

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
15 February 2007 (15.02.2007)

PCT

(10) International Publication Number
WO 2007/017716 A1

(51) International Patent Classification:

H04L 29/02 (2006.01) **H04M 11/06** (2006.01)**H04L 12/16** (2006.01) **H04N 7/173** (2006.01)**H04L 12/66** (2006.01)

(21) International Application Number:

PCT/IB2006/002035

(22) International Filing Date: 25 July 2006 (25.07.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

11/200,603 10 August 2005 (10.08.2005) US

(71) Applicant (for all designated States except US): **NORTEL NETWORKS LIMITED** [CA/CA]; 2531 Boulevard Alfred-Nobel, St. Laurent, Quebec H4S 2A9 (CA).(72) Inventors: **NANNRA, Anoop** 2012 New Carlisle Crescent; Orleans, Ontario K4A 4M1 (CA). **TIMMS, Andrew**; 277 Mounbatten Avenue, Ottawa, Ontario K1H 5W2 (CA). **HAYES, Hasler**; 7712 Bleeks Road, Box 327,Munster Hamlet Ontario K0A 3P0 (CA). **WATKINS, John**; 19 Laurel Street, Ottawa, Ontario K1R 6T8 (CA).

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

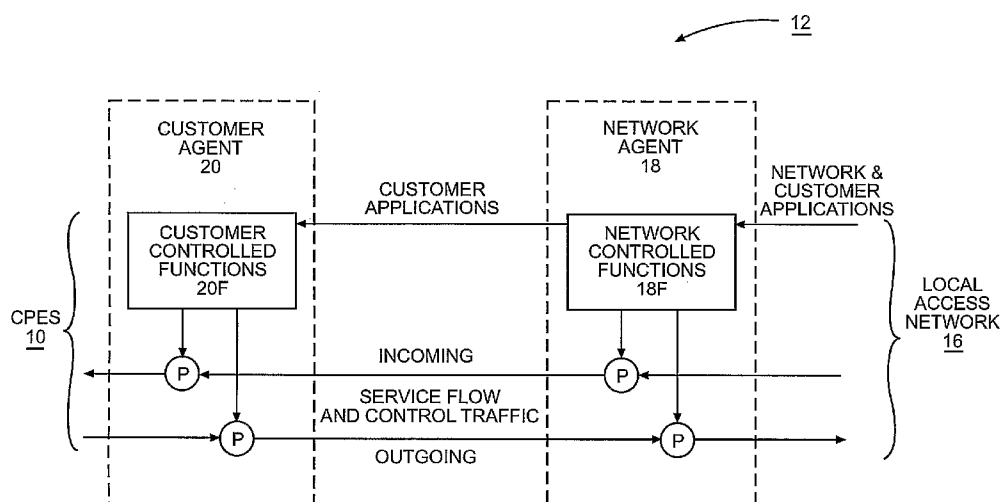
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT,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

Published:

— with international search report

[Continued on next page]

(54) Title: NETWORK CONTROLLED CUSTOMER SERVICE GATEWAY FOR FACILITATING MULTIMEDIA SERVICES OVER A COMMON NETWORK



(57) Abstract: The present invention provides a customer service gateway (12) acting as an interface between various customer premise equipment (30, 34, 40, 42) for a customer and a local access network (16). The customer service gateway (12) has one or more customer agents (20) and network agents (18). A network agent (18) is a secure and trusted agent of the service providers, and is not accessible by the customer service gateway (12) may support different types of services using different types of media from the different service providers. In operation, the service providers may sent applications to a network agent (18), which will run the applications to implement functions to monitor or control services of service flows for the services. The monitoring and control functions may be used to implement various types of service or service flow analysis, as well as any type of tagging, characterization, or processing of the service flows.

WO 2007/017716 A1



— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(48) Date of publication of this corrected version:

3 May 2007

(15) Information about Correction:

see PCT Gazette No. 18/2007 of 3 May 2007

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.

***NETWORK CONTROLLED CUSTOMER SERVICE GATEWAY FOR
FACILITATING MULTIMEDIA SERVICES OVER A COMMON NETWORK***

Field of the Invention

- 5 **[0001]** The present invention relates to communications, and in particular to a technique for controlling services in a multi-service environment supported by one or more access networks.

Background of the Invention

- 10 **[0002]** Traditionally, dedicated access networks have been used to provide dedicated services. For example, cable networks would provide television services, telephone networks would provide telephone services, and data networks would provide data services. With the rapid acceptance and expansion of packet-based technologies, there is a movement toward
15 providing disparate services over a common packet network. The goal is to allow multiple application service providers to connect to subscribers over one or more access networks operated by one or more network service providers. Applications can be any mixture of real time, near real time, and low priority applications, which may require any level of trustworthiness or security
20 mechanisms.

- [0003]** While significant progress has been made toward providing core networks capable of transporting packets for various services, access networks connecting to a subscriber's residence or place of business are still relatively separate. Although data services may be overlaid on telephony
25 access networks, these access networks are not configured to support a wide range of simultaneous services such as telephony, video and multimedia. Further, there is little control over the various types of media provided via the data services.

- [0004]** As these media services mature, there will be a need to support
30 voice, audio, video, and other real-time or streaming applications where timely delivery of packets is important, over a common access network. Any access network providing a connection to the subscriber premises is likely to have finite bandwidth with respect to the number of services that are available and contending for that finite bandwidth. Given the movement to provide multiple

services over a single access network and the different quality of service requirements associated with these services, there is a need for a technique to control the allocation of bandwidth for services and assure that subscribers are not allowed access to bandwidth or services to which they are not entitled.

- 5 Given that different types of services often require various types of policing and control, there is a need for a technique to provide additional traffic control, monitoring, and processing functions at the customer premises to fully support the different service types. Further, since multiple service providers can provide services over the common access network, there is a further need for
- 10 a technique to allow different service providers to provide services and have their services controlled in a desired manner. In essence, there is a need to provide control and policing on a service-by-service basis over a common access network for different types of services from different service providers in an efficient and effective manner.

15

Summary of the Invention

- [0005] The present invention provides a customer service gateway acting as an interface between various customer premise equipment for a customer and one or more local access networks, which leads to one or more service
- 20 provider networks. The customer service gateway has one or more customer agents and one or more network agents. A network agent is a secure and trusted agent of the service providers, and is not accessible for manipulation by the customer or the customer premise equipment. The customer service gateway may support different types of services using different types of media
- 25 from the different service providers. In operation, the service providers may send applications to a network agent, which will run the applications to implement functions to monitor or control services or service flows for the services. The monitoring and control functions may be used to implement various types of service, or service flow analysis, as well as any type of
- 30 tagging, characterization, or processing of the service flows. Other functions may be provided to the customer agent by the customer or through the network agent by the service providers, wherein the customer agent will run the applications to implement select functions for the services or service flows.

[0006] The customer agent and network agent may operate on incoming or outgoing service flows, as well as provide overall service control. The service providers may also provide policy criteria to the network agent as well as to the customer agent, wherein the agents will operate to enforce appropriate policies when implementing the services and supporting the service flows, to ensure that the services are provided having a desired quality of service and that only authorized services are provided in an appropriate fashion.

[0007] Those skilled in the art will appreciate the scope of the present invention and realize additional aspects thereof after reading the following detailed description of the preferred embodiments in association with the accompanying drawing figures.

Brief Description of the Drawing Figures

[0008] The accompanying drawing figures incorporated in and forming a part of this specification illustrate several aspects of the invention, and together with the description serve to explain the principles of the invention.

[0009] FIGURE 1 is a block representation of a communication environment according to one embodiment of the present invention.

[0010] FIGURE 2 is a logical representation of a customer service gateway according to one embodiment of the present invention.

[0011] FIGURES 3A-3C represent an exemplary communication flow according to one embodiment of the present invention wherein a digital rights management function is implemented at the customer service gateway.

[0012] FIGURE 4 is a block representation of a customer service gateway according to one embodiment of the present invention.

[0013] FIGURE 5 is a block representation of a network service edge according to one embodiment of the present invention.

[0014] FIGURE 6 is a block representation of a network policy server according to one embodiment of the present invention.

Detailed Description of the Preferred Embodiments

[0015] The embodiments set forth below represent the necessary information to enable those skilled in the art to practice the invention and illustrate the best mode of practicing the invention. Upon reading the

following description in light of the accompanying drawing figures, those skilled in the art will understand the concepts of the invention and will recognize applications of these concepts not particularly addressed herein. It should be understood that these concepts and applications fall within the scope of the disclosure and the accompanying claims.

[0016] With reference to Figure 1, a communication environment according to one embodiment of the present invention is illustrated. The communication environment may include various types of customer premise equipment (CPE) 10. The CPEs 10 are associated with a customer service gateway 12 to receive packet-based services from a core packet network 14 via a local access network 16. Depending on configuration, the customer service gateway 12 may include one or more network agents 18 and one or more customer agents 20, which cooperate to support various types of services from different service providers. The network agent 18 is a secured and trusted agent under the control of the service provider, while the customer agent is an unsecured agent, which may operate under the control of the customer as well as the service provider. In general, the network agent 18 is not accessible by the customer or CPEs 10.

[0017] The network agent 18 provides a logical interface to the local access network 16 and supports secure functions, which monitor or control service flows according to various policies of the service providers. Service flow control may include, but is not limited to, controlling the individual service, prioritizing traffic and service flows, as well as actually processing traffic in the service flows. The policies are provided to ensure that only authorized services are allowed and that content for the services is properly received at the appropriate CPE 10. As such, the present invention provides an efficient and effective monitoring and control for various services at a central point, the customer service gateway 12, where coherent and consistent policy enforcement can be applied for a customer using the appropriate policies of the service providers. The functions may be part of applications that are received from the various service providers and that run on the network agent 18. The functions include, but are not limited to, authorizing services, characterizing service flows, prioritizing services or services flows, reordering packets within service flows, routing packets, tagging service flows for

subsequent processing, encrypting and decrypting service flows, compressing and decompressing service flows, converting between protocols, and any other monitoring control function deemed desirable at the customer premises.

[0018] Different services may be associated with different service

5 providers. The present invention allows different service providers to establish secure and trusted control of the network agent 18. The functions provided by the network agent 18 may be used to support television, telephone, and high-speed internet access; support pay-per-view or other pay-per-use services; implement digital rights management, including
10 termination and encryption for audio and video streams; control firewall operation, including opening and closing ports from the network side; provide network control for Network Address Translation (NAT); provide secure interfaces for utility meter reading; provide location validation for people on the customer premises, such as in home arrest and curfew control; or provide
15 medical instrument telemetry and alarms for home health care. Any of these or other functions may be provided over a common network along with other services and service flows, using different encryption and decryption, over the same local access network 16. In prior implementations, separate secure networks were required to provide a trusted service.

20 **[0019]** The customer agent 20 provides a logical interface for the CPEs 10 and can run applications provided by the customer or the service providers.

The applications and functions provided thereby can be controlled or modified by the customer within limits provided by the service providers. Control messaging and service flows may pass through the customer agent 20 and
25 the network agent 18, wherein either agent can provide various monitoring and control functions. Those functions provided by the customer agent 20 are potentially customizable by the customer, while functions provided by the network agent 18 are secure and controlled solely by appropriate service providers. The customer will not have access to or control of the network
30 agent 18.

[0020] With continued reference to Figure 1, a network gateway 22 may be provided between a network service edge (NSE) 24 and the local access network 16. The NSE 24 cooperates with the network gateway 22 to provide an interface between the local access network 16 and the core packet

network 14. For services provided to the CPEs 10 via the local access network 16, the customer service gateway 12 and the NSE 24 will operate to establish virtual communication pipes over the local access network 16 for each of the services provided to the CPEs 10. In essence, the virtual communication pipes are virtual paths having defined parameters that are sufficient to support the traffic flow, in either direction, associated with a particular service.

[0021] The network agent 18 of the customer service gateway 12 and the NSE 24 operates under the control of a network policy server (NPS) 26, which essentially instructs the network agent 18 and the NSE 24 to establish the virtual communication pipes for selected services and control the traffic flows therein. The network agent 18 and NSE 24 will cooperate to allocate resources and ensure a desired quality of service, along with providing control or shaping of traffic flow for the service. Depending on the available bandwidth and the number of services implemented, the network agent 18 and NSE 24 may also provide packet queuing and make decisions on prioritizing packets based on the parameters associated with each service.

[0022] In one embodiment, different types of services may be supported over different virtual communication pipes to various ones of the CPEs 10.

The CPEs 10 may take many forms and support various types of services, such as circuit-switched or packet-based telephony, television, data, audio, and video. Various types of CPE 10 are represented in Figure 1, but those skilled in the art will recognize that the invention is not limited to the illustrated embodiments. The CPE 10 may take the form of a telephony terminal 28, which is associated with the customer service gateway 12 via an integrated access device (IAD) 30, which effectively performs voice over packet-to-Plain Old Telephone System (POTS) adaptation. For television service, a television 32 may be supported by a set top box (STB) 34, which cooperates with the customer service gateway 12 to facilitate television service. A notebook computer or PDA 36, as well as a mobile terminal 38 may facilitate local wireless communications via a local wireless access point 40, which may facilitate local wireless communications using Wireless Local Area Network (WLAN), Bluetooth, or other local wireless technology. A personal computer 42 may also be logically associated with the customer service gateway 12 to

facilitate various types of media services, including streaming audio, video, and voice, along with traditional data services. Other types of devices, such as location and medical monitoring equipment (not shown) may be provided as CPE 10.

5 **[0023]** For any of the varied services capable of being provided to the CPEs 10, the network agent 18, customer service gateway 12, and NSE 24 will function to allocate bandwidth for the virtual communication pipe and control the traffic flow for the service, other services, and their respective virtual communication pipes, to ensure that each service is delivered with an appropriate quality of service, as well as preventing unauthorized use of any resource either at the core, at any service provider, or at any CPE device.

10 **[0024]** In operation, the NPS 26 will have access to information bearing on the services that a particular subscriber is authorized to use. The information controlling access to these services is generally referred to as a user policy, which will have various parameters defining the resources that are either necessary or authorized to be used to facilitate the service. The NPS 26 will also keep track of the overall resources available through the local access network 16 as well as the services being implemented at any given time. As such, the NPS 26 will recognize which resources are being used and which resources are available for new services. Based on this information, intelligent decisions can be made to ensure that a requested service can be fulfilled. The NPS 26 illustrated represents a primary policy server for a primary service provider. The present invention allows alternate service providers (ASPs) 44 to provide services along with the primary service provider via the customer service gateway 12.

25 **[0025]** In general, the services are provided in uni-directional or bi-directional communication flows with the CPE 10 over the local access network 16, wherein the packet flows are controlled in the downstream direction (toward the CPE 10) by the NSE 24, and controlled in the upstream direction (from the CPE 10) by the network agent 18 of the customer service gateway 12. The traffic flows, which ride on top of the packet flows, may be controlled in part by service controllers (SCs, which are not shown), which may interact with the CPE 10 to facilitate the transmission of packets between the CPE 10 and a content server (CS) 46. In general, the service controllers

will cooperate with the content servers 46, and perhaps with the CPE 10, to facilitate the delivery of content to effect a service over one of the virtual communication pipes. Alternatively, the services may be provided by other service provider entities or other entities provided in an associated Internet Protocol (IP) network 48 or the Public Switched Telephone Network (PSTN) 50, which may be coupled to the core packet network 14 via an appropriate gateway (not shown).

[0026] To establish service flows for a given service, the NPS 26 may instruct the customer service gateway 12 and NSE 24 to establish a virtual communication pipe for a requested service. Once the virtual communication pipe is established, the service controllers will communicate with the appropriate content server 46, and perhaps the affected CPE 10, to facilitate packet delivery for the requested service. If the requested service is high-definition television content, the content server 46 delivers a high-definition television program over an appropriately configured virtual communication pipe to the television 32 via the set top box 34. The customer service gateway 12 and NSE 24 ensure that the content is delivered with a required quality of service, and ensure that other services do not interfere with the high-definition television content. The NPS 26 controls the customer service gateway 12 and NSE 24 to ensure that the services do not conflict. To prevent such conflict, a requested service may be denied if there is insufficient bandwidth or other resources to provide the service; quality of service levels may be adjusted, if authorized, to accommodate the multiple services; or a service may be eliminated according to a defined priority profile.

[0027] In one embodiment of the present invention, the various services may be accounted for in different manners, such that telephone services are billed at a different rate than television or data services. In this instance, various ones of the NSE 24, NPS 26, service controller, or content server 46 may facilitate accounting or billing, and may generate billing information or send sufficient information to a billing server (BS) 52 to effect billing for the particular services. Depending on the implementation of the services, each service may be accounted for on a per-service basis, such as pay-per-view television, or a service may be provided on a limited basis for a monthly fee wherein additional features may include additional charges.

[0028] With reference to Figure 2, a logical representation of a customer service gateway 12 is provided. As noted, the customer service gateway 12 will include a customer agent 20 and a network agent 18. The information passed through the customer service gateway 12 is categorized as either control or service flow traffic, which is supported by packet-based communications. Accordingly, outgoing service flow traffic will flow from the CPEs 10 through the customer agent 20 and network agent 18 toward a desired destination via the local access network 16. Incoming service flow traffic will flow into the CPEs 10 from the local access network 16 via the customer agent 20 and the network agent 18. The incoming and outgoing control traffic will flow in similar fashion.

[0029] In addition to facilitating service flow and control traffic, network and customer applications may be provided to the network agent 18 from the various service providers, including both primary and alternate service providers 44. These network and customer applications, when run on the respective network agent 18 and customer agent 20, will provide network controlled functions 18F and customer controlled functions 20F. In essence, the network agent 18 may receive network and customer applications, and run the network applications and forward the customer applications to the customer agent 20. The customer applications may be modified to allow the customer to gain access to and otherwise control operation of the customer applications to provide various customized functions. The network applications will reside solely in the network agent 18, will be secure with respect to the service providers, and will not be accessible by the customer or CPEs 10.

[0030] When running network applications, the network agent 18 will implement the network controlled functions 18F on the incoming and outgoing service flow and control traffic, as necessary. The network controlled functions 18F will generally relate to monitoring or control of the one or more service flows and control traffic. Such monitoring and control is generally referred to as processing (P), wherein different monitoring and control functions may be provided for different applications and different services. Accordingly, either the service flow traffic or the control traffic may be monitored or controlled for a particular application.

[0031] Similarly, the customer controlled functions 20F may be implemented on the incoming or outgoing service flow control traffic. The functions will generally include monitoring or control, which are again generally referred to as processing (P). From this illustration, it is apparent
5 that secure applications may be downloaded to the network agent 18 and run in a trusted fashion to implement network controlled functions 18F. Customer applications, provided from the service providers or by the customer, can run on the customer agent 20 to provide customer controlled functions 20F, which may be altered, modified, or controlled by the customer without influencing the
10 network controlled functions 18F or allowing the customer access to the network controlled functions 18F.

[0032] Turning now to Figures 3A-3C, an exemplary communication flow is provided for implementing digital rights management (DRM) according to one embodiment of the preset invention. Assume that a service requiring DRM is
15 requested by a generic customer endpoint 54, and that the service is provided by an alternate service provider 44. The NPS 26 is associated with a primary service provider, which is primarily responsible for providing fundamental resources and control to the customer premises. When the customer endpoint 54 is turned on, a power up alert is sent to the customer agent 20 of
20 the customer service gateway 12 (step 100). The customer agent 20 will be interrogated by the network agent 18 to obtain basic start up and initialization information regarding the customer endpoint 54 (step 102). The customer agent 20 will provide the requested information in a response sent to the network agent 18 (step 104), which will negotiate with the network gateway 22
25 to facilitate initialization of the communication link that will be established between the customer service gateway 12 and the network gateway 22 over the local access network 16 (step 106).

[0033] Next, the network agent 18, which may communicate using the Internet Protocol (IP), will cooperate with the NSE 24 to facilitate address
30 negotiation, perhaps by using the Dynamic Host Configuration Protocol (DHCP), assuming addressing is not pre-provisioned (step 108). Either upon request or on a periodic basis, the NPS 26, which is associated with a service provider, will download a basic bandwidth (BW) and resource policy to the network agent 18 (step 110), which will acknowledge receipt of the policy

(step 112). The NPS 26 will also provide specific customer policy information to any appropriate alternate service providers 44 (step 114), which will acknowledge receipt of the specific customer policy information (step 116). Meanwhile, the network agent 18 and the network gateway 22 will cooperate
5 to establish a secure access link for the communication link established through the local access network 16 (step 118).

[0034] Next, the NPS 26 will send one or more secure applications to the network agent 18 (step 120). The secure applications may be any applications that the primary service provider needs to run in a secure and
10 trusted fashion on the network agent 18 of the customer service gateway 12. One or more of the secure applications may relate to implementing DRM from the primary service provider or by the alternate service providers 44. Implementation of the various functions may require applications from the different service providers, wherein the applications work together to
15 accomplish an overall task. In this instance, assume that one of the secure applications provided to the network agent 18 from the NPS 26 relates to one aspect of implementing DRM from the primary service provider's perspective (step 120). The NPS 26 will then send cryptography information to the network agent 18 (step 122) as well as to the alternate service providers 44
20 (step 124). The cryptography information may include keys or other encryption seeds, and the alternate service providers 44 may be able to verify the cryptography information (step 126), and as such will acknowledge receipt of the proper cryptography information from the NPS 26 (step 128).

[0035] At this point, the network agent 18 and an alternate service provider
25 44 are able to establish a secure provider link therebetween (step 130). Over the secure provider link, the alternate service provider 44 may download one or more secure applications, including in this example a secure application for implementing DRM as required by the alternate service provider 44 (step 132). Upon receipt of the secure applications, the network agent 18 will send
30 an acknowledgement back to the alternate service provider 44 (step 134). Receipt of the original secure applications may trigger the alternate service provider 44 to provide additional secure applications, including a content tagging application, to the network agent 18 (step 136). The network agent 18 will acknowledge receipt of the additional secure applications (step 138).

The content tagging application may cooperate with the DRM applications from the alternate service provider 44 as well as the primary service provider. The content tagging may be used to identify and tag traffic where DRM should be applied. Once identified, the DRM applications are used to process the traffic accordingly.

[0036] At this point, assume the customer endpoint 54 initiates a service request for a service to be provided by the alternate service provider (ASP) 44 (step 140). The service request will be received by the customer agent 20 of the customer service gateway 12. The customer agent 20 will process the request and forward it to the network agent 18 (step 142), which will verify that the request is within the policy previously provided by the NPS 26 (step 144). Assuming the request is within the given policy, the network agent 18 will send the service request to the NPS 26 (step 146), which will determine whether the request is authorized. If the request is authorized (step 148), the NPS 26 will forward the service request to the appropriate alternate service provider 44 for authorization and fulfillment (step 150). If the service request is authorized (step 152), acknowledgements may be propagated back through the NPS 26, network agent 18, and customer agent 20 to the customer endpoint 54 (steps 154, 156, 158, and 160).

[0037] At this point, the alternate service provider 44 will begin sending content (traffic) for the requested service to the network agent 18 of the customer service gateway 12 (step 162). The network agent 18 will run the primary and alternate service provider applications to implement the respective monitoring, tagging, and DRM functions (step 164). These applications may include monitoring all incoming traffic, identifying traffic associated with the requested service from the alternate service provider 44, recognizing that the traffic requires DRM, and implementing DRM processing for the content of the requested service. The processing may include tagging for subsequent processing at the customer agent 20 or the customer endpoint 54, protocol conversion, compression, decryption, or any other functions deemed necessary and supported by the requisite applications. After processing for the respective applications running on the network agent 18, the content is sent to the customer agent 20 (step 166), which may run the customer applications to implement any functions deemed appropriate at the

customer agent 20 (step 168) prior to being sent to the customer endpoint 54 (step 170).

[0038] The applications running on the customer agent 20 may be modified or configured by the customer to implement customized functions on the content. Actual applications may be provided via the network agent 18 or directly from the customer or appropriate customer endpoint 54. Tagging may take place at the network agent 18 or at the customer agent 20 for subsequent processing at the customer endpoint 54. When tagging occurs at the network agent 18, subsequent processing may take place at the customer agent 20 as well. Although the above illustration is focused on streaming content requiring DRM from an alternate service provider 44 to the customer endpoint 54, any type of media session may be provided by the primary service provider or the alternate service provider 44, in either direction. For services that may result in traffic moving in either direction, functions afforded by applications at the customer agent 20 and the network agent 18 may be implemented as necessary or desired.

[0039] Accordingly, the customer service gateway 12 acts as a policy enforcement point capable of receiving applications from various service providers on how to tag, process, or otherwise control upstream or downstream traffic flows. The customer service gateway 12 provides a trusted service management point on the customer premises for the primary service provider as well as for alternate service providers 44 that have established a relationship with the primary service provider. In addition to various processing functions, the customer service gateway 12 may be used to schedule and steer traffic according to defined policies, and may be used to provide specific billing based on the actual content, services, or quality of experience actually afforded to the customer.

[0040] While services are provided, the customer service gateway 12 and the NSE 24 will continue managing the respective packet flows according to the policy parameters. Such management will include classifying traffic flows for the various services that are implemented; providing queuing; maintaining a desired quality of service; shaping, controlling, processing, or filtering the traffic; or preventing unauthorized use of the local access network 16 by other CPEs 10. The customer service gateway 12 and NSE 24 will effectively route

all traffic for all services over the appropriate virtual communication pipes according to the defined policy parameters. Traffic for the service may be recognized by checking an identifier or label provided with the packets and associated with the particular service. In a preferred embodiment, the source and destination addresses, and potentially the respective ports used by the CPE 10 and the content server 46, are monitored to identify packets to be processed and transported over the virtual communication pipe in association with the service and according to the policy parameters. Accordingly, differentiated services may be provided over a single local access network 16 in a controlled fashion. With the present invention, the local access network 16 can be effectively partitioned among multiple services in a manner wherein the respective services will not negatively impact the others.

[0041] In addition to the above benefits, another embodiment of the present invention allows for differentiated billing for the respective services.

Since the services may be established on an individual basis, accounting for these services may also be provided on an individual basis. Various entities illustrated in Figure 1 may be used to collect accounting information, which will be processed and sent directly or indirectly to the billing server 52. The accounting information may be processed during the service, after the service, or a combination thereof. For example, when a service is terminated, the customer endpoint 54 may send a request to terminate the service, and the NPS 26 will take the necessary steps to remove the service policy and tear down the virtual communication pipe established between the customer service gateway 12 and the NSE 24.

[0042] The NPS 26 may send a message to terminate the service policy to the NSE 24, which may then send a message to terminate the service policy to the customer service gateway 12. If billing is based on content, the service provider or network agent 18 may generate billing information and send the billing information to the billing server 52. Alternatively, the NSE 24 may generate the billing information and forward the billing information to the billing server 52. Those skilled in the art will recognize numerous techniques for monitoring the service, accounting for the service, and delivering accounting or billing information to an appropriate billing server 52 to facilitate billing for the provided service.

[0043] Turning now to Figure 4, a block representation of a customer service gateway 12 is provided according to a standalone embodiment of the present invention. The customer service gateway 12 may include a control system 56 having memory 58 with sufficient software 60 to implement the customer agent 20 and the network agent 18 as described above. The control system 56 may be associated with one or more local access network interfaces 62 to facilitate communications over the local access network 16. The control system 56 will also be associated with any number of CPE interfaces 64, which are used to interface with the CPEs 10 in direct or indirect fashion. The CPE interfaces 64 may include network, audio, video, and voice interfaces.

[0044] As seen in Figure 5, the NSE 24 is configured similarly to the customer service gateway 12. The NSE 24 will include a control system 66 having memory 68 with sufficient software 70 to operate as described above. The software 70 will provide a policy enforcement function 72 to establish virtual communication pipes with the customer service gateway 12 over the local access network 16 and control services according to parameters received from the NPS 26. The control system 66 will be associated with one or more communication interfaces 74 to facilitate communications over the local access network 16 directly or indirectly via the network gateway 22, as well as with the NPS 26.

[0045] With reference to Figure 6, the NPS 26 may represent a logical function, but may be implemented in a traditional network server having a control system 76 with memory 78 for software 80 to control the operation as described above. The software 80 will include a policy server function 82, which will act to control the customer service gateway 12 and the NSE 24 to provide and control services over the local access network 16, as well as cooperate with the alternate service providers 44, content servers 46, session controllers, or other entities involved in providing the services. For such communications, the control system 76 is associated with at least one communication interface 84.

[0046] Those skilled in the art will recognize improvements and modifications to the preferred embodiments of the present invention. All such

improvements and modifications are considered within the scope of the concepts disclosed herein and the claims that follow.

Claims

What is claimed is:

1. A customer service gateway comprising:
 - a customer premise equipment interface;
 - a local access network interface; and
 - a control system associated with the customer premise equipment interface and the local access network interface and adapted to provide a customer agent and a network agent, which cooperate with one another to support services between customer premise equipment and at least one service provider, the network agent adapted to provide trusted service management on behalf of the at least one service provider at a customer premise.
2. The customer service gateway of claim 1 wherein the network agent is further adapted to:
 - receive service provider applications from the at least one service provider; and
 - run the service provider applications to implement provider functions for the services or service flows associated with the services to provide the trusted service management.
3. The customer service gateway of claim 2 wherein the provider functions control either the services or traffic in the service flows.
4. The customer service gateway of claim 3 wherein the provider functions process the traffic in the service flows.
5. The customer service gateway of claim 3 wherein the provider functions tag the traffic in the service flows for subsequent processing.
6. The customer service gateway of claim 2 wherein the provider functions monitor either the services or the traffic in the service flows.

7. The customer service gateway of claim 1 wherein there is no customer access to the network agent.
8. The customer service gateway of claim 1 wherein the customer agent is further adapted to:
 - 5 • receive customer applications; and
 - run the customer applications to implement additional functions for the services or service flows associated with the services.
9. The customer service gateway of claim 8 wherein at least one of the customer applications is received from the network agent.
- 10 10. The customer service gateway of claim 8 wherein the customer applications at the customer agent are customizable by a customer or the customer premise equipment.
11. The customer service gateway of claim 10 wherein the network agent is further adapted to limit customer customization of at least one of the
15 customer applications.
12. The customer service gateway of claim 1 wherein the network agent is further adapted to receive a service policy for the at least one service provider and establish communications links having defined resources for the services and support the services according to the service
20 policy.
13. The customer service gateway of claim 1 wherein the at least one service provider comprises a plurality of service providers including a primary service provider, the network agent adapted to simultaneously facilitate a plurality of services associated with a plurality of the plurality
25 of service providers.
14. The customer service gateway of claim 13 wherein at least two of the plurality of services are different types of media services.

15. The customer service gateway of claim 1 wherein the customer agent is adapted to support a plurality of different types of the customer premise equipment.
- 5 16. The customer service gateway of claim 1 wherein at least one of the services comprises customer monitoring.
17. The customer service gateway of claim 1 wherein implementing the trusted service management provides service flows for the services having a defined quality of service under control of the at least one service provider.
- 10 18. The customer service gateway of claim 1 wherein the trusted service management provides digital rights management for the services.
19. The customer service gateway of claim 1 wherein the trusted service management controls streaming media services comprising audio or video.
- 15 20. The customer service gateway of claim 1 wherein the trusted service management controls voice services.
21. The customer service gateway of claim 1 wherein the trusted service management controls internet access.
22. A method comprising:
- 20
- providing a customer premise equipment interface;
 - providing a local access network interface; and
 - providing a customer agent and a network agent, which cooperate with one another to support services between customer premise equipment and at least one service provider, the network agent adapted to provide trusted service management on behalf of the
- 25
- at least one service provider at a customer premise.

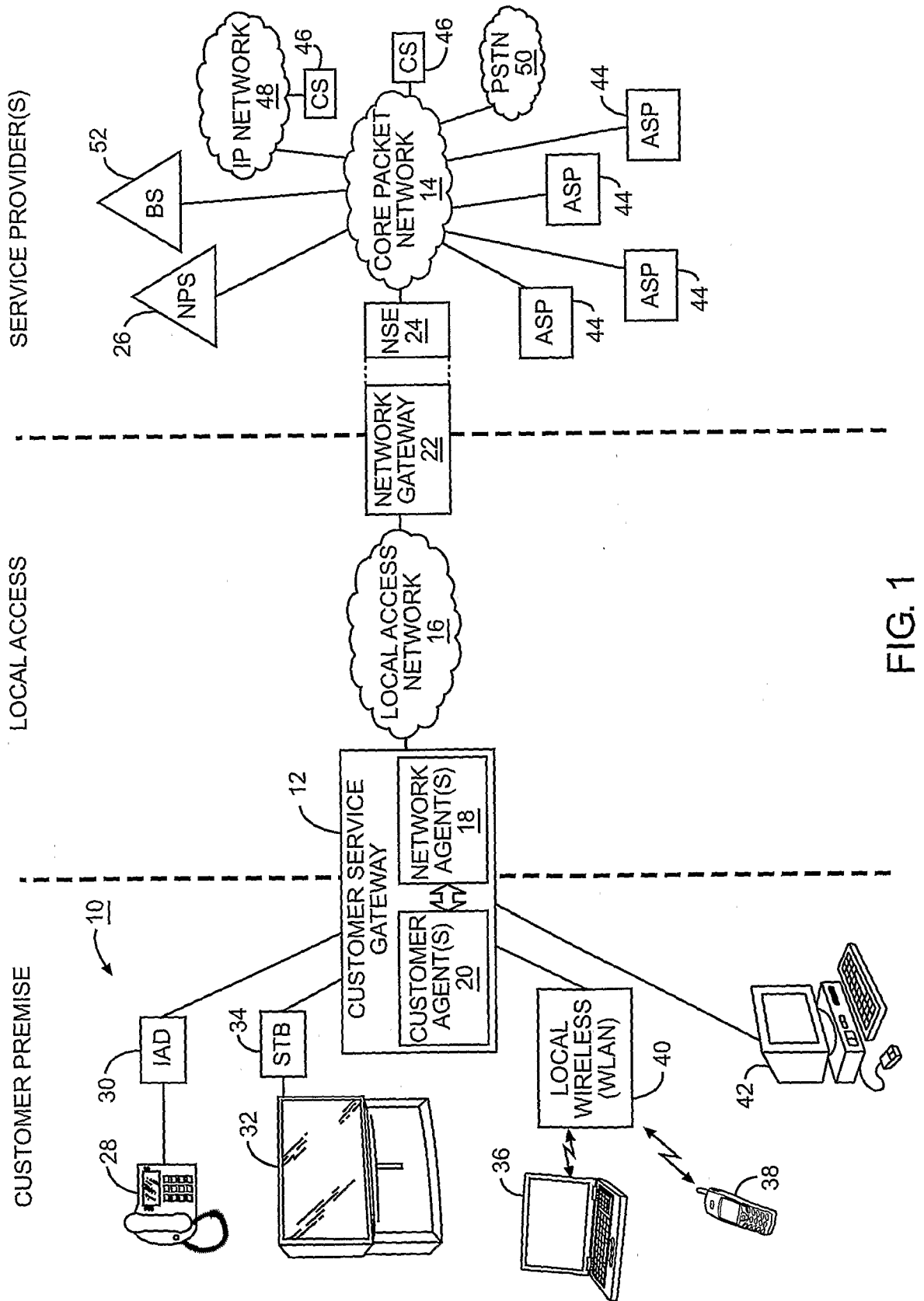


FIG. 1

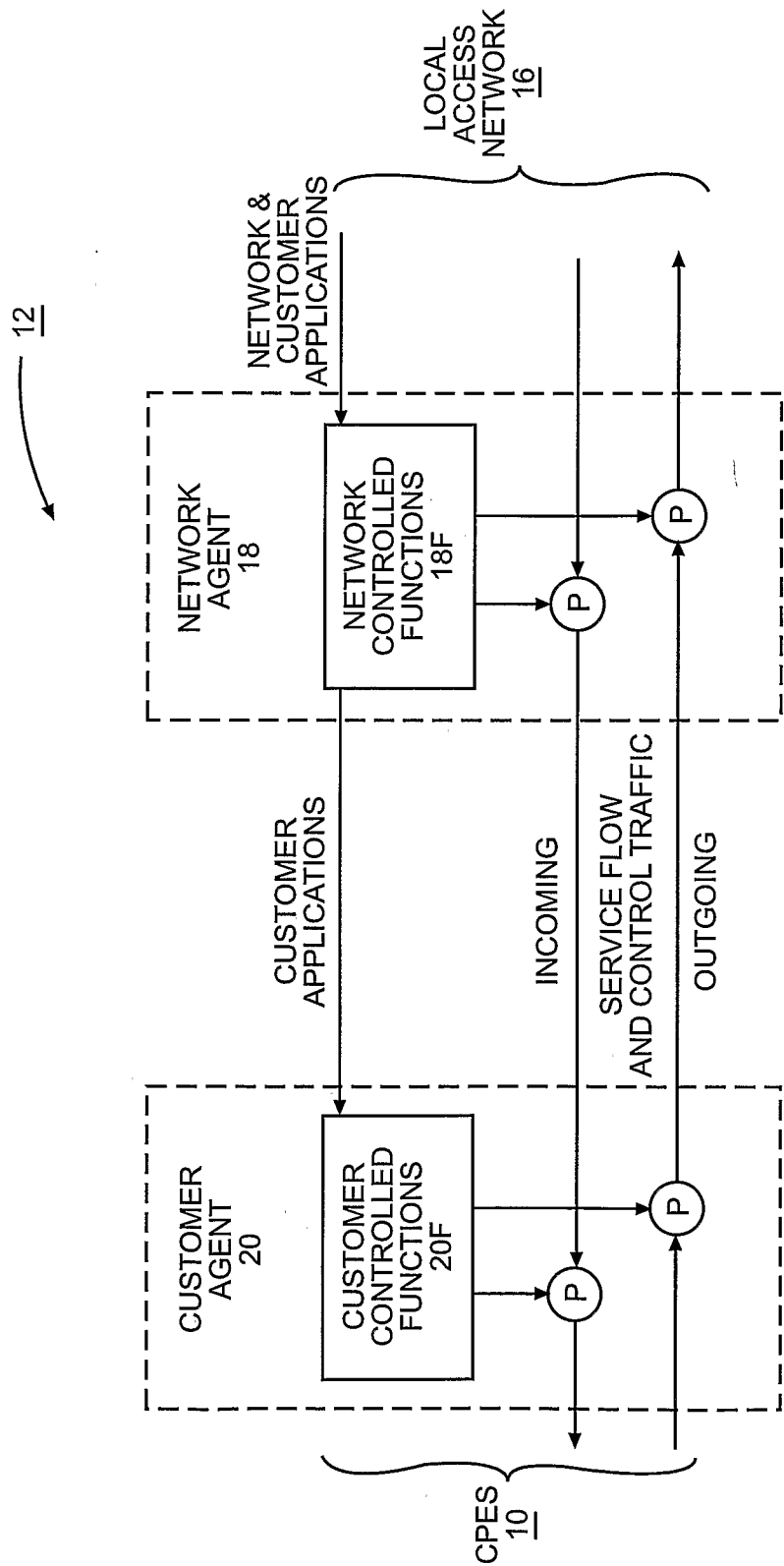


FIG. 2

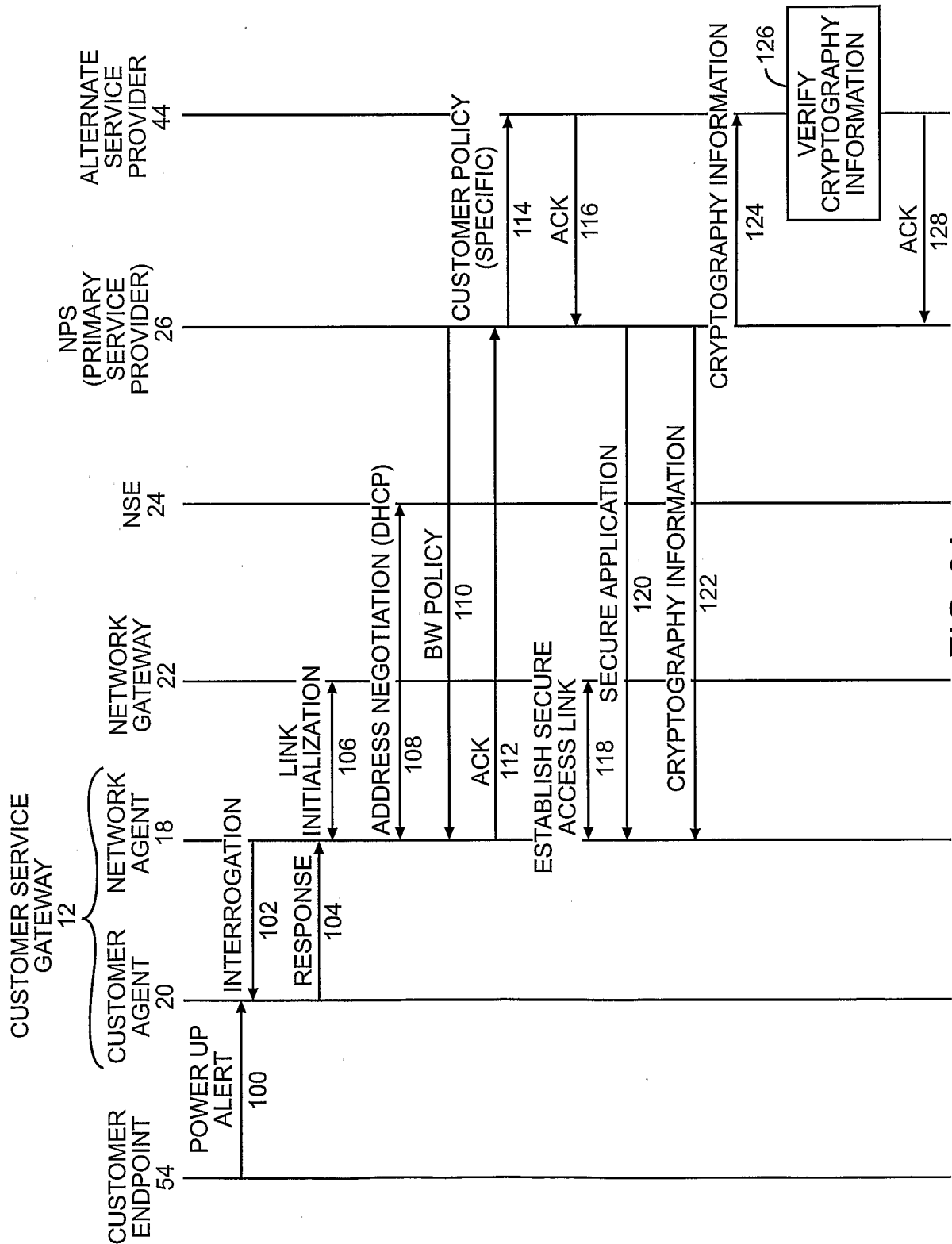
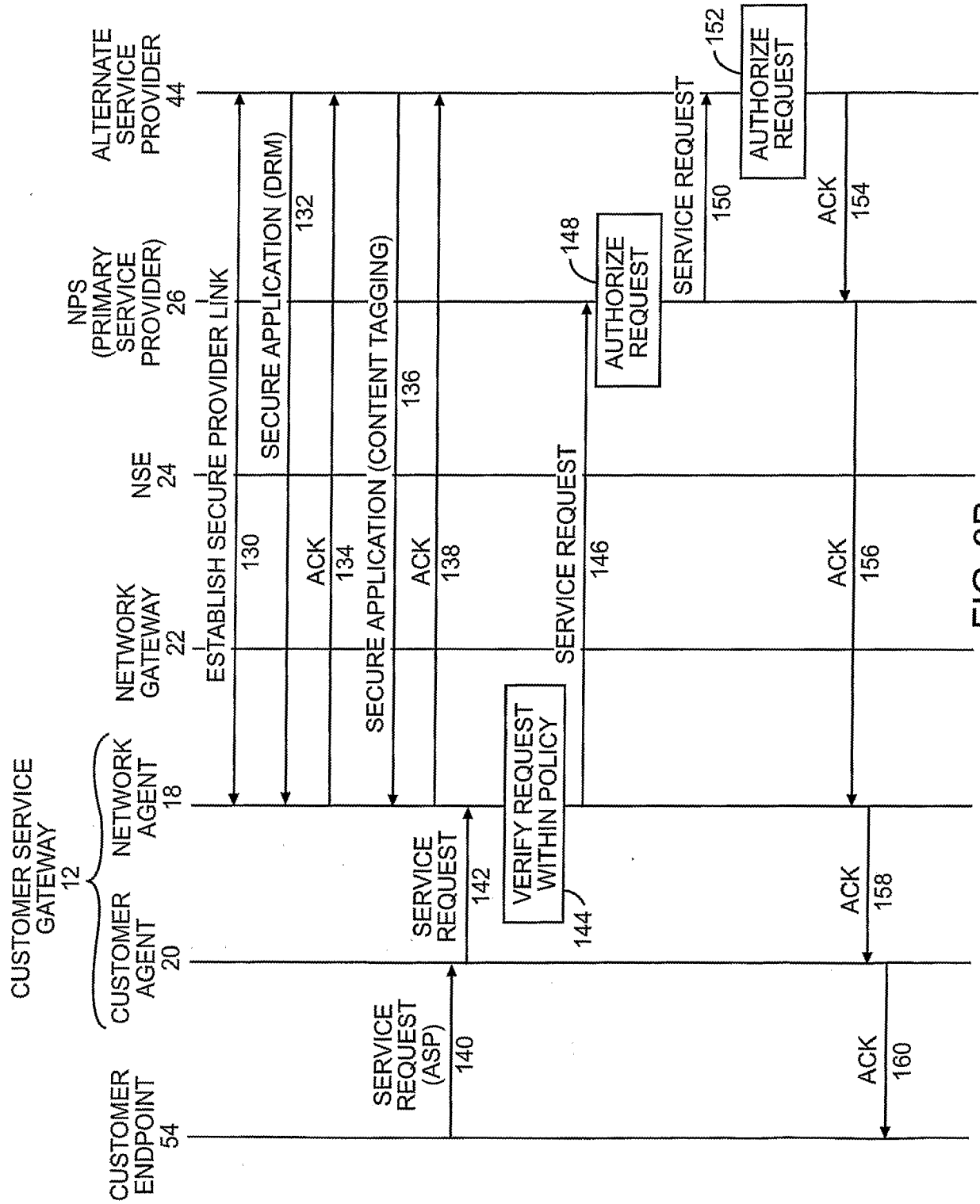


FIG. 3A



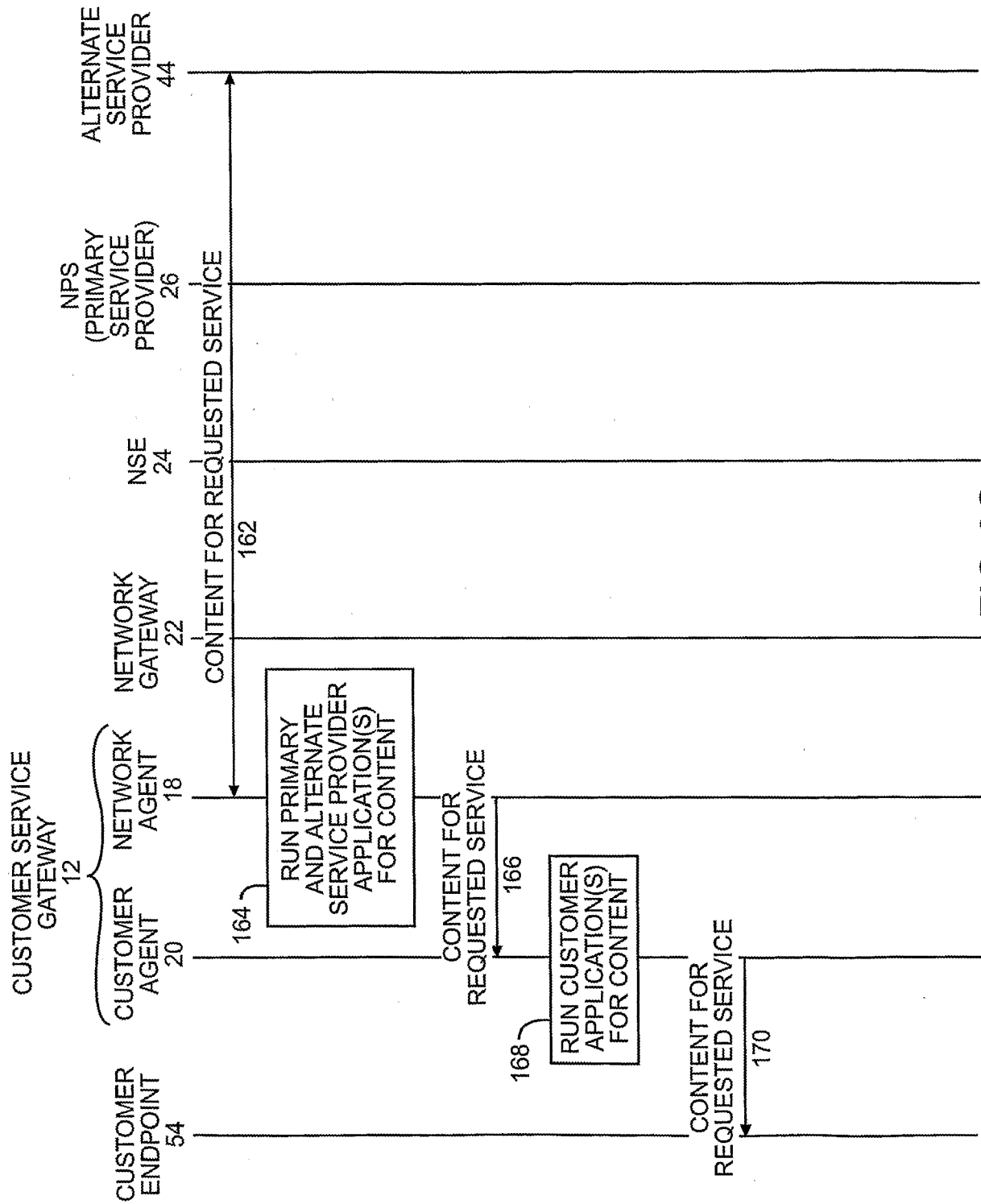


FIG. 3C

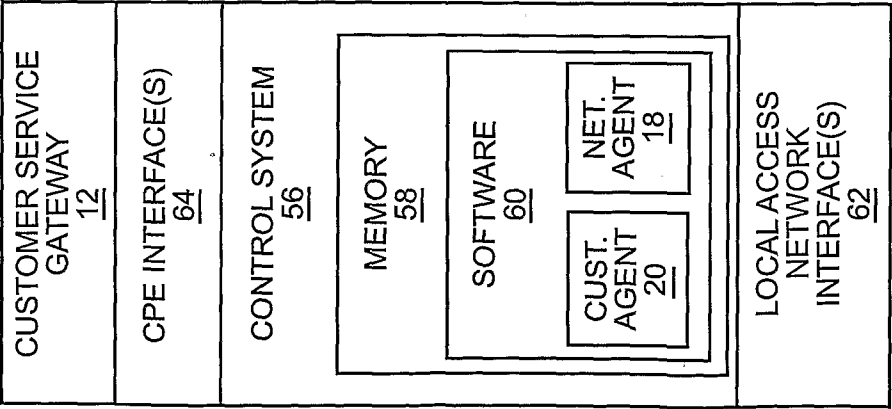


FIG. 4

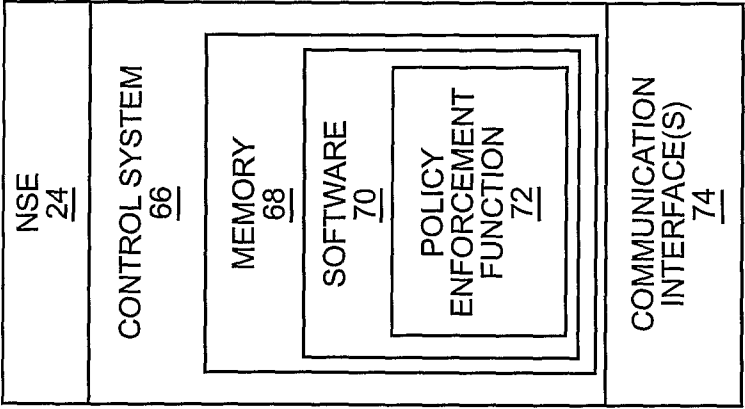


FIG. 5

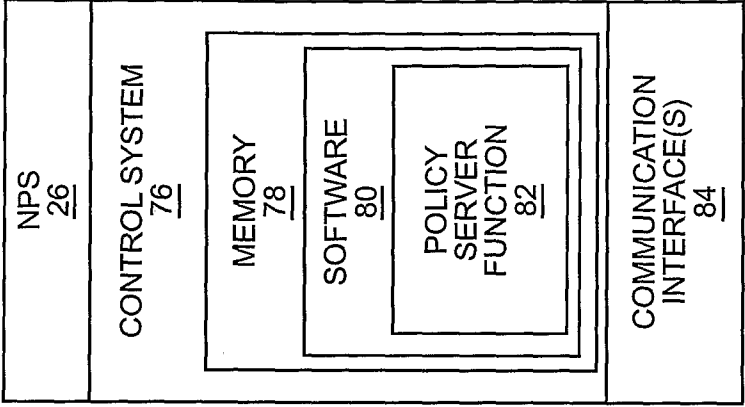


FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2006/002035

A. CLASSIFICATION OF SUBJECT MATTER IPC: H04L 29/02 (2006.01) , H04L 12/16 (2006.01) , H04L 12/66 (2006.01) , H04M 11/06 (2006.01) , H04N 7/173 (2006.01) According to International Patent Classification (IPC) or to both national classification and IPC											
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC: H04L, H04M, H04N Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used) Delphion, Derwent: network agent, gateway, secure, service, control, network, web, LAN											
C. DOCUMENTS CONSIDERED TO BE RELEVANT <table border="1"> <thead> <tr> <th>Category*</th> <th>Citation of document, with indication, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>EP 0 895 374 A2 Fujino et al., 03 February 1999 (03-02-1999), abstract, paragraphs [0011-0018], [0047-0048], [0104-0106], figures 1, 4A and 4B, 5 and 7.</td> <td>1-6, 15, 18-22</td> </tr> <tr> <td>A</td> <td>US 2003/0236997 A1 Jacobson, 25 December 2003 (25-12-2003), whole document.</td> <td>1-22</td> </tr> </tbody> </table>			Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	X	EP 0 895 374 A2 Fujino et al., 03 February 1999 (03-02-1999), abstract, paragraphs [0011-0018], [0047-0048], [0104-0106], figures 1, 4A and 4B, 5 and 7.	1-6, 15, 18-22	A	US 2003/0236997 A1 Jacobson, 25 December 2003 (25-12-2003), whole document.	1-22
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.									
X	EP 0 895 374 A2 Fujino et al., 03 February 1999 (03-02-1999), abstract, paragraphs [0011-0018], [0047-0048], [0104-0106], figures 1, 4A and 4B, 5 and 7.	1-6, 15, 18-22									
A	US 2003/0236997 A1 Jacobson, 25 December 2003 (25-12-2003), whole document.	1-22									
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex. <table border="1"> <tr> <td> * Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed </td> <td> "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family </td> </tr> </table>			* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family							
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family										
Date of the actual completion of the international search 02 March 2007 (02-03-2007)		Date of mailing of the international search report 6 March 2007 (06-03-2007)									
Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001-819-953-2476		Authorized officer Stuart Ginn 819- 934-5147									

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2006/002035

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
EP0895374	03-02-1999	JP11055324 A US6085222 A	26-02-1999 04-07-2000
US2003236997	25-12-2003	AU2003251583 A1 WO2004002111 A1	06-01-2004 31-12-2003