



(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/EP2010/050303

(22) International Filing Date:
12 January 2010 (12.01.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09170588.9 17 September 2009 (17.09.2009) EP

(71) Applicant (for all designated States except US): **NOKIA SIEMENS NETWORKS OY** [FI/FI]; Karaportti 3, FI-02610 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **JANK, Uwe** [DE/DE]; Gartenstrasse 54, 14612 Falkensee (DE). **KO-RTWICH, Christian** [DE/DE]; Tile-Brügge-Weg 79, 13509 Berlin (DE).

AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

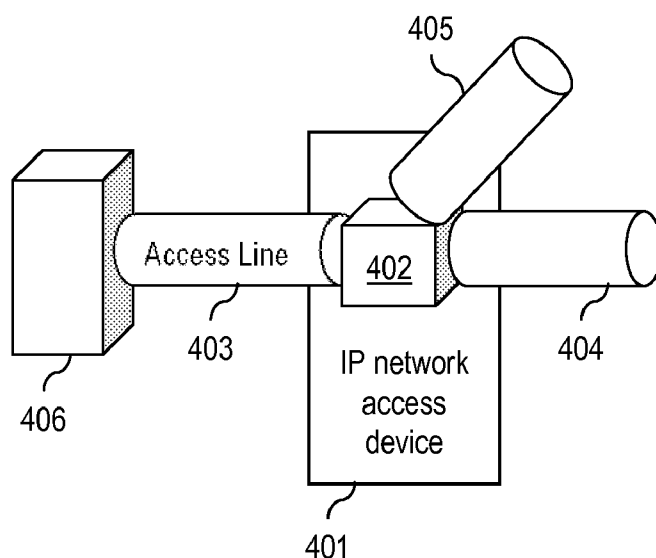
Published:

— with international search report (Art. 21(3))

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

(54) Title: METHOD AND DEVICE FOR PROCESSING DATA IN A NETWORK

Fig.4



(57) Abstract: A method and a device for processing data in a network are provided, wherein based on a request conveyed via an access line, a virtual network is dynamically adjusted by at least one network access device. Also, a communication system is suggested comprising at least one such device.

DescriptionMethod and device for processing data in a network

5 The invention relates to a method and to a device for processing data in a network. Also, a communication system is suggested comprising at least one such device.

10 Network operators offer different kinds of access to the Internet, e.g., via DSL or mobile (cellular) phones. Such Internet access can be used by customers or applications transferring data over a network (e.g., an IP) layer. The Internet access provided is mainly directed to IP-based transport of data utilizing one level of quality of service (QoS), in most
15 cases according to a "best effort" scheme.

This scenario bears the disadvantage that a direct connection between end user applications is not feasible without an interaction of a (third party) server or application.

20

It is also detrimental that a quality of service level cannot be dynamically assigned to a connection that is set up across the Internet in an easy and cost-efficient manner. An example of such QoS level refers to a latency of data transfer, which
25 is important for users running applications that require interaction with as little delay as possible (e.g., application sharing or online gaming).

The **problem** to be solved is to overcome the disadvantages
30 stated above and in particular to provide a solution that allows utilizing a private or a virtual network (in particular LAN) via an IP-based network, e.g., on a temporary basis and/or with a particular QoS level.

35 This problem is solved according to the features of the independent claims. Further embodiments result from the depending claims.

In order to overcome this problem, a method for processing data in a network, in particular an IP network, is provided

- wherein based on a request conveyed via an access line, a virtual network is dynamically adjusted by at least one network access device.

It is noted that the virtual network provides a virtual network service to several entities (users, applications or devices), which can be interconnected by the virtual network and can utilize particular services or quality of service levels that are supplied by said virtual network.

It is further noted that the virtual network could also be referred to as a private network or an emulated virtual network or an emulated private network. The network may be a local area network (LAN). The network access device may be an IP network access device.

This approach in particular enables access to IP-based networks and provides additional dynamic connections of IP-based devices with dedicated connection requirements, like QoS level, link layer broadcast capability, etc.

Advantageously, the approach provided enables using link layer broadcast protocols between entities, e.g., terminal devices, applications or users.

The approach further enables a cost efficient way to realize predefined (e.g., high) QoS-levels, e.g., for online gaming applications or video conferencing applications or shared medical applications (wherein several users participate in one medical scenario, e.g., operation, wherein at least some of the users are remotely connected via the network). These scenario in particular relate to a connection that temporarily allows for such particular QoS level, e.g., for the duration of the game or the medical interaction.

In an embodiment, the virtual network is temporarily active.

Hence, the virtual network in this case may also be referred to as transient virtual network.

- 5 In another embodiment, based on the request, the at least one network access device conducts at least one of the following steps:
- the at least one network access device authenticates and/or authorizes the requesting entity;
 - 10 - the at least one network access device checks an availability of a QoS level requested and in particular, if feasible and admissible, reserves resources for provisioning of this QoS level requested;
 - the at least one network access device checks paths
 - 15 of emulated wires for suspicious segments;
 - the at least one network access device determines charging and/or billing information.

If the required checks have been successfully completed, the
20 access line or tunnel is connected to the virtual network.

In a further embodiment, the request conveyed via the access line is triggered by a user, a device or an application connected to the access line.

25

In a next embodiment, the request comprises an authorization of the user, the device or the application.

The network access device may receive and validate such
30 authorization of the requesting entity (e.g., user, application or terminal device). Based on the authorization a decision could be made (by the network access device) whether or not the virtual network service will (still) be provided, i.e., whether the entity is allowed to connect to the virtual
35 network or whether to adjust the virtual network pursuant to the entity's request.

It is also an embodiment that the virtual network is dynamically adjusted comprising at least one of the following:

- setting up the virtual network or a portion thereof;
- tearing down the virtual network or a portion thereof;
- configuring the virtual network or a portion thereof.

Dynamically adjusting the virtual network also refers to adjusting a connection of or to the virtual network.

Pursuant to another embodiment, the virtual network is adjusted

- by connecting or disconnecting at least one emulated wire with a forwarding engine of the at least one network access device;
- by connecting or disconnecting the access line with the forwarding engine.

The forwarding engine may provide a routing or switching function for the virtual network.

Hence, the emulated wires may intermesh the network access devices in a way that for all connected devices or applications a single broadcast medium is provided.

Ethernet MAC address learning may be utilized in order to increase the efficiency of the forwarding engine.

According to an embodiment, the forwarding engine provides layer-3 and/or layer-2 forwarding services.

It is noted that the forwarding engine may supply broadcast and/or multicast capabilities. This advantageously allows for spanning a broadcast (or multicast) domain over a large geographic region.

According to another embodiment, the virtual network provides a quality of service level.

The quality of service (QoS) level can be set via the request conveyed by the access line or it may be predefined for the particular virtual network service requested. The network access device may check during the setup of the service whether or not this QoS level requested could be provided from the available network resources.

In yet another embodiment, based on the request, an ad-hoc setup is conducted.

Such ad-hoc setup may configure a complete (sub-)set of emulated wires for the network access devices involved based on an (initial) request of an entity (user, terminal device or application). This requires retrieving information regarding all emulated wire destinations, be it from a locally stored database or from a remote database by using an appropriate database access protocol. It is noted that such information can be distributed among several sources, e.g., databases, throughout the network.

According to a next embodiment, based on the request, an incremental adjustment of the virtual network is conducted.

On demand of an entity (user, terminal device or application), the IP network access device may configure, set up or select emulated wires to those forwarding engines, which are already connected and are part of the virtual network. Hence, data about such destinations from a locally or remotely accessible database may be retrieved. Said database can be dynamically updated with related information about any forwarding engine joining or leaving the virtual network service. In particular, a centrally accessible database can be provided, related database access information can be set up to be accessible to all IP network access devices supporting such service.

The problem mentioned above is also solved by a network access device

- comprising at least one forwarding engine for being connected to at least one emulated wire,
- 5 - wherein the at least one forwarding engine is connected to at least one access line,
- wherein based on a request conveyed via the at least one access line, a virtual network utilizing said at least one emulated wire and the at least one forwarding engine is dynamically adjustable.
- 10

This network access device may thus operate as indicated above and will in more details explained hereinafter.

- 15 The problem stated above is also solved by a device comprising a processing unit that is arranged such that the steps of the method described are executable thereon.

20 This device may be a network access device, in particular an IP network access device. The device may also be associated with any such access device.

25 The device may also be a terminal device or user device that triggers the request to dynamically adjust the virtual network.

30 It is further noted that said processing unit can comprise at least one, in particular several means that are arranged to execute the steps of the method described herein. The means may be logically or physically separated; in particular several logically separate means could be combined in at least one physical unit.

35 Said processing unit may comprise at least one of the following: a processor, a microcontroller, a hard-wired circuit, an ASIC, an FPGA, a logic device.

The solution provided herein further comprises a computer program product directly loadable into a memory of a digital computer, comprising software code portions for performing the steps of the method as described herein.

5

In addition, the problem stated above is solved by a computer-readable medium, e.g., storage of any kind, having computer-executable instructions adapted to cause a computer system to perform the method as described herein.

10

Furthermore, the problem stated above is solved by a communication system comprising at least one device as described herein.

15 Embodiments of the invention are shown and illustrated in the following figures:

Fig.1 shows a schematic diagram depicting a basic approach to utilize a transient emulated private LAN via an IP-based network;

20

Fig.2 shows a flow chart depicting a sequence of messages and operations for setting up an access line of a device, wherein the device requests access to a transient emulated private LAN through an IP-based network;

25

Fig.3 shows an extension of the schematic diagram presented in Fig.1 to cope with different autonomous domains of the IP-based network;

30

Fig.4 shows a schematic diagram of a network access device, which is in particular an IP network access device, that comprises a forwarding engine and is connected via said forwarding engine to an access line and the forwarding engine is connected to emulated wires;

35

Fig.5 shows a schematic message flow for setting up a (fully meshed) virtual network.

An IP network infrastructure deploys technologies and protocols, which are capable of emulating wires between edges of the IP network. Moreover, it is possible to deploy non-IP technology, implemented in the IP network devices, for these emulated wires thereby protecting the emulated wires and thus the data conveyed across from threats that are based on IP technology.

A set of emulated wires, e.g., together with layer-2 forwarding engines, can be used to provide an emulated Local Area Network (LAN) for all connected terminals. An example of such a service is the so called Virtual Private LAN Service (VPLS) in MPLS enabled networks as defined by the IETF standards.

The approach provided herein in particular comprises IP network access devices that provide access for IP based devices as follows:

- A common access to the IP based network as known and already implemented today (e.g., DSL, GPRS, UMTS).
- On request, a (transient) virtual network (also referred to as emulated private LAN) can be set up with other devices or applications connected to the same IP network (e.g., the Internet).

It is in particular suggested that the virtual network is dynamically set up pursuant to a request of an entity (e.g., a user, a terminal or an application) for an access line. Hence, the request for an access line may lead to a service provided by a component of the network, e.g., the network access device. Such request may be a direct request from the entity or any network-based interaction between the entity and the network access device.

It is noted that the virtual network as referred to herein may optionally be transient, i.e. set up and/or configured

for a limited period of time. This advantageously allows for a cost-efficient approach to provide, e.g., high level QoS for a predefined duration that may be associated with an application running. This efficiently avoids expensive special permanent connections providing high level QoS persistently, but at high cost.

The virtual network may comprise emulated wires across the IP-based network and associated layer-2 forwarding engines in the IP network access devices. Hence, the emulated wires may intermesh the IP network access devices in a way that for all connected devices or applications a single broadcast medium is provided. An example is a direct connection of two terminals' access lines via a single emulated wire.

A deployment of non-IP-based transport technology throughout the IP network infrastructure for the transient wired connections significantly increases the security. A non-IP-based transport technology is transparent to the IP-layer and allows using existing (and often complex) configurations of the terminal devices.

Security of the service could be further increased by utilizing special approaches (e.g., usual OAM protocol methods) to trace paths of the emulated wires through the IP network and thus to detect any suspicious path segments (e.g., redirections to malicious devices). This can be done prior to the emulated wires actually being used for conveying traffic.

Before or during setup of the (transient) virtual network, the requesting user or device could also request a QoS level (e.g., providing an average and a maximum latency) for the service. The IP network access device may check during the setup of the service whether or not this QoS level requested could be provided from the available network resources.

The result of this check could be used to decide whether or not the virtual network will nevertheless be set up. This de-

cision may be made automatically by the IP network access device or - after having signaled the result - by the requesting entity, e.g., user, application or terminal device.

5 The IP network access device may provide appropriate procedures before or during the setup of the service that allows authorizing the requesting entity (e.g., user, application or terminal device). Based on such authorization a decision could be made (by the IP network access device) whether or
10 not the service will still be provided.

The IP network access device may convey information about the service usage to particular devices, e.g., charging and billing systems. This could be achieved, e.g., by using RADIUS
15 or DIAMETER protocol messages towards affected servers.

The requested and/or provided QoS level could also be used for charging purposes related to the service requested, in particular by using an appropriate tariff model.

20

Further Implementation Details:

In this example, a transient emulated private LAN is chosen as an example for a virtual network. However, any virtual
25 network (persistent or transient) may be utilized accordingly.

A request for a transient emulated private LAN can be signaled by using the access protocol between the device to be
30 connected (e.g., a PC or a mobile phone) and an IP network access device. Existing access protocols may be adjusted accordingly for that purpose, in case available signaling does not allow for such a request to be appropriately processed.

35 Based on this request, the IP network access device may set up transient emulations of wires (emulated wires) to all participating IP network access devices throughout the IP net-

work as well as a local (e.g., layer-2) forwarding engine, and may further (in particular optionally)

- authorize the requesting entity (e.g., user, application or device),
- 5 - check the availability of a QoS level requested and - if feasible and admissible - reserve the resources for provisioning of this QoS level requested,
- check paths of the wires for suspicious segments;
- provide appropriate charging or billing information.

10

If the required checks have been successfully completed, the access line or tunnel requested will be connected to the (transient) emulated private LAN.

15 **Fig.1** shows a schematic diagram depicting a basic approach to utilize a transient emulated private LAN via an IP-based network.

In Fig.1, each of devices 101 to 104 requests the same "emulated private LAN" service via its access line 105 to 108.
20 The access line 105 connects the device 101 with a transient layer-2 forwarding engine 116 of an IP network access device 109, the access line 106 connects the device 102 with a transient layer-2 forwarding engine 117 of an IP network access
25 device 110, the access line 107 connects the device 103 with a transient layer-2 forwarding engine 118 of an IP network access device 111 and the access line 108 connects the device 104 with the transient layer-2 forwarding engine 118 of the IP network access device 111.

30

An IP-based network 112 provides the services of the emulated private LAN, wherein a transient emulated wire 113 connects the transient layer-2 forwarding engine 116 of the IP network access device 109 with the transient layer-2 forwarding engine 117 of the IP network access device 110, a transient emulated wire 114 connects the transient layer-2 forwarding engine 117 of the IP network access device 110 with the transient layer-2 forwarding engine 118 of the IP network access
35

device 111 and a transient emulated wire 115 connects the transient layer-2 forwarding engine 118 of the IP network access device 111 with the transient layer-2 forwarding engine 116 of the IP network access device 109.

5

Fig.2 shows a flow chart depicting a sequence of messages and operations for setting up an access line of a device, wherein the device requests access to a transient emulated private LAN through an IP-based network.

10

A device 201 requesting the service of a transient emulated private LAN through an IP network sends an according request 202 to an IP network access device 203. The IP network access device 203 may conduct several optional checks, e.g., whether the device 201 is authorized to obtain access to the transient emulated private LAN, whether the QoS requested is available, etc. (see operation 204).

15

If the optional checks confirm that access to the transient emulated private LAN shall be provided for the device 201, the IP network access device 203 sets up an emulated private LAN towards another IP network access device 205 (see message 206). The message 206 is acknowledged by a response 207 from the IP network access device 205.

20

25

As an option, the IP network access device 203 may check whether or not the paths of the wires are subject to a malicious use, i.e. whether there are suspicious segments on the paths to the IP network access device 205 (see messages 208 and 209).

30

The IP network access device 203 attaches in a step 210 the access line of the device 201 to the transient emulated private LAN.

35

In a step 211, the IP network access device 203 may conduct charging operations regarding the attachment of the device

201 to the transient emulated private LAN, e.g., dependent also on the QoS level provided.

5 The setup of the access line is confirmed via a message 212 sent from the IP network access device 203 to the device 201.

Next, user traffic 213 can be conveyed between the device 201 and a device 214 that has already been connected to the transient emulated private LAN.

10

After the transmission of user traffic 213 is finished or the participation of the device 201 in the transient emulated private LAN is no longer required, the device 201 sends a release access line message 215 to the IP network access device 15 203. The IP network access device 203 detaches the access line from the transient emulated private LAN (see operation 216). A communication 217 between the IP network access device 203 and the IP network access device 205 indicates that the transient emulated private LAN or a part of it is torn 20 down. This, however, may be only applicable in case (this part of) the transient emulated private LAN is no longer required, e.g., in case no other devices are still connected utilizing this service.

25 Devices that need to be connected to other access devices of the emulated private LAN may utilize the same procedure. Each device may be permanently connected or it may provide at least one permanently available "wire end point".

30 An exemplary scenario may utilize a non-IP-based transport across the IP network, e.g., using MPLS-based pseudo-wire services (e.g., multi-segmented PWE3) and VPLS according to IETF standards.

35 Different IP network domains, in particular as used throughout the Internet, may deploy different technologies for providing "wire" segments. In particular domain edges may be re-

quired to connect "wire" segments in a suitable manner, similar to a phone call setup in an SS#7 network.

Fig.3 shows an extension of the schematic diagram presented

5 in Fig.1 to cope with different autonomous domains of the IP-based network. Such different domains could be found in the public Internet. The transient emulated private LAN could be utilized across a deployment of segmented wires even in case different technologies for emulating the transient wire are
10 deployed or in case different administrative domains require terminating the wire emulation at the edge or (domain) border gateway. Advantageously, the domain border gateways only need to support segmented wire emulations.

15 According to Fig.3, each of devices 301 to 303 requests a service "emulated private LAN" via its access line 304 to 306. The access line 304 connects the device 301 with a transient layer-2 forwarding engine 307 of an IP network access device 310, the access line 305 connects the device 302 with
20 a transient layer-2 forwarding engine 308 of an IP network access device 311 and the access line 306 connects the device 303 with a transient layer-2 forwarding engine 309 of an IP network access device 312.

25 IP-based networks 313 and 314 provide the services of the emulated private LAN, wherein IP network domain border gateways 319, 320 are located between the IP-based networks 313 and 314. The IP network access devices 310 and 312 are located in the IP-based network 314 and the IP network access device 311 is located in the IP-based network 313.
30

A transient emulated wire segment 321 connects the transient layer-2 forwarding engine 307 of the IP network access device 310 via the IP network domain border gateway 319 with a transient emulated wire segment 315 that is connected to the
35 transient layer-2 forwarding engine 308 of the IP network access device 311.

A transient emulated wire segment 316 connects the transient layer-2 forwarding engine 308 of the IP network access device 311 via the IP network domain border gateway 320 with a transient emulated wire segment 317 that is connected to the transient layer-2 forwarding engine 309 of the IP network access device 312.

A transient emulated wire 318 connects the transient layer-2 forwarding engine 307 of the IP network access device 310 with the transient layer-2 forwarding engine 309 of the IP network access device 312.

The Network Access Device

Fig. 4 shows a schematic diagram of a network access device 401, which is in particular an IP network access device that comprises a forwarding engine 402 and is connected via said forwarding engine 402 to an access line 403. Also, the forwarding engine 402 is connected to emulated wires 404 and 405 (that could also be referred to as pseudo-wires), which may be segments of emulated wires (in case border gateways to other networks are involved as shown in Fig.3).

An entity 406, e.g., a user, a terminal device or an application, may utilize the access line to set up, configure, or tear down its connection to a virtual network, e.g., an emulated private LAN via said access line 403. The entity may use at least one (transient) emulated wire to get connected to the virtual network. The forwarding engine 402 may switch traffic between the access line 403 and the emulated wires 404, 405.

It is also possible that a pool of statically configured emulated wires is available, which are not transient, but may exist (semi-)permanently (e.g., in a pool). In addition, a pool of forwarding engines could be available in a (semi)-permanent manner. Also, the network access device 401 may comprise several forwarding engines 402.

The approach suggested herewith in particular allows dynamically setting up and tearing down an interconnection of emulated or pseudo wire(s), forwarding engine(s) and access line(s) triggered via the access line, e.g., pursuant to a request from the entity.

The network access device may be an IP network access device, based on or associated with, e.g., a BRAS, a DSLAM, a GGSN, related nodes according to an LTE architecture, a WIMAX or a WLAN access point etc. The network access device may be a device to which the entity can be connected via an access line. Access lines between the entity and the network access device may be direct connections via dedicated physical links (e.g., DSL lines) or protocol tunnels on any layer like PPPoE through a DSL or optical line, a GTP tunnel according to GPRS or UMTS networks or even a wireless link.

An interconnection of multiple such forwarding engines via emulated wires, especially when being fully meshed, forms a (segment of a) virtual network, optionally a transient virtual network.

The (segment of the) virtual network may be set up on demand of the entity, e.g., a user, a terminal device or an application. The virtual network may provide and/or offer (e.g., optionally) special services.

The network access device supports at least one emulated wire, at least one forwarding engine and at least one access line.

The forwarding engine forwards any protocol frame received from any of the emulated wires towards the access line and vice versa forwards any protocol frame received from the access line towards its destination emulated wire or, if the destination is not known at the (transient) forwarding engine, to all emulated wires connected.

Any protocol frame received from any emulated wire may not be forwarded into any other or the same pseudo-wire. This ensures that traffic terminates and does not endlessly travel throughout the emulated wires.

If the protocol to be switched by this network access device supports broadcast and/or multicast services (e.g., like Ethernet broadcast), broadcasting and/or multicasting of protocol frames can be supported by the forwarding engine.

An interconnection of the forwarding engine with at least one emulated wire and at least one access line may advantageously be triggered by a request from an access line protocol. For example, such connection may be made (immediately) after the configuration has been completed (successfully).

The network access device may support more than one access line at the same time and it may provide in particular at least one of the following mechanisms:

(a) Connecting multiple access lines to the same forwarding engine on demand for a particular service and forwarding data between all access lines and all emulated wires may be conducted as follows:

- The network access device may forward any frame received from an access line towards its destination access line or destination emulated wire or to all emulated wires and access lines attached in case the destination is not known.
- The network access device may forward any frame received from any emulated wire towards its destination access line or all of them, but not into any emulated wire.

(b) Setting up and tearing down of multiple combinations of forwarding engines and related emulated wires may be conducted as specified above if different access lines

require different services. In this case, resource management may be required for forwarding engines and emulated wires, and mechanisms for handling lack of such resources may also be supplied.

5

If an IP network access device supports this approach also with regard to provisioning dedicated QoS levels for the forwarding of data traffic (e.g., a certain maximum latency of frames or a guaranteed particular bandwidth), it will advantageously implement related resource management and mechanisms for handling a lack of such resources.

10

Options for the Implementation of the Network and Service

15

(a) Ad-hoc setup:

20

An ad-hoc setup of the complete set of emulated wires and forwarding engines for the network access devices involved can be provided based on a first request of an entity (user, terminal device or application). This requires retrieving information regarding all emulated wire destinations, be it from a locally stored database or from a remote database by using an appropriate database access protocol. It is noted that such information can be distributed among several sources, e.g., databases, throughout the network.

25

(b) Incrementally growing network:

30

On demand of an entity (user, terminal device or application), the IP network access device sets up or selects emulated wires to all forwarding engines, which are already connected and participating in the virtual network service. Hence, data about such destinations from a locally or remotely accessible database may be retrieved. Said database can be dynamically updated with related information about any forwarding engine joining or leaving the virtual network service. In particular, a centrally accessible database can be provided, related database access information can be set up to be accessible

35

to all IP network access devices supporting such service.

Access Line Protocols for Signaling the Service Request

5

No additional or new protocols, messages or message elements may be required for the access line to signal a demand for adjusting (in particular setting up) the virtual network.

10 Advantageously, as an option, additional AAA and security features could be provided or implemented.

PPPoE access over fixed lines supports addressing a service in a PPPoE Active Discovery Initiation message (PADI). Subscriber authentication could be provided according to known
15 PPPoE connections. Also, the known mechanisms for accounting could be used. Further AAA aspects might be handled in-band with the data traffic depending on the application using the virtual network service.

20

A setup of a mobile subscriber's data network connection, e.g., in GPRS or UMTS networks, uses "Activate PDP Context" messages, which address an Access Point Name (APN). This APN information element could be used to address the virtual network service, e.g., by using dedicated APN strings. Also, an
25 existing mechanism could be deployed to handle AAA aspects for this virtual network service.

A service address may be supplied to the user, terminal device or application. It may be done via separate (e.g., manual) communication means; however, other, also more sophisticated kinds of provisioning such information may be applicable (e.g., via a software installation CDROM or even via the IP network or related applications).

35

Protocol for the Forwarding Engine

Implementing the forwarding engine, the Ethernet seems a suitable protocol that meets several network scenarios (mobile, fixed). However, this approach is not restricted to the Ethernet. Ethernet MAC address learning may be utilized in order to increase the efficiency of the forwarding mechanism.

For access lines transferring layer 3 user data frames like for mobile subscribers, a special handling of user data frames could be provided: The data frames could be wrapped into layer 2 (e.g., Ethernet) frames before they are sent to the forwarding engine.

Also layer-3 technologies (e.g., IPv4 or IPv6 virtual routers) could be utilized for implementing the forwarding engine. However, there is no restriction to layer-3 technologies; in particular a layer-2 forwarding engine may provide additional options to the layer-3.

Utilizing a protocol with broadcast and multicast capabilities, the approach suggested herein could be used for spanning a single broadcast domain over large geographic regions, just on demand from an access line.

Emulated wires and Forwarding Engine

Several technologies could be used for implementing the emulated wires, e.g., VLAN stacking technologies, IP tunnels (e.g., IPsec), ATM VCs. Such technologies utilize some kind of encapsulation for the data frames that could be used transferring the data frames in a transparent manner and to address the remote end of the emulated wire.

Also, MPLS pseudo-wires could be used for the virtual network service suggested herein. The MPLS pseudo-wires are specified, e.g., by the IETF in RFC3985. Utilizing MPLS pseudo-wires allows connecting services across many operator and

network domains without any detrimental effect for the virtual network service described herein. This technology also provides means for handling QoS-related aspects, e.g., by utilizing protocols like RSVP-TE for the pseudo-wire setup as specified by the IETF. An exemplary protocol for a pseudo-wire setup is LDP as specified by the IETF. MPLS path vector monitoring could be used for security aspects, e.g., to check for suspicious path segments. An existing implementation for pseudo-wire and forwarding engine setup (e.g., so called VPLS according to RFC 4762) can be extended by a "setup on access line demand" instead of the actual "setup on configuration".

Service Trigger

- 15 This "setup on access line demand" can be triggered by the information in the access line protocol sent by the entity (e.g., user, terminal device or application). Thus, a "service trigger" can be implemented in the access line protocol, which in particular
- 20 - interrupts the further setup of the access line;
 - optionally performs related checks (e.g., authentication, resources);
 - sets up the emulated wires and forwarding engine if not done yet, and connects them;
 - 25 - optionally performs charging measures (e.g., using RADIUS and/or DIAMETER).

If these steps are successfully performed, the setup of the access line will be completed and the access line will get connected to the forwarding engine so that user data forwarding will be able to commence.

Ad-Hoc Setup

- 35 An advantageous implementation could be as follows: The address information of all remote forwarding engines to interconnect for a certain virtual network service is locally stored on all network access devices supporting this virtual

network service or the address information is accessible in a centrally located database.

In case of a local database being available in each of the
5 (IP) network access devices, based on the "service trigger" event, the (fully meshed) virtual network can be set up.

Fig.5 shows a schematic message flow for setting up a (fully meshed) virtual network. A device 501 requesting a virtual
10 network service, i.e., an access line to be connected to a transient emulated private LAN, sends a message 502 (comprising a PADI or a PADR message) to an IP network access device 503 thereby providing a service trigger 504.

15 The IP network access device 503 may conduct several optional checks, e.g., whether the device 501 is authorized to obtain access to the transient emulated private LAN, whether the specified QoS for the requested service is available, etc. (see operation 505).

20 If the optional checks confirm that access to the transient emulated private LAN shall be provided for the device 501, the IP network access device 503 sets up an emulated private LAN towards another IP network access device 506 (see message
25 507) conveying a service trigger 509. The message 507 is acknowledged by a response 508 from the IP network access device 506.

30 The IP network access device 506 sets up remaining emulated wires to other IP network access devices according to information obtained by the database (locally or centrally provided) pursuant to an operation 510.

35 As an option, the IP network access device 503 may check whether or not the paths of the emulated wires are subject to a malicious use, i.e. whether there are suspicious segments on the paths to the IP network access device 506 (see messa-

ges 511 and 512). This can be achieved, e.g., by utilizing an MPLS PING function.

Pursuant to a step 513, the IP network access device 503 sets up the forwarding engine and attaches all emulated wires and the access line of the device 501 to the transient emulated private LAN. In a step 514, the IP network access device 503 may conduct charging operations regarding the attachment of the device 501 to the transient emulated private LAN, e.g., dependent also on the QoS level provided.

According to a step 515, the IP network access device 506 sets up its forwarding engine and attaches all emulated wires.

The setup of the access line is confirmed via a message 516 (e.g., a PADS message) sent from the IP network access device 503 to the device 501.

A device 519 sends a message (e.g., a request for an access line to the transient emulated private LAN service via an, e.g., PADI or PADR message) to the IP network access device 506. In a step 518, the IP network may conduct several optional checks, e.g., whether the device 519 is authorized to obtain access to the transient emulated private LAN, whether the QoS requested is available, etc. If the optional checks confirm that access to the transient emulated private LAN shall be provided for the device 519, the IP network access device 506 attaches the access line to its forwarding engine and optionally provides charging services.

The setup of the access line is confirmed via a message 520 (e.g., a PADS message) sent from the IP network access device 506 to the device 519.

Next, user traffic 521 can be conveyed between the device 501 and a device 519.

After the transmission of user traffic 521 is finished or the participation of the device 501 in the transient emulated private LAN is no longer required, the device 501 sends a release access line message 522 (e.g., via a PADT message) to the IP network access device 503 providing a service trigger 523. The IP network access device 503 detaches the access line from the transient emulated private LAN (see operation 524).

Hence, the ad-hoc setup shows a second "service trigger" 504 and 509 in the IP network access devices when they get signaled the first request for setting up the emulated wire for the related virtual network service.

The schematic message flow of Fig.5 does not show tearing down of the whole ad-hoc service, it only indicates another service trigger 523, which may require separate signaling about the status of the access lines connected to the IP network access device 503.

20

For example, in a fully meshed network a status message (e.g. a notification message as defined for MPLS pseudo-wires using LDP as signaling protocol) could be provided, which is sent to all connected network access devices indicating whether a virtual network service is active or down in this device, i.e., whether or not there are access lines connected to the network access device. By evaluating status information from all connected network access devices and its own status, the particular network access device is able to trigger the tear down of the whole virtual network exactly when the very last access line gets disconnected from the service. That network access device may initiate a tear down similarly to the setup by signaling the tear down to its connected network access devices (e.g., providing a label release message as defined for MPLS pseudo-wires using LDP as signaling protocol).

Incrementally growing network

With regard to the incrementally growing network, additional protocols may be involved in particular because of a database that can be dynamically updated. However, the incrementally growing network approach could be extended such that creation, provisioning and tearing down of a virtual network service can be fully automated.

- 10 (a) Service creation, service withdrawal, provisioning and service database:

For service creation purposes (similarly to the service triggering as described for ad-hoc services) a subscriber (i.e., entity, e.g., user, terminal device or application) may trigger a service creation by addressing a dedicated "well-known" service in its request for an access line. The subscriber may get connected to an IMS-like system where a dedicated "in-band" protocol (e.g., a special extension based on a SIP according to RFC3261) is used to create and specify a new service in a database (referred to herein as "Service Database").

Here the subscriber may define, e.g., a service name, user account data (e.g., white and black lists, passwords), QoS profiles, whichever is supported by the network for accessing and using the virtual network service.

30 This approach could be used for the following business case: A user is charged when accessing the virtual network service, wherein a portion of the money paid by the service users is transferred to the user that creates this virtual network service.

35 The database activities may be conducted in-band between subscriber equipment and database (e.g., IMS) and may be fully transparent to the IP network access device. They

may also be performed via any usual (e.g., secured) Internet connection.

Hence, the subscriber creating the virtual network service may be responsible for distributing the access information for this virtual network service. The access information can be conveyed using various ways, e.g., verbal communication, email, paper, media of different kinds, etc.

This business scenario may be also utilized by an operator using other or the same means to create a new virtual network service via the database.

If any subscriber wants to access the service, this subscriber may add related information (service, authorization, etc.) to his access line request (usually by a user interface of a related application). Such related information may be provided via separate communication channels (phone, e-mail, etc.).

A withdrawal of the service could be conducted correspondingly to the creation of the service.

(b) Service Access and Usage:

Receiving a message requesting an access line to the virtual network service causes a "service trigger" in the IP network access device.

Such "service trigger" to JOIN a virtual network service can be implemented in the access line protocol implementation of the IP network access device, which in this case in particular

- interrupts the further setup of the access line;
- optionally performs related local checks (e.g., authentication, availability of resources);
- accesses the "Service Database" in order to, e.g.,

- optionally perform service checks, e.g., subscriber or access line authentication, authorization, accounting;
- adds its own address of the related forwarding engine in this IP network access device (optionally) together with additional data;
- retrieve addresses of all other forwarding engines of this service and (optionally) additional data;
- sets up the emulated wires to other forwarding engines as retrieved from the database, and sets up its own forwarding engine if not done yet, and connects them all;
- optionally performs charging measures (e.g. using RADIUS and/or DIAMETER);
- optionally performs further resource and/or security checks.

If these steps are completed successfully, the setup of the access line is done and the access line is connected to the forwarding engine so that user data forwarding can commence.

Thus, no implementation of a service trigger is needed in the IP network access device when an emulated wire is set up from a remote device. Such emulated wires are just set up and connected to the existing forwarding engine.

When a subscriber wants to stop using a virtual network service, the subscriber disconnects the access line by a related message of the access line protocol. This leads to a "service trigger" for a service LEAVE, which can be implemented in the access line protocol, to

- access the "Service Database" to, e.g.,
- optionally perform service accounting and other measures;
- (if this was the last local access line for this virtual network service) delete its own address of

the related forwarding engine in this IP network access device from the service database and (optionally) delete any additional data;

- tear down the emulated wires to other forwarding engines of this service, and tear down its own forwarding engine if not done yet (if this was the last local access line for this virtual network service);
- optionally perform charging measures (e.g., using RADIUS and/or DIAMETER)
- optionally perform further resource handling.

Hence, no dedicated measure for managing the tear down of the whole service is required to be implemented in the IP network access devices as this is managed at least indirectly via the "Service Database".

The access to the database might be implemented in the IP network access devices by any suitable protocol, e.g., by or based on dedicated SIP (RFC3261) specifications.

Exemplary Applications:

The approach provided herein applies to various applications.

For example, the virtual network service could be used for a geographically distributed LAN application, e.g., LAN gaming. This scenario can be combined with a high QoS regarding, e.g., a small latency or a maximum threshold of a latency value that must not be exceeded. Dedicated QoS management could be utilized for the emulated wires used in this transient emulated virtual LAN application. MPLS pseudo-wires can be used as emulated wires and traffic engineering of MPLS networks could be utilized in order to manage the QoS requirements.

In another example, geographically distributed IPv4 sub-networks could be provided with reduced routing effort by

combining all such IPv4 sub-networks to a (transient) emulated virtual LAN application.

Furthermore, the approach suggested could be used for next-
5 generation Internet architectures using the incrementally
growing network approach as described herein. Setup of (several) virtual network segments on demand could be conducted
only where and when needed, transporting any kind of traffic
(IPv4/IPv6/any other) between geographic locations could be
10 achieved without the need to implement all protocols in all
involved network devices; instead, only devices beyond the
access lines need to implement such new protocols. In this
scenario, the "core network" only needs to provide the IMS-
like database system for control purposes as described her-
15 ein, optionally including means or extensions for QoS, security or other service requirements.

List of Abbreviations:

	AAA	Authentication, Authorization and Accounting
	APN	Access Point Name
5	ATM	Asynchronous Transfer Mode
	BRAS	Broadband Remote Access Server
	DIAMETER	Diameter is a computer networking protocol for AAA
	DSL	Digital Subscriber Line
10	GGSN	Gateway GPRS Support Node
	GPRS	General Packet Radio Service
	IETF	Internet Engineering Task Force
	IP	Internet Protocol
	IPDSLAM	IP over DSL Access Multiplexer
15	IPsec	Internet Protocol security
	IMS	IP Multimedia Subsystem
	IT	Information Technology
	LAN	Local Area Network
	LDP	Label Distribution Protocol
20	LTE	Long Term Evolution (new mobile network standard family)
	MPLS	Multi-Protocol Label Switching
	OAM	Operation, Administration, Maintenance
	OEM	Original Equipment Manufacturer
25	PADI	PPPoE Active Discovery Initiation
	PADO	PPPoE Active Discovery Offer
	PADR	PPPoE Active Discovery Request
	PADS	PPPoE Active Discovery Session-confirmation
	PC	Personal Computer
30	PDP	Packet Data Protocol
	PPPoE	Point-to-Point Protocol over Ethernet
	PWE3	Pseudo-Wire Emulation Edge-to-Edge
	QoS	Quality of Service
	RADIUS	Remote Authentication Dial In User Service
35	RSVP-TE	Resource Reservation Protocol - Traffic Engineering
	SIP	Session Initiation Protocol
	SS#7	Signaling System number 7

	UMTS	Universal Mobile Telecommunications System
	VC	Virtual Channel
	VLAN	Virtual LAN
	VPLS	Virtual Private LAN Service
5	WiMAX	Worldwide interoperability for Microwave Access Forum
	WLAN	Wireless LAN

Claims:

1. A method for processing data in a network,
 - wherein based on a request conveyed via an access line, a virtual network is dynamically adjusted by at least one network access device.
2. The method according to claim 1, wherein the virtual network is temporarily active.
3. The method according to any of the preceding claims, wherein based on the request, the at least one network access device conducts at least one of the following steps:
 - the at least one network access device authenticates and/or authorizes the requesting entity;
 - the at least one network access device checks an availability of a QoS level requested and in particular, if feasible and admissible, reserves resources for provisioning of this QoS level requested;
 - the at least one network access device checks paths of emulated wires for suspicious segments;
 - the at least one network access device determines charging and/or billing information.
4. The method according to any of the preceding claims, wherein the request conveyed via the access line is triggered by a user, a device or an application connected to the access line.
5. The method according to claim 4, wherein the request comprises an authorization of the user, the device or the application.
6. The method according to any of the preceding claims, wherein the virtual network is dynamically adjusted comprising at least one of the following:
 - setting up the virtual network or a portion thereof;
 - tearing down the virtual network or a portion thereof;

- configuring the virtual network or a portion thereof.

7. The method according to any of the preceding claims, wherein the virtual network is adjusted

- by connecting or disconnecting at least one emulated wire with a forwarding engine of the at least one network access device;
- by connecting or disconnecting the access line with the forwarding engine.

8. The method according to claim 7, wherein the forwarding engine provides layer-3 and/or layer-2 forwarding services.

9. The method according to any of the preceding claims, wherein the virtual network provides a quality of service level.

10. The method according to any of the preceding claims, wherein based on the request, an ad-hoc setup is conducted.

11. The method according to any of the preceding claims, wherein based on the request, an incremental adjustment of the virtual network is conducted.

12. A network access device

- comprising at least one forwarding engine for being connected to at least one emulated wire,
- wherein the at least one forwarding engine is connected to at least one access line,
- wherein based on a request conveyed via the at least one access line, a virtual network utilizing said at least one emulated wire and the at least one forwarding engine is dynamically adjustable.

13. A device comprising a processing unit that is arranged such that the method according to any of claims 1 to 11 is executable thereon.

14. The device according to claim 13, wherein said device is a network access device or a terminal device that triggers the request to dynamically adjust the virtual network.
- 5 15. A communication system comprising at least one device according to any of claims 12 to 14.

Fig.1

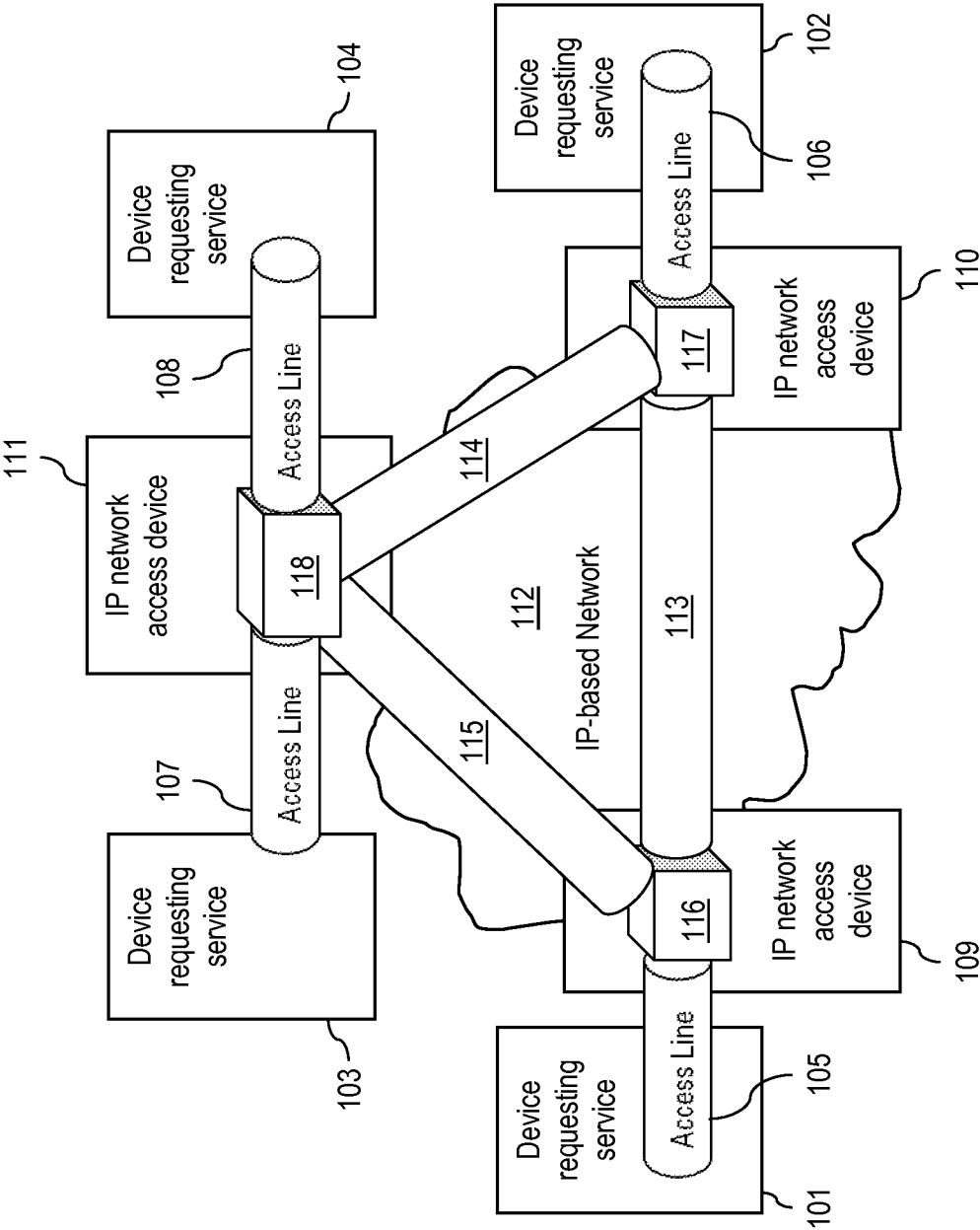


Fig.2

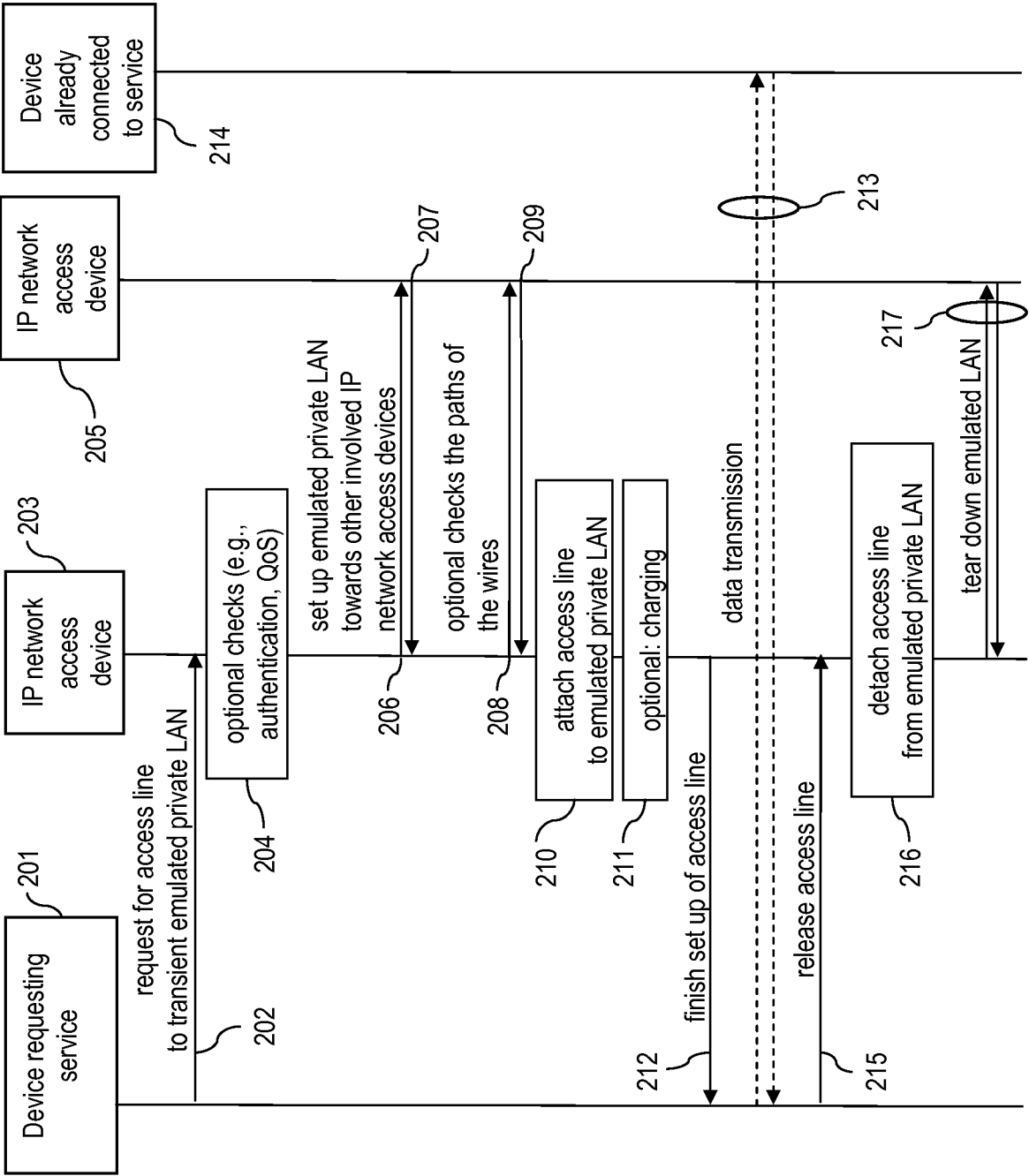


Fig.3

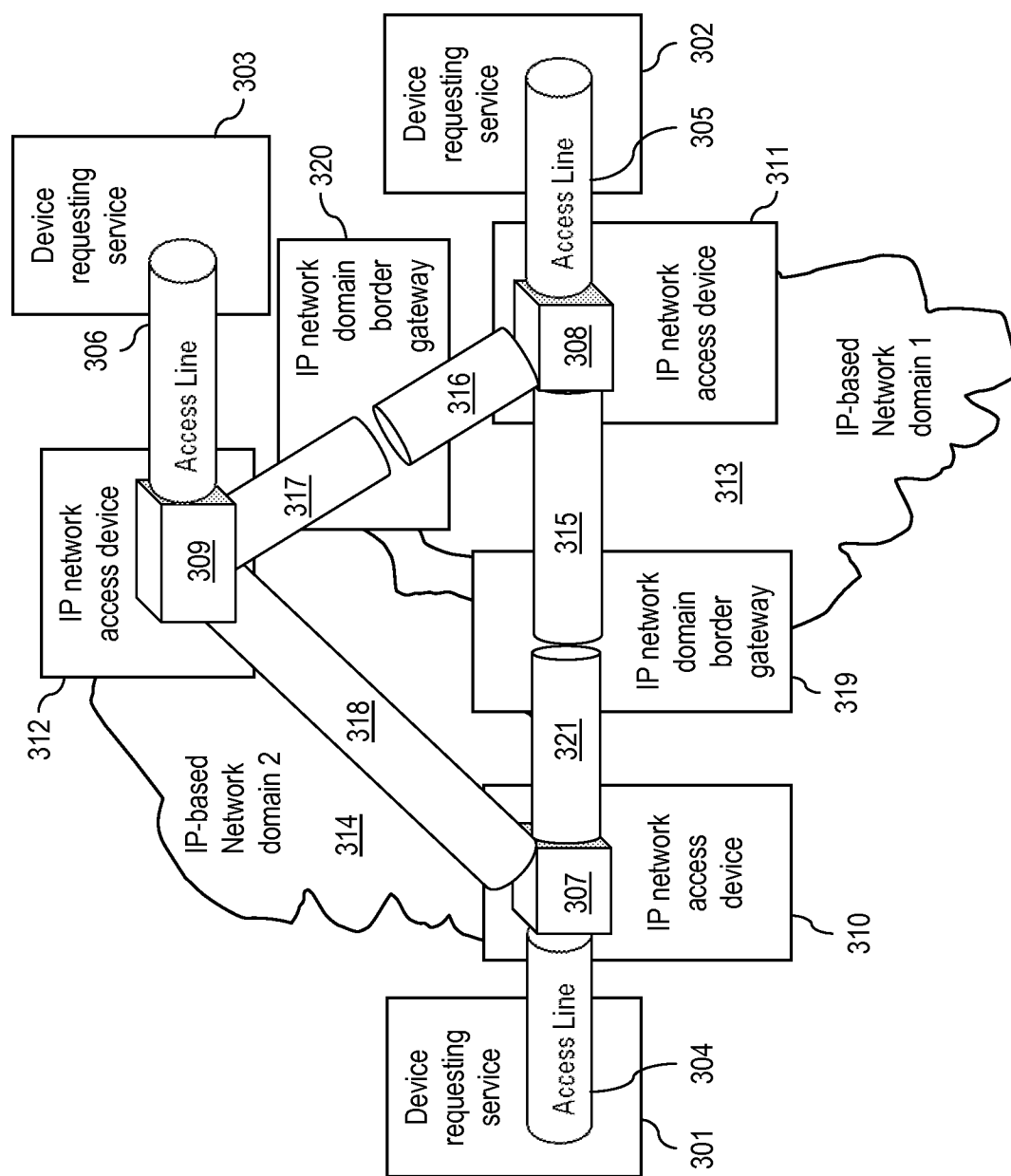


Fig.4

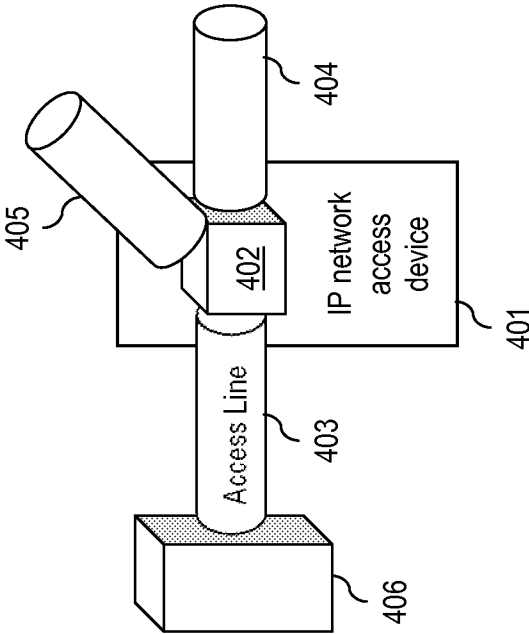
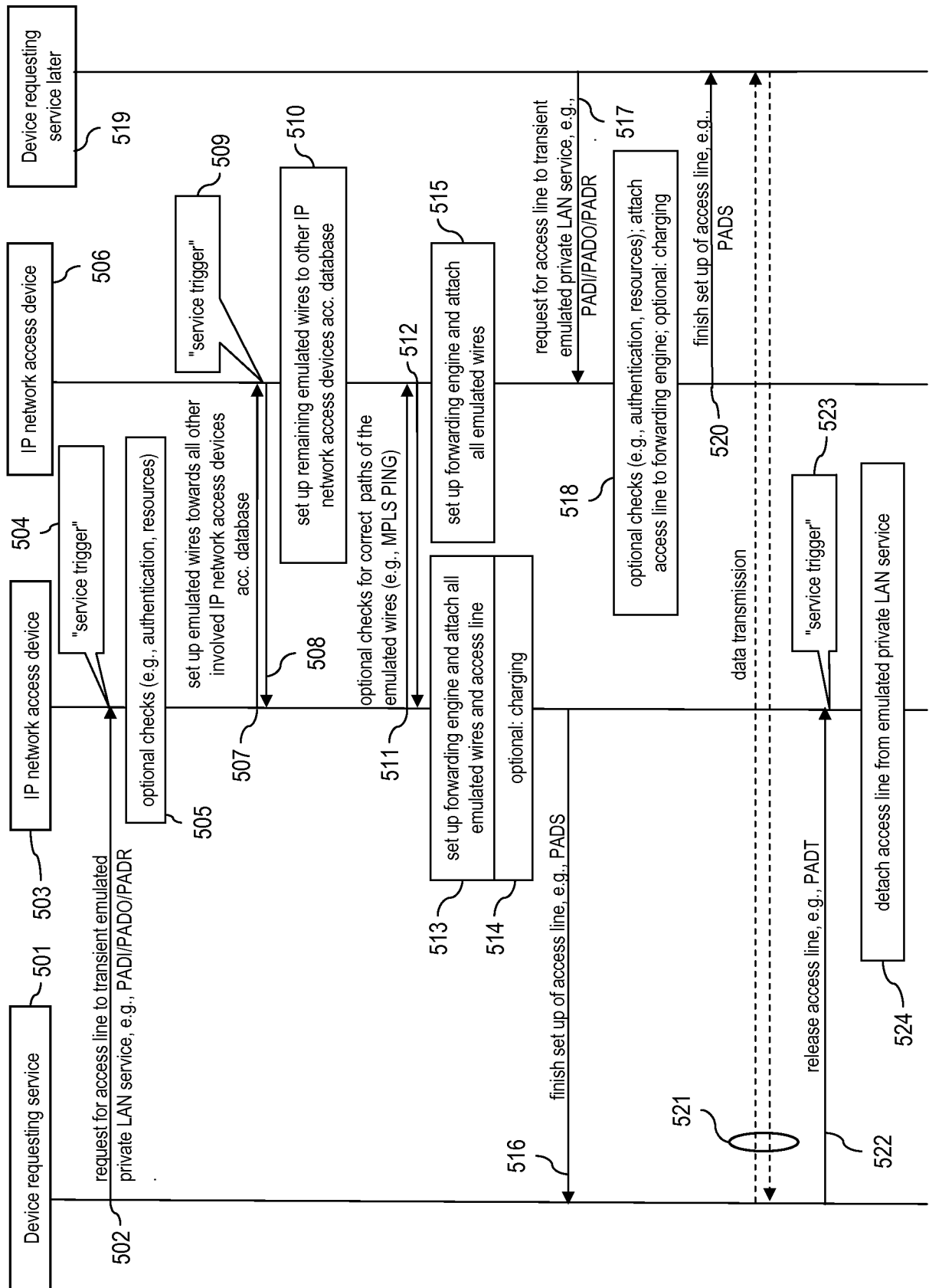


Fig.5



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/050303

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/06
ADD.

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)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/117954 A1 (DE NEVE HANS MARIA PAUL [BE] ET AL) 26 June 2003 (2003-06-26) paragraphs [0015] - [0049] paragraph [0004] paragraphs [0011], [0044] - [0049] paragraphs [0059] - [0062] paragraph [0077] paragraphs [0091] - [0092], [0095] -----	1-15
X	BRYANT S ET AL: "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture; rfc3985.txt" IETF STANDARD, INTERNET ENGINEERING TASK FORCE, IETF, CH, 1 March 2005 (2005-03-01) , XP015009756 ISSN: 0000-0003 * abstract paragraphs [04.1], [7.1] -----	1,2, 12-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* 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 document 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

1 July 2010

Date of mailing of the international search report

21/07/2010

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Pereira, Mafalda

Information on patent family members

PCT/EP2010/050303

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003117954 A1	26-06-2003	CN 1449162 A	15-10-2003
		EP 1331766 A1	30-07-2003