format. The PCAP format is described in detail in ..., which is incorporated by reference herein in its entirety. (*We should discuss a reference that describes PCAP.*)

The packet analyzer 530 may also take any number of forms. For example, the packet analyzer 530 may be implemented using the Ethereal network protocol analyzer, which is an open source (GNU public license) application that is readily available over the Internet. The Ethereal network protocol analyzer converts captured packets from the format in which they were stored (e.g., PCAP) by the collection agent 500 to a form that is readable by a user.
and/or a system administrator. The readable format typically includes a textual representation of the packets that may be, for example, in ASCII format, or in any other appropriate format.

The collection agent 500 also includes a second communication interface 540 for communicating with a user terminal (not shown). The user terminal may be directly coupled with the collection agent 500 or, alternatively, the user terminal may access the collection agent 500 remotely through a data network, for example. The user terminal is used to display the converted packets as produced by the packet analyzer 530. It will be appreciated that the particular arrangement of the various elements of the collection agent 500 are shown for purposes of illustration and the collection agent 500 may be configured in any number of ways. For example, a single communication interface could be used for both receiving captured packets from a network platform and for communicating with a user terminal. As a further alternative, the packet analyzer 530 could reside on the user terminal. In such a situation, the stored packets would be communicated from the collection agent to the user terminal, e.g., via the communication interface 540. In such an approach, conversion of the stored packets to a readable format would then be done on the user terminal. Of course, any number of other possible approaches and/or configurations may be used.

**Monitor Commands**

Figures 6A – 6D illustrate example formats of monitor commands that may be used to initiate monitor sessions in a network platform, such as the network platform 200 shown in Figures 2 – 4. Referring to Figure 6A, a first form of a monitor command 600 is shown. The monitor command 600 includes a command prefix 605 “MONITOR PROTOCOL” that is recognized by the packet-processing cards and the packet-switch card 220 of the platform 200 as a command to initiate a data monitoring session.
The monitor command 600 also includes a communication protocol field 610. The communication protocol field 610 is used to indicate the communication protocol that is desired to be monitored in a data monitoring session that will be initiated by the monitor command 600. There are numerous communication protocols that may be designated in the communication protocol field 610. For example, the communication protocol could be designated as the Mobile Internet Protocol, the Point-to-Point Protocol, or any number of other possible data communication protocols.

The monitor command 600 further includes a network platform address field 615 that is used to designate a network address of a platform (other than the network platform 200) for which data communication associated with that platform is to be monitored. For the network platform 200, the packet-switch card 220 is used to implement such monitoring sessions because the packets corresponding with the monitor command 600 will typically not be associated with a particular communication session.

For example, referring again to Figure 1, if a monitoring session is initiated on the PDSN 135 using monitor command 600, where the network platform address field 615 designates the network address of the HA 145, packets matching this criteria would include all packets communicated between the PDSN 135 and the HA 145. These packets could be associated with any number of communication sessions and would likely be processed by different packet-processing cards in the PDSN 135. However, due to the distributed processing of packets in the platform 200, all of these data packets will be routed through the packet-switch card 220. Therefore, implementing the monitor session requested by the monitor command 600 in this fashion will provide for identifying (and capturing) these packets.

The monitor command 600 also includes a timeout parameter field 620. The timeout parameter 620 is used to specify a length of time that a monitoring session will be active.
Alternatively, the timeout parameter included in the field 620 may indicated how long a monitor session should be kept open after receipt of a packet. In this situation, each time a packet is identified and captured for a particular monitoring session, the timeout period for that monitoring session would start over. The time duration specified in the timeout parameter field 620 may be provided in any number of different forms, such as seconds, hours or fractions of an hour, as some examples.

In certain embodiments, a range of acceptable timeout values may be specified. In such approaches, if the timeout value included in the monitor command is not within the specified range, a user entering the command may be notified via the user interface (e.g., the CLI interface implemented by the system manager card 230) that the monitor command entered is invalid.

In other embodiments, if the timeout parameter is designated as zero "0", the monitor session initiated by the command will be active until canceled by a subsequent command. Commands for canceling a monitor session may also take any number of forms. As one example, the command prefix could be "UNMONITOR" followed by the same designations of communication protocol and network platform address that were included in the monitor command 600. This UNMONITOR command would instruct the network platform (e.g., the packet-switch card 220) to terminate a monitoring session that was initiated in response to the monitor command 600. Alternatively, each monitor session could be assigned a session identification and the UNMONITOR command could designate this monitor session identification to terminate the corresponding monitor session.

Figure 6B illustrates another form of a monitor command 625 that may be used to initiate a monitoring session in the network platform 200. The monitor command 625, in like fashion as the monitor command 600, includes the command prefix field 605, the communication protocol field 610 and the timeout parameter field 620. The monitor
command 625 also includes a tunnel identification field 630, rather than the network platform address field 615. The monitor command 625 may be used to initiate a monitor session that captures packets that are communicated in a tunnel corresponding with the tunnel identification field 630. As with the monitor command 600, packets meeting the criteria of the monitor command 625 may be associated with any number of communication sessions. Therefore, a monitor session initiated by the monitor command 625 would also be implemented by the packet-switch card 220 in the network platform 200 for the same reasons described above with respect to the monitor command 600.

Figure 6C illustrates yet another form of a monitor command 635 that may be used to initiate monitoring sessions in the network platform 200. The monitor command 635, in like fashion as the monitor commands 600 and 625, includes the command prefix 605, the communication protocol field 610 and the timeout parameter field 620. The monitor command 635 also includes a mobile identification field 640. The mobile identification field 640 is used to specify a particular client device for which data communication is to be monitored, such as a mobile device. The mobile identification field 640 may take a number of forms. For example, the mobile identification field 640 may include an International Mobile Subscriber Identification number corresponding with the mobile device. Alternatively, the mobile identification field 640 may include an Internet Protocol address or a network address identifier of the mobile device.

A monitor session that is initiated in response to the monitor command 635 will be implemented on the packet-processing card that is responsible for processing packets for a corresponding communication session of the mobile device. Packets corresponding with that communication session are identified by the responsible packet-processing card as matching the criteria of the monitor session initiated by the monitor command 635, as was described
above. The identified packets would then be captured by the responsible packet-processing card and sent to the collection agent, as has also been described above.

Figure 6D illustrates yet another form of a monitor command 645. The monitor command 645 includes only the command prefix field 605, the communication protocol field 610 and the timeout parameter field 620. A data monitoring session that is initiated by the monitor command 645 will capture all packets that correspond with the communication protocol indicated in the communication protocol field 610. For similar reasons as those discussed above with respect to the monitor commands 600 and 625, a monitor session initiated in the platform 200 in response to the monitor command 645 will be implemented by the packet-switch card 220.

The monitor command 645 may be used to initiate monitor sessions that monitor specific types of data communication that occur relatively infrequently as compared to other data communication protocols. For example, the monitor command 645 may be used to initiate a data monitoring session to capture all data communication associated with RADIUS server accounting functions, for example. Depending on the network, use of the monitor command 645 to capture all data communication for protocols such a PPP or Mobile IP occurring in a particular network platform could produce an extensive amount of captured packets. Such a monitor session, due to the large number of packets captured, may not be desirable, as analysis of the results of such a monitor session may not be particularly useful and/or efficient due to the volume of packets collected.

**Captured Packet**

Figure 7 illustrates the form of a captured packet 700 as it may be communicated from a PDSN or HA to a collection agent. The captured packet 700 includes an IP header
710 that is used to route the packet from the network platform on which it was captured to the
collection agent. The captured packet 700 also includes a GRE header 720. The GRE header
720, as was previously discussed, is used by the collection agent to determine a monitoring
session with which the captured packet 700 is associated. The captured packet 700 also
includes a captured data portion 720. The captured data portion 720 is a copy of a data
packet (or a portion of the data packet) that was identified by an active monitor session being
executed on a network platform.

When the captured packet 700 is received at the collection agent, the GRE header 720
is examined to determine a GRE tunnel identification included in the header. The GRE
tunnel identification indicates the corresponding monitoring session and is assigned by the
network platform when the monitor session is initiated. The collection agent then determines
whether a file associated with that particular monitoring session is open. If a file is open, the
captured data portion 730 is saved (appended) to the open file in a predetermined format
(e.g., PCAP). If a file is not open, the collection agent opens a file, which is assigned a
filename corresponding with the monitor session (e.g., GRE tunnel identification), and then
saves the captured data portion 730 to the newly opened file.

The collection agent may also include a timeout value that determines how long a file
is kept open after receipt of the last packet stored in the file. For example, if a packet is not
received for ten minutes for a given monitoring session, the collection agent may close the
file. If a packet associated with the given monitor session arrives after the collection agent
has closed the associated file, the collection agent may reopen the file and append the newly
received packet to the file. Alternatively, the collection agent may open a new file and place
the newly received packet in that file. The two files could be distinguished by the collection
agent including timestamps in the filenames in addition to the monitor session identification.
The timestamp would indicate when each file was opened and, thus, the sequence in which the captured packets were received by the collection agent would be preserved.

**Methods for Monitoring Data Communication**

Figure 8 is a flowchart that illustrates a method 800 for monitoring data communication in a data network, such as the data network 100 of Figure 1. The method 800 may be implemented using a network platform (such as the network platform 200 illustrated in Figures 2 - 4) and a collection agent (such as the collection agent 500 illustrated in Figure 5), of course other systems and approaches may also be used. However, for purpose of this disclosure, data monitoring methods will be described with respect to the data network 100 of Figure 1, the network platform 200 of Figure 2 and the collection agent 500 of Figure 5.

The method 800, at block 810, includes accessing the network platform 200 via a user interface. The user interface, as was previously described, may be a command line interface that is implemented by the system manager card 230 in the network platform 200. As was also discussed above, the user interface of the system manager card 230 may be accessed by a user via a telnet or secure shell session.

At block 820, the method 800 includes communicating a monitor command to the network platform 200, where the monitor command indicates a category of data to monitor. The monitor command may, for example, take the form of one of the monitor commands described with respect to Figure 6. Alternately, other forms of monitor commands could be used to initiate a monitoring session. As was described above, a user may attach to a packet-processing card through the command line interface implemented by the system manager card 230. The monitor command may then be communicated to the packet-processing card (or alternatively to the packet-switch card 220) via the command line interface, the system manager card 230 and the system management bus 280.
For this example, after the monitor command is received at the packet-processing card, the packet processing card may examine the command to make sure that the syntax of the command is valid. In the event the syntax is not valid, the user may be provided with a notification of the error via the command line interface. If the syntax is correct, the packet-processing card that received the monitor command then distributes the monitor command to the other packet-processing cards of the network platform 200 and to the packet-switch card 220.

The monitor command may be distributed in any number of ways in the network platform. For example, the network platform 200 may include a configuration utility that provides for configuration of the various components of the platform via the system management bus 280. The packet-processing card that receives the monitor command could distribute the command using this configuration utility. Alternatively, the monitor command could be distributed over the high-speed backplane 270 (e.g., the MDB). In this situation, the packet-processing card that received the monitor command via the user interface (e.g., a command line interface) would communicate the monitor command to the packet-switch card 220. The packet-switch card 220 would retain a copy of the monitor command and then distribute the command to the other packet processing cards of the network platform.

As was discussed above, depending on the particular format of the monitor command, the monitor session initiated by that command will be executed by one of the packet-processing cards or the packet-switch card. For monitor commands that initiate monitoring sessions corresponding with a communication session for a particular user device, the monitor session may become active on a plurality of packet-processing cards in the network platform 200. However, packets captured for that monitor session would be captured by the packet-processing card responsible for processing that particular communication session. If a finite timeout parameter was defined in the monitor command that initiated the monitor
session, the monitor session would eventually timeout on the cards not processing that communication session, even if the monitor session remains active in the network platform on the packet processing card responsible for processing the communication session.

At block 830, the method 800 further includes identifying packets that match the criteria indicated in the monitor command that was communicated to the network platform 200. As previously described, depending on the particular form of monitor command, packets matching the command’s criteria will be identified either by a packet-processing card of the network platform 200 or by the packet-switch card 220 of the platform 200. It will be appreciated that multiple monitor sessions may be active at any given time and packets being communicated within the platform 200 are examined to determine if they match the specified criteria for any active monitor sessions.

At block 840, the method 800 includes communicating the identified (captured) packets from the network platform to a collection agent. As was discussed above, captured packets may be copies of packets (or portions thereof) that are identified as matching criteria of an active monitor session. These copies may be communicated to the collection agent using any number of approaches. For example, a GRE tunnel between the network platform 200 and the collection agent 500 may be established for each active monitor session. The packet-processing card or packet-switch card that captures the packet would then add a GRE header that includes the tunnel identification associated with the corresponding monitor session. Additionally, an IP header may be added for routing the packet to the collection agent, where the IP header includes the IP address of the collection agent.

At block 850, the method 800 includes receiving the captured (identified) packets at the collection agent. As described above, the captured packets may be communicated from the network platform 200 to the collection agent 500 via a GRE tunnel associated with the monitoring session for which the packet was identified. The packets are received via this
GRE tunnel over the communication interface 510. At block 860, the method 800 includes storing the packets in a predetermined format, such as PCAP format, as was described above. As was also described above, the packet storage module 520 of the collection agent 500 may also remove the IP headers and GRE headers of the corresponding packets before storing them in a file that corresponds with the respective monitoring session.

At block 870, the method 800 includes applying the packet analyzer 530 of the collection agent 500 to the captured packets that have been communicated to the collection agent 500 from the network platform 200. As previously discussed, applying the packet analyzer 530 to the captured packets converts the packets to a form (e.g., an ASCII textual form) that is readable by a user and/or system administrator for analysis of data communication that is occurring in the network platform 200. As described above, one example of an application that may be used to implement the packet analyzer 530 is the Ethereal network protocol analyzer, which is an open source application that is readily available over the Internet.

Figure 9 is a flowchart that illustrates another method 900 for monitoring data communication in, for example, a wireless data network that includes the network platform 200. The method 900 includes, at blocks 910, 920 and 930, accessing the network platform 200, communicating a command to a first packet-processing card of the network platform 200 and distributing the command to a second-packet processing card and the packet-switch card 220 of the platform 200. The command may, of course, be distributed to more packet-processing cards. The operations of blocks 910, 920 and 930 may be carried out in similar fashion as was described above with respect to the method 800 illustrated in Figure 8. For purposes of brevity and clarity, these operations will not be described in detail again with respect to the method 900, except as necessary to understand the differences between the method 800 and the method 900.
The monitor command communicated at block 920 may be a monitor command for initiating a monitor session. Such commands were described above with reference to Figure 6. Alternatively, the monitor command may instruct the platform to perform some other function related to monitoring data communication in a data network. For example, as was previously described, the monitor command may instruct the network platform 200 to terminate an active monitor using, for example, an “UNMONITOR” command that includes information identifying the monitor session to be terminated. Such information may be, e.g., a monitor session identification number or, alternatively, the parameters that were used to initiate the monitoring session.

As another example, the monitor command communicated to the network platform 200 at block 920 may provide the network platform 200 with a network address (e.g., IP address) of a collection agent to which the network platform is to send packets captured during data monitoring sessions that are executed on the platform 200. As another alternative, the monitor command may request that the network platform 200 indicate (via the user interface implemented on the system manager card 230) the current network address of a collection agent to which the network platform 200 is communicating captured packets. The syntax of such commands may vary and depends on the particular embodiment.

As another alternative, the monitor command communicated to the network platform 200 at block 920 may request that the network platform generate and display (via the user interface) a list of current monitor sessions that are active on the network platform. The generated list may include various information about each active monitor session, such as the user that initiated the session, the time the session was initiated, a GRE tunnel identifier associated with the session, and/or a monitor session identifier (e.g., such as to use in an UNMONITOR command), among other possible information regarding each monitoring session.
At block 940, the method 900 further includes determining whether a user that communicated the monitor command at block 920 is authorized to request the performance of the specific function indicated in the monitor command. For example, a system administrator may have certain privileges that other users do not. For instance, a system administrator may have the authorization to terminate (using an UNMONITOR command) any active monitoring session in the network platform 200. In comparison, other users may only be authorized to terminate monitoring session that they initiated. Likewise, a system administrator may be authorized to list all active monitoring sessions while individual users may be authorized to list only those sessions that they initiated.

The packet-processing cards and the packet-switch card 220 of the network platform 200 may determine whether a user is authorized to request the specific monitoring function (indicated in the monitor command that was communicated at block 920) based on a user identification and permission level associated with the command. The user identification and permission level may be communicated along with the command when it is sent from the system manager card 230 to the first-packet processing card. The user identification and permission level can then be compared with user identifications and permission levels associated with each active monitoring session to determine if the user that entered the command is authorized to request performance of the specific function. For example, if a user (not a system administrator) requests, using a monitor command, a list of all active monitoring sessions, the packet processing cards and packet-switch card 220 will compare the user identification and permission level associated with the command with the user identification and permission level associated with each of the active monitor sessions. A list would then be generated that only includes active monitor sessions where the user identification and permission level of the command match with the user identification and permission associated with the respective monitoring sessions.
In other instances, the network platform 200 may provide an indication to the user, via the user interface, that the user is not authorized to request a specific function. For example, if a user attempts to terminate a monitor session that he or she did not initiate, an indication may be provided to the user that he or she cannot request termination of that monitor session. In any event, if a user is authorized to request that a specific function be performed, the network platform 200 will proceed to perform the requested function.

It will be appreciated that the determination of whether a user is authorized to request that a specific monitor function indicated in the monitor command communicated at block 920 could be made by the first packet-processing card that receives the monitor command before the monitor command is distributed in the platform 200. In this situation, the user may be provided with an indication that he or she is not authorized to request the specific function indicated in the command. The command could then be removed from the platform 200 rather than distributing the command to the other packet-processing cards and the packet-switch card 220.

Conclusion

While a number of aspects and embodiments have been discussed above, it will be appreciated that various modifications, permutations, additions and/or sub-combinations of these aspects and embodiments are possible. It is therefore intended that the following appended claims and claims hereafter introduced are interpreted to include all such modifications, permutations, additions and/or sub-combinations as are within their true spirit and scope.
CLAIMS

What is claimed is:

1. A method for monitoring data communications, the method including:
   accessing a network platform via a user interface;
   communicating a command to the network platform via the user interface, the command indicating a category of data to monitor;
   identifying data packets in the network platform that correspond with the category of data to monitor; and
   communicating the identified packets from the network platform to a collection agent.

2. The method of claim 1, wherein communicating the command to the network platform comprises communicating the command to a card of the network platform, the method further comprising:
   distributing the command from the first card to at least one of (i) a packet-processing card included in the network platform and (ii) a packet-switch card included in the network platform, wherein:
   identifying the data packets that correspond with the category of data to monitor comprises identifying the data packets using one of the first card, the packet-processing card or the packet-switch card; and
   communicating the identified data packets to the collection agent comprises communicating the identified packets to the collection agent from the first card, the packet-processing card or the packet-switch card-card that is used for identifying.
3. The method of claim 2, wherein distributing the command from the first card to the packet-processing card comprises:

   communicating the command from the first card to the packet-switch card; and
   communicating the command from the packet-switch card to the packet-processing card.

4. The method of claim 2, wherein communicating the command to the first card comprises:

   entering the command using a command line interface (CLI) implemented by a system-manager card of the network platform; and
   communicating the command from the system-manager card to the first card via a bus.

5. The method of claim 1, wherein the first card comprises one of a packet-processing card and a packet-switch card.

6. The method of claim 1, wherein accessing the network platform using a user interface comprises accessing the network platform by logging into a system-manager card of the network platform.

7. The method of claim 1, wherein communicating the identified packets to the collection agent comprises communicating respective portions of the identified packets to the collection agent.
8. The method of claim 1, wherein communicating the identified packets to the collection agent comprises communicating copies of the identified packets.

9. The method of claim 1, further comprising:
   receiving the identified packets at the collection agent;
   storing the identified packets in a predetermined digital format in the collection agent.

10. The method of claim 9, wherein the predetermined digital format is compatible with a given packet analyzer application.

11. The method of claim 10, further comprising applying the given packet-analyzer application to the stored packets to convert the stored packets from the predetermined digital format to an American Standard Code for Information Interchange format.

12. The method of claim 1, wherein communicating the identified packets from the network platform to the collection agent comprises communicating the identified packets via a tunnel.

13. The method of claim 12, wherein the tunnel comprises one of a generic routing encapsulation tunnel, an Internet-Protocol-in-Internet-Protocol tunnel and a Universal Datagram Protocol tunnel.

14. A method for monitoring data communications, the method comprising:
   accessing a network platform via a user interface;
communicating a command to a first card of the network platform via the user interface, the command instructing the network platform to perform a specific function related to monitoring data communications in the network platform;

   distributing the command to at least one of (i) a packet-processing card in the network platform and; (ii) a packet-switch card in the network platform;

   determining, based on a user identification and permission level associated with the command, using one of the first card, the packet-processing card or the packet-switch card; whether a user associated with the command is authorized to request performance of the specific function; and

   in the event the user is authorized to request performance of the specific function, performing the specific function.

15. The method of claim 14, wherein in the event that the user is not authorized to request performance of the specific function, providing a notification, via that user interface, that the user is not authorized.

16. The method of claim 14, wherein the command includes a user identification and a permission level associated with the user identification, the user identification and permission level being used to determine whether the user is authorized to request performance of the specific function.

17. The method of claim 14, wherein the first card is a packet-processing card and performing the specific function indicated in the command comprises:

   identifying data packets, using the first card or the packet-processing card, that correspond with data communication associated with a given user device, wherein the card of
the first card and the packet-processing card used to identify the packets is responsible for processing a communication session associated with the given user device; and

communicating the identified data packets from the first card or the packet-processing card to a collection agent.

18. The method of claim 17, wherein the collection agent is implemented on a system manager card of the network platform.

19. The method of claim 17, wherein identifying packets that correspond with data communication associated with the given user device comprises identifying packets corresponding with an International Mobile Subscriber Identity of the given user device.

20. The method of claim 17, wherein identifying packets that correspond with data communication associated with the given user device comprises identifying packets corresponding with a Network Address identifier of the given user device.

21. The method of claim 17, wherein identifying packets that correspond with data communication associated with the given user device comprises identifying packets corresponding with an Internet Protocol address of the given user device.

22. The method of claim 14, wherein performing the specific function indicated in the command comprises:

identifying data packets, using the packet-switch card, that correspond with data communication associated with a given network platform; and
communicating the identified data packets from the packet-switch card to a collection agent.

23. The method of claim 22, wherein identifying packets that correspond with data communication associated with the given network platform comprises identifying packets corresponding with a tunnel identifier that is associated with the given network platform.

24. The method of claim 22, wherein identifying packets that correspond with data communication associated with the given network platform comprises identifying packets that correspond with an Internet Protocol Address of the given network platform.

25. The method of claim 14, wherein performing the specific function indicated in the command comprises:

   identifying data packets that correspond with data communication associated with a given communication protocol using the packet-switch card; and

   communicating the identified data packets from the packet-switch card to a collection agent.

26. The method of claim 14, further comprising including a timeout parameter in the command, wherein the timeout parameter indicates to the first card, the packet-processing card and the packet-switch card, an amount of time to wait for a data packet that meets criteria specified in the command, wherein expiration of the amount of time without identification of a data packet meeting the criteria occurring results in a monitoring session for identifying packets that meet the criteria being terminated.
27. The method of claim 14, wherein performing the specific function indicated in the command comprises:

terminating a monitoring session for identifying data packets meeting a given criteria.

28. The method of claim 14, wherein performing the specific function indicated in the command comprises:

setting a network address of a collection agent for receiving packets from the network platform, wherein the packets received by the collection agent are identified for communication to the collection agent in accordance with criteria defined in other commands communicated to the network platform via the user interface.

29. The method of claim 14, wherein performing the specific function indicated in the command comprises:

listing a network address, via the user interface, of a collection agent that receives packets from the network platform, wherein the packets received by the collection agent are identified for communication to the collection agent in accordance with criteria defined in other commands communicated to the network platform via the user interface.

30. The method of claim 14, wherein performing the specific function indicated in the command comprises:

generating and displaying a list of active monitoring sessions being executed on the network platform.

31. A method for monitoring data communications, the method comprising:

accessing a network platform via a user interface;
communicating a command to a first card of the network platform via the user interface, the command instructing the network platform to perform a specific function related to monitoring data communications in the network platform;

   distributing the command to at least one of (i) a packet-processing card in the network platform and; (ii) a packet-switch card in the network platform;

   performing the specific function using the first card, the second packet-processing card or the packet-switch card.

32. The method of claim 31, wherein the first card is a packet-processing card and performing the specific function indicated in the command comprises:

   identifying data packets, using the first card or the second packet-processing card, that correspond with data communication associated with a given user device, wherein the card of the first card and the packet processing card used to identify the packets is responsible for processing a communication session associated with the given user device; and

   communicating the identified data packets from the first card or the packet-processing card to a collection agent.

33. The method of claim 31, wherein performing the specific function indicated in the command comprises:

   identifying data packets, using the packet-switch card, that correspond with data communication associated with a given network platform; and

   communicating the identified data packets from the packet-switch card to a collection agent.
34. The method of claim 31, wherein performing the specific function indicated in the command comprises:

identifying data packets that correspond with data communication associated with a given communication protocol using the packet-switch card; and

communicating the identified data packets from the packet-switch card to a collection agent.

35. A system for monitoring data communications comprising:

a network platform for providing at least one of packet data serving node services and home agent services, the network platform, in operation, receiving a command instructing the network platform to perform a specific function related to monitoring data communication in the network platform; and

a collection agent coupled with the network platform, the collection agent comprising:

- a packet storage module; and

- a packet analyzer, wherein

the collection agent, in operation:

receives packets from the network platform, the received packets being associated with one or more monitoring sessions that are in process on the network platform;

stores packets in a predetermined format that corresponds with the packet analyzer; and

applies the packet analyzer to the received packets to convert the stored packets to a textual format for analysis by a user.

36. The system of claim 35, wherein the network platform comprises:
a backplane for routing data within the platform;

a packet-switch card coupled with the backplane, the packet-switch card aggregating the flow of data in the platform;

a plurality of packet-processing cards coupled with the backplane, the packet-processing cards providing the at least one of packet data serving node services and home agent services;

a system manager card, the system manager card implementing a user interface for accessing the network platform;

a bus coupled with the system manager card, the packet-switch card and the packet-processing cards, wherein the command instructing the network platform to perform the specific function is communicated to a first card of the plurality of packet processing cards and the packet-switch card via the system manager card and the bus using the user interface.

37. The system of 36, wherein:

in the event the first card comprises a packet-processing card of the plurality of packet-processing cards, the first card distributes the command to (i) the other packet-processing cards of the plurality of packet-processing cards; and (ii) the packet-switch card; and

in the event the first card comprises the packet-switch card, the first card distributes the command to the plurality of packet-processing cards, and

the specific function is performed by one of the plurality of packet-processing cards or the packet-switch card.
ACCESSING NETWORK PLATFORM

COMMUNICATING COMMAND TO PLATFORM INDICATING CATEGORY OF DATA TO MONITOR

IDENTIFYING PACKETS MATCHING CATEGORY

COMMUNICATING IDENTIFIED PACKETS TO COLLECTION AGENT

RECEIVING IDENTIFIED PACKETS AT COLLECTION AGENT

STORING RECEIVED PACKETS IN PREDETERMINED FORMAT

APPLYING PACKET ANALYZER TO STORED PACKETS

FIGURE 8
9/9

ACCESSING NETWORK PLATFORM

COMMUNICATING COMMAND TO FIRST PACKET-PROCESSING CARD INDICATING SPECIFIC DATA MONITORING FUNCTION TO PERFORM

DISTRIBUTING COMMAND TO SECOND-PACKET PROCESSING CARD AND PACKET SWITCH CARD

DETERMINING WHETHER USER ASSOCIATED WITH COMMAND IS AUTHORIZED TO REQUEST PERFORMANCE OF SPECIFIC FUNCTION

IF USER IS AUTHORIZED, PERFORM FUNCTION

IF USER IS NOT AUTHORIZED, PROVIDE NOTIFICATION

FIGURE 9