



(86) Date de dépôt PCT/PCT Filing Date: 2007/09/04
(87) Date publication PCT/PCT Publication Date: 2009/03/04
(45) Date de délivrance/Issue Date: 2013/09/03
(85) Entrée phase nationale/National Entry: 2008/09/05
(86) N° demande PCT/PCT Application No.: CA 2007/001556
(87) N° publication PCT/PCT Publication No.: 2009/030012

(51) Cl.Int./Int.Cl. *H04L 9/32* (2006.01),
H04L 12/28 (2006.01), *H04B 7/00* (2006.01),
H04B 3/00 (2006.01)
(72) Inventeurs/Inventors:
CAMILLE, JEAN-PAUL, CA;
TIN, NOEL TAI-TUNG, CA;
CHAN, FRANK SIU HONG, CA
(73) Propriétaire/Owner:
BCE INC., CA
(74) Agent: SMART & BIGGAR

(54) Titre : METHODE ET SYSTEME D'APPROVISIONNEMENT D'EQUIPEMENT AUX LOCAUX DE L'ABONNE
(54) Title: METHOD AND SYSTEM FOR PROVISIONING CUSTOMER PREMISES EQUIPMENT

(57) **Abrégé/Abstract:**

A method for execution by at least one entity in the service provider network is provided. The method includes receiving an access request from a communication device; determining a logical identifier intended for use by the communication device during an eventual communication session; and identifying, based on the logical identifier, an object linked to a physical location of the communication device. In one aspect, the method includes obtaining account credentials for a customer known to be associated with the object, whereas in another aspect, the method comprises establishing a data session between the communication device and a network entity associated with the object without necessarily obtaining any account credentials.



ABSTRACT

1
2
3 A method for execution by at least one entity in the service provider network is provided.
4 The method includes receiving an access request from a communication device;
5 determining a logical identifier intended for use by the communication device during an
6 eventual communication session; and identifying, based on the logical identifier, an object
7 linked to a physical location of the communication device. In one aspect, the method
8 includes obtaining account credentials for a customer known to be associated with the
9 object, whereas in another aspect, the method comprises establishing a data session
10 between the communication device and a network entity associated with the object without
11 necessarily obtaining any account credentials.

1 **METHOD AND SYSTEM FOR PROVISIONING**
2 **CUSTOMER PREMISES EQUIPMENT**

3
4
5 **FIELD OF THE INVENTION**

6
7 The present invention relates generally to providing access to a public data
8 network such as the Internet and, more particularly, to a method and system
9 for provisioning customer premises equipment to allow access to such a
10 network.

11
12
13 **BACKGROUND OF THE INVENTION**

14
15 Internet access is an example of a service that can be provided by a service
16 provider to its customers. In a typical scenario, the service provider creates
17 an account for a given customer, including account credentials to be used
18 when accessing the Internet. The service provider then ships a modem or
19 other communication device to the customer and provides the customer with
20 the account credentials; the service provider also records a hardware identifier
21 of the modem in association with the customer. Upon receipt and installation
22 of the modem by the customer, the modem is powered on, and the modem
23 contacts service provider equipment at a default location (which may be hard
24 coded in the modem). The service provider equipment recognizes the
25 hardware identifier of the modem as being associated with the service
26 provider. For security purposes, to confirm that the modem is indeed being
27 operated by the customer, the service provider then requires the customer to
28 enter the account credentials before allowing access to the Internet via a
29 gateway, edge router or other form of switch.

30
31 One problem that plagues service providers is that customers are frequently
32 inconvenienced by having to enter their account credentials when the modem
33 is initially powered on or after every factory reset. In addition, it also happens
34 that the service provider may send a replacement modem to the customer in

1 response to the customer noticing that the modem that they had previously
2 ordered did not yet arrive. In this case, when shipping the replacement
3 modem, the service provider records the hardware identifier of the
4 replacement modem in association with the customer. However, if the original
5 modem is ultimately received by the customer before the replacement
6 modem, and is installed, then when its hardware identifier is provided to the
7 service provider equipment at the default location, this hardware identifier will
8 not be recognized as being associated with the customer because the
9 hardware identifier currently associated with the customer is the hardware
10 identifier of the replacement modem. In short, the customer could be denied
11 access to the Internet because the original modem was used instead of the
12 replacement modem, which can lead to further frustration on the part of the
13 customer, in fact adding to the frustration that may have led to a request for
14 the replacement modem in the first place.

15

16 Thus, there exists a need in the industry to alleviate the above difficulties
17 when regulating a customer's access to a public data network and maintain an
18 accurate customer-to-modem association.

19

20

21 SUMMARY OF THE INVENTION

22

23 A first broad aspect of the present invention seeks to provide a method for
24 execution by at least one entity in a service provider network. The method
25 comprises receiving an access request from a communication device;
26 determining a logical identifier intended for use by the communication device
27 during an eventual communication session; identifying, based on the logical
28 identifier, an object linked to a physical location of the communication device;
29 and obtaining account credentials for a customer known to be associated with
30 said object.

31

32 A second broad aspect of the present invention seeks to provide a computer-
33 readable medium comprising computer-readable program code which, when
34 interpreted by at least one computing apparatus in a service provider network,

1 causes the at least one computing apparatus to execute a method. The
2 computer-readable program code comprises first computer-readable program
3 code for causing the computing apparatus to be attentive to receipt of an
4 access request from a communication device; second computer-readable
5 program code for causing the computing apparatus to determine a logical
6 identifier intended for use by the communication device during an eventual
7 communication session; third computer-readable program code for causing
8 the computing apparatus to identify, based on the logical identifier, an object
9 linked to a physical location of the communication device; and fourth
10 computer-readable program code for causing the computing apparatus to
11 obtain account credentials for a customer known to be associated with said
12 object.

13

14 A third broad aspect of the present invention seeks to provide at least one
15 network entity in a service provider network, comprising means for receiving
16 an access request from a communication device; means for determining a
17 logical identifier intended for use by the communication device during an
18 eventual communication session; means for identifying, based on the logical
19 identifier, an object linked to a physical location of the communication device;
20 and means for obtaining account credentials for a customer known to be
21 associated with said object.

22

23 A fourth broad aspect of the present invention seeks to provide a service
24 provider network, which comprises a first entity and a second entity. The first
25 entity is configured to receive an access request from a communication
26 device; and determine a logical identifier intended for use by the
27 communication device during an eventual communication session. The
28 second entity is configured to identify, based on the logical identifier, an object
29 linked to a physical location of the communication device; and obtain account
30 credentials for a customer known to be associated with said object.

31

32 A fifth broad aspect of the present invention seeks to provide a method for
33 execution by customer premises equipment. The method comprises
34 transmitting an access request to a network entity over a communication link;

1 obtaining account credentials over the communication link during a
2 configuration session established with a walled garden entity; transmitting the
3 account credentials to the network entity over the communication link; and
4 establishing a communication session with a gateway, the gateway having
5 been previously associated with the account credentials.

6
7 A sixth broad aspect of the present invention seeks to provide a computer-
8 readable medium comprising computer-readable program code which, when
9 interpreted by a computing apparatus, causes the computing apparatus to
10 execute a method. The computer-readable program code comprises first
11 computer-readable program code for causing the computing apparatus to
12 transmit an access request to a network entity over a communication link;
13 second computer-readable program code for causing the computing
14 apparatus to obtain account credentials over the communication link during a
15 configuration session established with a walled garden entity; third computer-
16 readable program code for causing the computing apparatus to transmit the
17 account credentials to the network entity over the communication link; and
18 fourth computer-readable program code for causing the computing apparatus
19 to establish a communication session with a gateway, the gateway having
20 been previously associated with the account credentials.

21
22 A seventh broad aspect of the present invention seeks to provide customer
23 premises equipment, comprising a memory and a processing unit. The
24 processing unit is configured to transmit an access request to a network entity
25 over a communication link; obtain account credentials over the communication
26 link during a configuration session established with a walled garden entity;
27 store the account credentials in the memory; transmit the account credentials
28 to the network entity over the communication link; and establish a
29 communication session with a gateway, the gateway having been previously
30 associated with the account credentials.

31
32 An eighth broad aspect of the present invention seeks to provide customer
33 premises equipment, comprising means for transmitting an access request to
34 a network entity over a communication link; means for obtaining account

1 credentials over the communication link during a configuration session
2 established with a walled garden entity; means for storing the account
3 credentials in the memory; means for transmitting the account credentials to
4 the network entity over the communication link; and means for establishing a
5 communication session with a gateway, the gateway having been previously
6 associated with the account credentials.

7
8 A ninth broad aspect of the present invention seeks to provide a method for
9 execution by at least one entity in a service provider network. The method
10 comprises receiving an access request from a communication device;
11 determining a logical identifier intended for use by the communication device
12 during an eventual communication session; identifying, based on said logical
13 identifier, an object linked to a physical location of the communication device;
14 and establishing a data session between the communication device and a
15 network entity associated with said object.

16
17 A tenth broad aspect of the present invention seeks to provide a computer-
18 readable medium comprising computer-readable program code which, when
19 interpreted by at least one computing apparatus in a service provider network,
20 causes the at least one computing apparatus to execute a method. The
21 computer-readable program code comprises first computer-readable program
22 code for causing the computing apparatus to be attentive to receipt of an
23 access request from a communication device; second computer-readable
24 program code for causing the computing apparatus to determine a logical
25 identifier intended for use by the communication device during an eventual
26 communication session; third computer-readable program code for causing
27 the computing apparatus to identify, based on said logical identifier, an object
28 linked to a physical location of the communication device; and fourth
29 computer-readable program code for causing the computing apparatus to
30 establish a data session between the communication device and a network
31 entity associated with said object.

32
33 An eleventh broad aspect of the present invention seeks to provide at least
34 one network entity in a service provider network, comprising means for being

1 attentive to receipt of an access request from a communication device; means for
2 determining a logical identifier intended for use by the communication device during an
3 eventual communication session; means for identifying, based on said logical identifier, an
4 object linked to a physical location of the communication device; and means for
5 establishing a data session between the communication device and a network entity
6 associated with said object.

7
8 A twelfth broad aspect of the present invention seeks to provide a service provider network
9 comprising a first entity and a second entity. The first entity is configured to receive an
10 access request from a communication device and determine a logical identifier intended for
11 use by the communication device during an eventual communication session. The second
12 entity is configured to identify, based on the logical identifier, an object linked to a physical
13 location of the communication device and establish a data session between the
14 communication device and a network entity associated with said object.

15
16 In accordance with another aspect, the invention relates to a method for execution by at
17 least one entity in a service provider network. The method comprises receiving an access
18 request from a communication device at an authorization entity. The method also
19 comprises, at an authorization entity:

- 20 - determining at an authorization entity an object linked to a physical location of the
21 communication device;
- 22 - selecting a logical identifier for use by the communication device during an eventual
23 communication session;
- 24 - storing in a location information database an association between the logical
25 identifier and the object; and
- 26 - providing the logical identifier to the communication device and to a configuration
27 entity.

28 The method also comprises, at the configuration entity;

- 29 - obtaining the logical identifier from the authorization entity;
- 30 - consulting the location information database, based on the logical identifier, to
31 determine the object; and

- obtaining account credentials for a customer known to be associated with the object at the configuration entity.

In accordance with another aspect, the invention relates to a service provider network. The service provider network comprises a first entity configured to receive an access request from a communication device. The first entity is also configured to determine an object linked to a physical location of the communication device. The first entity is further configured to select a logical identifier for use by the communication device during an eventual communication session. The first entity is also configured to store in a location information database an association between the logical identifier and the object. The first entity is also configured to provide the logical identifier to the communication device and to a second entity. The second entity is configured to obtain the logical identifier from the communication device during a configuration session. The second entity is also configured to consult the location information database, based on the logical identifier, to determine the object. The second entity is further configured to obtain account credentials for a customer known to be associated with the object.

In accordance with another aspect, the invention relates to a service provider network comprising:

-a first entity configured to:

- receive an access request from a communication device;
- determine a logical identifier intended for use by the communication device during an eventual communication session; and

- a second entity configured to:

- identify, based on the logical identifier, an object for allowing communication to be established with the communication device, the object linked to a physical location of the communication device; and
- obtain account credentials for a customer known to be associated with said object;

- a third entity configured to transmit the account credentials to the communication device;

- 1 - wherein the access request specifies first credentials and wherein the first entity is
- 2 further configured to obtain an identity of the second entity based on the first
- 3 credentials;
- 4 - wherein the first entity is further configured to cause establishment of a
- 5 configuration session between the second entity and the communication device;
- 6 - wherein the first entity is further configured to provide the logical identifier to the
- 7 second entity further to identification thereof based on the first credentials;
- 8 - wherein the third entity is further configured to transmit the account credentials over
- 9 the configuration session;
- 10 - wherein the first entity is further configured to receive the account credentials from
- 11 the communication device;
- 12 - wherein the first entity is further configured to obtain an identity of a fourth entity
- 13 based on the account credentials;
- 14 - wherein the account credentials are received in association with a second access
- 15 request by the communication device;
- 16 - wherein the first entity is further configured to cause establishment of a
- 17 communication session between the fourth entity and the communication device;
- 18 and
- 19 - wherein the first entity is further configured to select a new logical identifier for use
- 20 by the communication device.

21
22 These and other aspects and features of the present invention will now become apparent
23 to those of ordinary skill in the art upon review of the following description of specific
24 embodiments of the invention in conjunction with the accompanying drawings.

25 26 BRIEF DESCRIPTION OF THE DRAWINGS

27
28 Fig. 1 shows an architecture for delivery of communication services to a customer
29 associated with a customer premises, in accordance with a non-limiting embodiment of the
30 present invention.

31
32 Fig. 2 shows, within the architecture of Fig. 1, shipping of customer premises equipment to

- 1 the customer for installation at the customer premises.
- 2
- 3 Fig. 3 shows, within the architecture of Fig. 1, issuance of an access request by the
- 4 customer premises equipment.
- 5

1 Figs. 4A and 4B show identification of a logical identifier to be used by the
2 customer premises equipment and two alternative ways of engaging the
3 customer premises in a configuration session with an activation entity in a
4 service provider network.

5
6 Fig. 5 shows the configuration session established pursuant to either Fig. 4A
7 or Fig. 4B.

8
9 Fig. 6 shows, within the architecture of Fig. 1, issuance of a second access
10 request by the customer premises equipment.

11
12 Figs. 7A and 7B show identification of a logical identifier to be used by the
13 customer premises equipment and two alternative ways of engaging the
14 customer premises in the data session with a gateway to a public data
15 network.

16
17 Fig. 8 shows the data session established pursuant to either Fig. 7A or Fig.
18 7B.

19 20 21 DETAILED DESCRIPTION OF NON-LIMITING EMBODIMENTS

22
23 With reference to Fig. 1, there is shown an architecture for delivery of
24 communication services to be enjoyed by a customer ABC associated with a
25 customer premises 100. The customer premises 100 is located at a "service
26 point location" (such as a civic address, a set of geo-coordinates, etc.), which
27 is in this case the civic address "12 Main Street". Customer ABC is a
28 customer of a service provider, which operates a service provider network 140
29 and also provides access to a public data network 170 such as the Internet.
30 Furthermore, the service provider operates a network access server 130 that
31 allows a connection to be established between customer premises equipment
32 (not shown) at the customer premises 100 and either the service provider
33 network 140 or the public data network 170. In some cases, the public data

1 network 170 may be reachable via the service provider network 140 rather
2 than directly via the network access server 130.

3
4 The network access server 130 can be connected to the customer premises
5 100 in a variety of ways. In the specific non-limiting example illustrated in Fig.
6 1, the network access server 130 is connected to an access node 110, which
7 leads to the customer premises 100 (as well as to other customer premises -
8 not shown) via a physical link 105, such as a copper twisted pair, cable, fiber,
9 fixed wireless, free-space optical, etc. In a specific non-limiting embodiment,
10 the access node 110 can be implemented as a digital subscriber line access
11 multiplexer (DSLAM) with a plurality of ports, each port connected to a
12 different physical link. In the specific non-limiting example illustrated in Fig. 1,
13 one of the ports of the DSLAM 110, denoted P1, is connected to the physical
14 link 105 that leads to the customer premises 100. A database 120 stores a
15 mapping between ports of the DSLAM 110 and associated service point
16 locations, such as an association between port P1 and the civic address "12
17 Main Street". The database 120 may be populated and maintained by an
18 operation support system (OSS) 115, which represents a collection of systems
19 that perform management, inventory, engineering, planning, repair and other
20 functions for the service provider.

21
22 The DSLAM 110 is connected to the network access server 130 via a set of
23 logical links. More specifically, each of the ports of the DSLAM 110 that leads
24 to a given service point location is associated with a respective one of the
25 logical links. In the specific non-limiting example illustrated in Fig. 1, port P1 is
26 associated with a logical link 125. A database 135 stores a mapping between
27 the ports of the DSLAM 110 and associated logical links, such as a mapping
28 between port P1 and logical link 125. The database 135 may be populated by
29 the DSLAM 110 itself, or by the OSS 115. In specific non-limiting
30 embodiments, the logical links can be permanent virtual circuits (PVCs) or
31 virtual local area networks (VLANs), to name a few non-limiting possibilities.

32
33 In other embodiments of the present invention, the DSLAM 110 may not be
34 present. For example, consider the case where in the absence of a DSLAM

1 the aforesaid logical link 125 (such as a VLAN or PVC) extends all the way to
2 the customer premises 100. Even under this scenario, communication
3 established over the logical link 125 is still destined to reach the service point
4 location of the customer premises 100. Thus, it can be said that DSLAM port
5 P1 and/or logical link 125 represent an "object" linked to the physical location
6 of the customer premises 100 (i.e., a location-linked object), and which allows
7 communication to be established with the customer premises equipment 200
8 at that location. The location-linked object could be physical (as in the case of
9 a DSLAM port) or logical (as in the case of a VLAN or PVC). Still other
10 examples of a location-linked object will now become apparent to those of
11 ordinary skill in the art without departing from the scope of the present
12 invention.

13

14 In accordance with an embodiment of the present invention, the service
15 provider also operates a configuration entity 145, which is responsible for
16 assisting in configuration of customer premises equipment that may be used
17 by various customers, including customer ABC. Further details regarding
18 operation of the configuration entity 145 will be given later on. For the time
19 being, it should simply be appreciated that the configuration entity 145 is
20 accessible by the network access server 130 via the service provider network
21 140.

22

23 The service provider further operates an authorization entity 160, which is
24 responsible for processing "access requests" received along the logical links
25 (including logical link 125). An "access request" comprises a message or
26 collection of messages specifying a set of account credentials, which may or
27 may not be valid and, if valid, may be a set of "default" credentials or a set of
28 "customer account" credentials. In order to assist in performing its functions,
29 the authorization entity 160 has access to a database 165 that stores a
30 mapping between sets of account credentials and associated network entities.
31 The network entity associated with a given set of account credentials is the
32 entity responsible for managing a communication session initiated following
33 an access request that specifies the given set of account credentials.
34 Examples of network entities that may be responsible for managing a

1 communication session initiated following an access request that specifies a
2 particular set of account credentials include entities (such as a gateway 175)
3 that are connected to the public data network 170 and allow full or partial
4 access thereto, as well as entities (such as the configuration entity 145) that
5 perform specific functions within a corresponding sub-region of the service
6 provider network 140 (sometimes referred to as a “walled garden”).

7
8 In the specific non-limiting example illustrated in Fig. 1, the database 165
9 stores an association between a set of “default” credentials and the
10 configuration entity 145. This means that a communication session initiated
11 following an access request that specifies the set of default credentials is to be
12 managed by the configuration entity 145. It should be appreciated that the
13 contents of the database 165 may be updated in a dynamic fashion as new
14 sets of valid credentials are added, deleted or changed, and/or as changes
15 occur to the network entities with which certain ones of the sets of credentials
16 are associated.

17
18 The service provider also operates an activation entity 155, which is
19 responsible for directly or indirectly interacting with customers in order to allow
20 service activation, service deactivation and service changes for individual
21 customers, including customer ABC. To this end, the activation entity 155
22 may comprise or connect to a customer service computer system or online
23 portal. The activation entity 155 is also connected to the configuration entity
24 145, either directly (as illustrated) or via the service provider network 140.
25 Furthermore, the activation entity 155 has access to the database 165, either
26 directly (as illustrated) or via the service provider network 140.

27
28 In order to assist in performing its functions, the activation entity 155 has
29 access to a database 150 that stores various information for each customer,
30 namely a service point location, a DSLAM port and, ultimately, a set of
31 account credentials. In the specific non-limiting example illustrated in Fig. 1,
32 the database 150 stores the civic address “12 Main Street” for customer ABC.
33 Also, port P1 of the DSLAM 110 is included in the database 120 in association
34 with customer ABC. (It should be appreciated that in order to associate

1 customer ABC with port P1 of the DSLAM 110, one can simply consult the
2 database 120 based on customer ABC's civic address "12 Main Street".)

3

4 In the example of Fig. 1, it has been assumed that customer ABC has not yet
5 placed an order for a service that requires the use of customer premises
6 equipment. For this reason, no customer premises equipment is illustrated in
7 Fig. 1 and also there is no information in the database 150 regarding any
8 account credentials for customer ABC.

9

10 However, consider now the case where customer ABC places an order for a
11 service requiring customer premises equipment such as a modem or other
12 communication device. This can be done through an order processing
13 function of the activation entity 155. More specifically, customer ABC
14 (residing at the civic address "12 Main Street") contacts the service provider to
15 subscribe to a given service requiring customer premises equipment. With
16 reference now to Fig. 2, the outcome of customer ABC having contacted the
17 service provider may be for the activation entity 155 to assign a set of
18 customer account credentials to customer ABC and thus to associate this set
19 of customer account credentials to customer ABC in the database 150. In the
20 specific non-limiting example of Fig. 2, the set of customer account credentials
21 is denoted "XYZ".

22

23 Depending on the service ordered by customer ABC, the set of customer
24 account credentials can be associated with corresponding access
25 permissions. In the present example, the access permissions associated with
26 the set of customer account credentials "XYZ" allow full access to the public
27 data network 170, which is accessed via the gateway 175. Thus, the
28 activation entity 155 updates the database 165 accessed by the authorization
29 entity 160 so that the set of customer account credentials "XYZ" will be
30 associated with the configuration entity 145. This means that a
31 communication session initiated following an access request that specifies the
32 set of customer credentials "XYZ" is to be managed by the gateway 175.

33

1 At this stage, the order processing function of the activation entity 155 may
2 cause a modem or other customer premises equipment 200 to be shipped to
3 customer ABC's civic address (i.e., "12 Main Street"). The customer premises
4 equipment 200 may be pre-programmed with the default set of credentials
5 mentioned above and, if necessary, with information allowing the customer
6 premises equipment 200 to locate the network access server 130. Upon
7 receipt at the customer premises 100, the customer premises equipment 200
8 is installed and powered on. A computing device 215 may be connected to
9 the customer premises equipment 200 in order to allow customer ABC to
10 enjoy the various communication services provided by the service provider.

11

12 Although the customer premises equipment 200 is described as having been
13 shipped by the service provider to customer ABC's civic address (in this case,
14 "12 Main Street"), in other non-limiting embodiments, the customer premises
15 equipment 200 may be obtained from another source (or may already be at
16 the customer premises 100 when customer ABC places the order). In such
17 cases, it will be assumed for the present purposes that the customer premises
18 equipment 200 is capable of being programmed with the set of default
19 credentials mentioned above and, if necessary, with information allowing the
20 customer premises equipment 200 to locate the network access server 130.

21

22 Turning now to Fig. 3, the customer premises equipment 200 undergoes a
23 configuration process, which can occur at power-up, with or without triggering
24 by customer ABC. The configuration process includes the customer premises
25 equipment 200 issuing an access request 300 comprising the set of default
26 credentials mentioned above (and which may have been programmed by the
27 service provider prior to shipping). The access request 300 may be
28 formulated as one or more messages. The access request 300 reaches the
29 DSLAM 110 (more specifically, port P1) over the physical link 105, and then
30 reaches the network access server 130 over logical link 125. The network
31 access server 130 is operable to relay the set of default credentials comprised
32 in the access request 300 to the authorization entity 160 in the form of a
33 message 325.

34

1 The message 325 may be sent in accordance with a variety of protocols,
2 including but not limited to RADIUS (Remote Authentication Dial In User
3 Service). It should be understood that although the message 325 may have a
4 different format from the access request 300, it may nevertheless still be
5 considered an access request in the generic sense of the expression. The
6 authorization entity 160, which may be implemented in hardware, software,
7 control logic or a combination thereof, implements a process that may
8 comprise execution of background tasks, which can be interrupted under
9 various circumstances. For example, in order to service the message 325
10 from the network access server 130, the authorization entity 160 may execute
11 the following steps.

12

13 Specifically, the authorization entity 160 consults the database 165 based on
14 the set of credentials in the message 325 in order to identify the entity
15 responsible for managing a communication session initiated following the
16 access request 300 (which can be the gateway 175, the configuration entity
17 145 or another "walled garden" gateway). Communication between the
18 authorization entity 160 and the database 165 may take place using a variety
19 of protocols, including but not limited to LDAP (Lightweight Directory Access
20 Protocol). In the specific non-limiting example illustrated in Fig. 3, the set of
21 credentials in the message 325 corresponds to the set of default credentials
22 and therefore, according to the database 165, the entity responsible for
23 managing a communication session initiated following the access request 300
24 is the configuration entity 145.

25

26 The authorization entity 160 then selects a logical identifier to be used by
27 equipment for communication over logical link 125 (over which the access
28 request 300 was received) during an eventual communication session.
29 Alternatively, the authorization entity 160 may involve another entity in the
30 selection of this logical identifier. The selected logical identifier may be an
31 Internet Protocol (IP) address, for example, such as an Ipv4 or Ipv6 address.
32 Alternatively, the selected logical identifier may be a VLAN tag. In the specific
33 non-limiting example illustrated in Fig. 3, the selected logical identifier is
34 192.100.100.100. A database 305 is provided that stores a mapping that

1 relates logical links to logical identifiers selected to be used by equipment for
2 communication over those logical links (such as, in this example, the
3 relationship between logical link 125 and logical identifier 192.100.100.100).
4 The database 305 may be accessible to the authorization entity 160 and/or to
5 the network access server 130. It should be appreciated that selection of the
6 logical identifier for use by equipment for communication over logical link 125
7 can be effected in a variety of ways, including selection from a pool 315 of
8 available logical identifiers. Other implementations are of course possible.

9
10 One will appreciate that once a given logical identifier is associated with a
11 given logical link, it becomes possible to go one step further and associate
12 that logical identifier with a DSLAM port, which is uniquely associated with a
13 known service point location. Specifically, when the information stored in the
14 database 305 is combined with the information stored in the database 135,
15 one obtains an association between logical identifiers and ports of the DSLAM
16 110. This association or mapping can be stored in a location information
17 database (LID) 310. In the specific non-limiting example of Fig. 3, the location
18 information database 310 stores an association between IP address
19 192.100.100.100 and DSLAM port P1. The location information database 310
20 is accessible to the configuration entity 145 for future use as will be described
21 herein below. It should be appreciated that the location information database
22 310 may be created and maintained in a dynamic and transparent fashion,
23 such that it always contains the most up-to-date information regarding the
24 association between logical identifiers and DSLAM ports for specific service
25 point locations.

26
27 Turning now to Figs. 4A and 4B, a "configuration session" is established
28 between the customer premises equipment 200 and the entity whose identity
29 was learned by having consulted the database 165 (in this case, the
30 configuration entity 145). To this end, the authorization entity 160 sends a first
31 message 400 to the customer premises equipment 200 to inform the customer
32 premises equipment 200 of the logical identifier selected for use by equipment
33 for communication over logical link 125 (in this case, 192.100.100.100).

1 In addition, as shown in Fig. 4A, the authorization entity 160 sends a second
2 message 405 to the configuration entity 145 to inform the configuration entity
3 145 of the logical identifier being used by the customer premises equipment
4 200 (in this case, 192.100.100.100), and thereby to engage it in
5 communication with the customer premises equipment 200.

6
7 Alternatively, as shown in Fig. 4B, the customer premises equipment 200
8 sends a second message 410 to the configuration entity 145 to engage it in
9 communication with the customer premises equipment 200.

10
11 In either case, and as shown in Fig. 5, a configuration session 500 is thus
12 established between the customer premises equipment 200 and the
13 configuration entity 145.

14
15 The configuration entity 145 then consults the location information database
16 310 based on the logical identifier being used by the customer premises
17 equipment 200, in order to obtain from the location information database 310
18 the identity of the associated DSLAM port. In the specific non-limiting
19 example of Fig. 5, the configuration entity 145 consults the location
20 information database 310 based on the logical identifier 192.100.100.100 in
21 order to obtain from the location information database 310 the identity of port
22 P1 of the DSLAM 110. In an alternative embodiment, the configuration entity
23 145 can perform a two-step process to obtain the same information, namely
24 by accessing the database 305 based on the logical identifier
25 192.100.100.100 in order to obtain the identity of logical link 125, and then by
26 accessing the database 135 based on the identity of logical link 125 in order to
27 obtain the identity of port P1 of the DSLAM 110.

28
29 Next, the configuration entity 145 sends a message to the activation entity 155
30 that specifies the identity of port P1. Upon receipt of this message, the
31 activation entity 155 consults the database 150 in order to identify the
32 customer associated with port P1 of the DSLAM 110. In the specific non-
33 limiting example of Fig. 1, the activation entity 155 determines that customer
34 ABC is associated with port P1 of the DSLAM 110. Moreover, the activation

1 entity 155 obtains from the database 150 the set of customer account
2 credentials "XYZ" associated with customer ABC. The activation entity 155
3 formulates a response message specifying the set of customer account
4 credentials "XYZ". Upon receipt of this response message, the configuration
5 entity 145 sends its contents (i.e., the set of customer account credentials
6 "XYZ") to the customer premises equipment 200 as part of the configuration
7 session 500. The configuration process now terminates.

8
9 Upon receipt of the set of customer account credentials "XYZ", the customer
10 premises equipment 200 stores it in memory and uses it to make a second
11 access request while the customer premises equipment 200 is still powered
12 on. The result is now described with reference to Fig. 6.

13
14 Specifically, the customer premises equipment 200 issues a second access
15 request 600 comprising the set of customer account credentials "XYZ" stored
16 at the customer premises equipment 200 and received during the
17 configuration session 500. In accordance with various non-limiting
18 embodiments, issuance of the second access request 600 can be triggered by
19 the customer ABC (by virtue of accessing Internet using the computing device
20 215) or by the customer premises equipment 200.

21
22 The second access request 600 reaches the DSLAM 110 (more specifically,
23 port P1) over the physical link 105, and then reaches the network access
24 server 130 over logical link 125. The network access server 130 is operable
25 to relay the set of customer account credentials "XYZ" comprised in the
26 second access request 600 to the authorization entity 160 in the form of a
27 message 605.

28
29 As with the message 325, the message 605 may be sent in accordance with a
30 variety of protocols, including but not limited to RADIUS. Also, it should be
31 understood that although the message 605 may have a different format from
32 the second access request 600, it may nevertheless still be considered an
33 access request in the generic sense of the expression. Upon receipt of the
34 query message 605, the authorization entity 160 consults the database 165

1 based on the set of credentials in the message 605 in order to identify the
2 entity responsible for managing a communication session initiated following
3 the second access request 600 (which, it is recalled, can be the gateway 175,
4 the configuration entity 145 or another "walled garden" gateway). In the
5 specific non-limiting example illustrated in Fig. 6, the set of credentials in the
6 message 605 corresponds to the customer account credentials "XYZ" and
7 therefore, according to the database 165, the entity responsible for managing
8 a communication session initiated following the second access request 600 is
9 the gateway 175 to the public data network 170.

10
11 Optionally, the authorization entity 160 may then assign (or may involve
12 another entity in the assignment of) a new logical identifier to logical link 125
13 over which the second access request 600 was received. The new logical
14 identifier is stored in the database 305 in association with logical link 125.
15 Alternatively, the same logical identifier as before (in this case,
16 192.100.100.100) may be used, in which case the previous step is not
17 necessary. One will appreciate that if a new logical identifier is indeed
18 selected to be used by equipment for communication over logical link 125
19 (which is itself associated with DSLAM port P1), then the association between
20 such new logical identifier and port P1 can be automatically updated in the
21 location information database 310.

22
23 Turning now to Figs. 7A and 7B, a "data session" is established between the
24 customer premises equipment 200 and the entity whose identity was learned
25 by having consulted the database 165 (in this case, the gateway 175). To this
26 end, the authorization entity 160 can send a first message 700 to the customer
27 premises equipment 200 to inform the customer premises equipment 200 of
28 the logical identifier selected to be used by equipment for communication over
29 logical link 125. Where the selected logical address has not changed, the
30 previous step may not be required.

31
32 In addition, as shown in Fig. 7A, the authorization entity 160 sends a second
33 message 705 to the gateway 175 to inform the gateway 175 of the logical
34 identifier being used by the customer premises equipment 200 (in this case,

1 192.100.100.100), and thereby to engage it in communication with the
2 customer premises equipment 200.

3
4 Alternatively, as shown in Fig. 7B, the customer premises equipment 200
5 sends a second message 710 to the gateway 175 to engage it in
6 communication with the customer premises equipment 200.

7
8 In either case, and as shown in Fig. 8, a data session 800 is thus established
9 between the customer premises equipment 200 and the gateway 175.

10
11 It will therefore be appreciated that customer ABC is not asked to enter the set
12 of customer account credentials "XYZ", as these are obtained by the customer
13 premises equipment 200 automatically as part of the configuration session
14 500, and stored at the customer premises equipment 200 for later use.
15 However, even though this process has been automated, this does not make it
16 less secure. Consider a malicious user who would intercept the customer
17 premises equipment 200. Such a user would still not be able to gain access to
18 the public data network 170 because the set of customer account credentials
19 "XYZ" required to access the public data network 170 are derived from the
20 service provider's own pre-determined knowledge of which service point
21 location is connected to which DSLAM port.

22
23 In fact, any modem connected to the physical link 105 leading to port P1 of the
24 DSLAM 110 could be made to function seamlessly from 12 Main Street,
25 provided it were initially programmed with the aforementioned set of default
26 credentials. Recognition of this feature now allows customer ABC to employ
27 third party customer premises equipment (e.g., a modem could be purchased
28 from a source other than the service provider). In accordance with
29 embodiments of the invention, such a modem would obtain the user account
30 credentials for customer ABC merely by being connected to the service point
31 location known by the service provider to be associated with customer ABC.

32
33 Moreover, since the configuration process is repeated when a new modem is
34 powered up, there is no longer a danger that service would be refused due to

1 an out-of-date association between the hardware identifier of a device and a
2 given customer. This is because knowledge of the hardware identifier is not
3 required in the embodiments described above. Naturally, it should be
4 understood that associations based on hardware identifiers can still be useful
5 as a supplement to the teachings herein, particularly for purposes other than
6 the configuration process described above.

7
8 It should further be appreciated that although the first access request 300 was
9 described as containing the set of default credentials, this is not a requirement
10 of the present invention. Rather, in some embodiments, any type of access
11 request, whether it contain a set of default credentials, a set of invalid
12 credentials or no credentials at all, can be mapped in database 165 to an
13 associated network entity, specifically the authentication entity 145. The
14 result would be the same, namely that the configuration session 500 would be
15 established between the customer premises equipment 200 and the
16 authentication entity 145, and the set of customer account credentials "XYZ"
17 would be transmitted to the customer premises equipment 200 over the
18 configuration session 500 for transmission by the customer premises
19 equipment 200 as part of the second access request 600.

20
21 In fact, it should further be appreciated that in some embodiments, the two-
22 step process described above, involving (1) the first access request 300
23 (which, it has been established above, may or may not contain the set of
24 default credentials) that causes establishment of the configuration session
25 500 over which are exchanged the set of customer account credentials "XYZ"
26 and (2) the second access request 600 that sends back the set of customer
27 account credentials "XYZ" for establishment of the data session 800, can be
28 reduced to a one-step process with the same end effect of allowing the
29 customer premises equipment 200 to access a desired resource such as the
30 public data network 170. Specifically, the configuration session 500, and the
31 delivery of the customer account credentials "XYZ" over the configuration
32 session 500, can be dispensed with. This leads to the scenario where the
33 knowledge of the DSLAM port associated with customer ABC residing at 12
34 Main Street serves implicitly as the customer account credentials for customer

1 ABC. Specifically, when an access request is received via a port of the
2 DSLAM 110 (containing any kind of credentials, valid or invalid, or no
3 credentials at all), knowledge of the DSLAM port over which the access
4 request was received allows identification of the customer (by consulting
5 database 120), which would allow determination of the account credentials (by
6 consulting database 150), which then allows determination of the network
7 entity with which the customer premises equipment 200 should communicate
8 (by consulting database 165). Thus, the customer premises equipment which
9 issued the access request is automatically directed to the appropriate network
10 entity with which a data session, rather than a configuration session, is
11 established. It is to be noted that the authentication entity 160 or an entity on
12 behalf thereof can still be involved, as previously described, in the selection of
13 a logical identifier (e.g., IP address) to be used by the equipment for
14 communication over the logical link 125 (over which the access request was
15 received).

16

17 Those skilled in the art will appreciate that in some embodiments, groups of
18 two or more of the various network entities (e.g., the configuration entity 145,
19 the authorization entity 160, the activation entity 155, etc.) may be collocated
20 in a single physical component or piece of equipment. By the same token, the
21 functionality of individual ones of the various network entities (e.g., the
22 configuration entity 145, the authorization entity 160, the activation entity 155,
23 etc.) may be distributed over two or more physical components or pieces of
24 equipment.

25

26 Those skilled in the art will also appreciate that in some embodiments, some
27 or all of the functionality of the various network entities (e.g., the configuration
28 entity 145, the authorization entity 160, the activation entity 155, etc.) may be
29 implemented using pre-programmed hardware or firmware elements (e.g.,
30 application specific integrated circuits (ASICs), electrically erasable
31 programmable read-only memories (EEPROMs), etc.), or other related
32 components. In other embodiments, some or all of the functionality of the
33 various network entities may be achieved using a computing apparatus that
34 has access to a code memory (not shown) which stores computer-readable

1 program code for operation of the computing apparatus, in which case the computer-
2 readable program code could be stored on a medium which is fixed, tangible and readable
3 directly by the various network entities, (e.g., removable diskette, CD-ROM, ROM, fixed
4 disk, USB drive), or the computer-readable program code could be stored remotely but
5 transmittable to the various network entities via a modem or other interface device (e.g., a
6 communications adapter) connected to a network (including, without limitation, the
7 Internet) over a transmission medium, which may be either a non-wireless medium (e.g.,
8 optical or analog communications lines) or a wireless medium (e.g., microwave, infrared or
9 other transmission schemes) or a combination thereof.

10
11 While specific embodiments of the present invention have been described and illustrated, it
12 will be apparent to those skilled in the art that numerous modifications and variations can
13 be made.

86503-295

WHAT IS CLAIMED IS:

1. A method for execution by at least one entity in a service provider network, the method comprising:
 - at an authorization entity:
 - receiving an access request from a communication device;
 - determining an object linked to a physical location of the communication device;
 - selecting a logical identifier for use by the communication device during an eventual communication session;
 - storing in a location information database an association between the logical identifier and said object; and
 - providing the logical identifier to the communication device and to a configuration entity;
 - at the configuration entity:
 - obtaining the logical identifier from the authorization entity;
 - consulting the location information database, based on the logical identifier, to determine said object; and
 - obtaining account credentials for a customer known to be associated with said object.
2. The method defined in claim 1, wherein the communication device communicates via an access node and wherein said object is a port of the access node to which the communication device is connected by a physical link.
3. The method defined in claim 2, wherein the physical link includes at least one of: a copper twisted pair link, a cable link, a fiber link, a fixed wireless link and a free-space optical link.
4. The method defined in claim 3, wherein said identifying comprises consulting a first database and wherein said obtaining account credentials comprises consulting a second database.
5. The method defined in claim 4, wherein the access node is a DSLAM.

86503-295

- 1 6. The method defined in claim 1, wherein the communication device communicates via a
2 logical link and wherein said object is said logical link.
- 3 7. The method defined in claim 6, wherein said identifying comprises (I) accessing a first
4 database that stores a mapping between logical identifiers and associated logical links;
5 and (II) accessing a second database that stores a mapping between logical links and
6 associated objects.
- 7 8. The method defined in claim 7, wherein the logical link comprises at least one of a PVC
8 and a VLAN.
- 9 9. The method defined in claim 1, wherein said selecting is effected from a pool of
10 available logical identifiers.
- 11 10. The method defined in claim 1, wherein the logical identifier comprises at least one of
12 an IP address and a VLAN tag.
- 13 11. The method defined in claim 1, further comprising transmitting the account credentials
14 to the communication device.
- 15 12. The method defined in claim 1, wherein the account credentials are transmitted to the
16 communication device over the configuration session.
- 17 13. The method defined in claim 1, wherein the configuration session is established in
18 response to receiving the access request.
- 19 14. The method defined in claim 13, wherein the access request specifies first credentials.
- 20 15. The method defined in claim 14, wherein the account credentials are unique to the
21 customer.
- 22 16. The method defined in claim 15, wherein the first credentials are default credentials
23 associated with the service provider network.
- 24 17. The method defined in claim 16, wherein the default credentials are common to a
25 plurality of devices including the communication device.

86503-295

- 1 18. The method defined in claim **17**, wherein the default credentials are pre-programmed
2 into the communication device prior to shipping.
- 3 19. The method defined in claim **12**, further comprising effecting authorization of the access
4 request and, if successful, redirecting the access request to a walled garden for
5 establishment of the configuration session.
- 6 20. The method defined in claim **1**, the access request being a first access request, the
7 method further comprising receiving a second access request from the communication
8 device, the second access request comprising the account credentials previously
9 transmitted to the communication device by the configuration entity.
- 10 21. The method defined in claim **20**, further comprising effecting authorization of the
11 second access request and, if successful, redirecting the second access request to a
12 gateway to a public data network.
- 13 22. The method defined in claim **21**, further comprising causing establishment of a data
14 session with the communication device.
- 15 23. The method defined in claim **22**, wherein the communication device uses the logical
16 identifier during the data session.
- 17 24. A service provider network comprising:
- 18 - a first entity configured to:
 - 19 - receive an access request from a communication device;
 - 20 - determine an object linked to a physical location of the communication device;
 - 21 - select a logical identifier for use by the communication device during an eventual
22 communication session;
 - 23 - store in a location information database an association between the logical
24 identifier and said object; and
 - 25 - provide the logical identifier to the communication device and to a second entity;
 - 26 - the second entity configured to:
 - 27 - obtain the logical identifier from the communication device during a configuration
28 session;

86503-295

- 1 - consult the location information database, based on the logical identifier, to
- 2 determine said object; and
- 3 - obtain account credentials for a customer known to be associated with said
- 4 object.

5 25. The network defined in claim **24**, wherein to determine the logical identifier, the first
6 entity is configured to select the logical identifier from a pool of available logical
7 identifiers.

8 26. The network defined in claim **24**, wherein the access request specifies first credentials
9 and wherein the first entity is further configured to obtain an identity of the second entity
10 based on the first credentials.

11 27. The network defined in claim **26**, wherein the first entity is further configured to cause
12 establishment of the configuration session between the second entity and the
13 communication device.

14 28. The network defined in claim **27**, wherein the first entity is further configured to provide
15 the logical identifier to the second entity further to identification thereof based on the
16 first credentials.

17 29. The network defined in claim **28**, further comprising:

- 18 - a third entity configured to transmit the account credentials to the communication
- 19 device.

20 30. The network defined in claim **29**, wherein the third entity is further configured to
21 transmit the account credentials over the configuration session.

22 31. The network defined in claim **30**, wherein the second and third entities are the same.

23 32. The network defined in claim **30**, wherein the first entity is further configured to receive
24 the account credentials from the communication device.

25 33. The network defined in claim **32**, wherein the first entity is further configured to obtain
26 an identity of a fourth entity based on the account credentials.

86503-295

- 1 34. The network defined in claim **33**, wherein the account credentials are received in
2 association with a second access request by the communication device.
- 3 35. The network defined in claim **34**, wherein the first entity is further configured to cause
4 establishment of a communication session between the fourth entity and the
5 communication device.
- 6 36. The network defined in claim **35**, wherein the fourth entity is a gateway to a public data
7 network.
- 8 37. The network defined in claim **35**, wherein the first entity is further configured to select a
9 new logical identifier for use by the communication device.
- 10 38. The network defined in claim **24**, further comprising an access network having a port to
11 which the communication device is connected by a physical link, wherein said object is
12 said port of the access network.
- 13 39. The network defined in claim **38**, wherein the physical link includes at least one of: a
14 copper twisted pair link, a cable link, a fiber link, a fixed wireless link and a free-space
15 optical link.
- 16 40. The network defined in claim **39**, wherein to identify the object, the second entity is
17 configured to consult a first database and wherein to obtain the account credentials, the
18 second entity is configured to consult a second database.
- 19 41. The network defined in claim **40**, wherein the access node is a DSLAM.
- 20 42. The network defined in claim **24**, further comprising a logical link over which the
21 communication device communicates, wherein said object is said logical link.
- 22 43. The network defined in claim **42**, wherein to identify the object, the first entity is
23 configured to (I) access a first database that stores a mapping between logical
24 identifiers and associated logical links; and (II) access a second database that stores a
25 mapping between logical links and associated objects.

86503-295

1 44. The network defined in claim 43, wherein the logical link comprises at least one of a
2 PVC and a VLAN.

3 45. A service provider network comprising:

- 4 - a first entity configured to:
 - 5 - receive an access request from a communication device;
 - 6 - determine a logical identifier intended for use by the communication device
 - 7 during an eventual communication session; and
- 8 - a second entity configured to:
 - 9 - identify, based on the logical identifier, an object for allowing communication to
 - 10 be established with the communication device, the object linked to a physical
 - 11 location of the communication device; and
- 12 - obtain account credentials for a customer known to be associated with said
- 13 object;
- 14 - a third entity configured to transmit the account credentials to the communication
- 15 device;
- 16 - wherein the access request specifies first credentials and wherein the first entity is
- 17 further configured to obtain an identity of the second entity based on the first
- 18 credentials;
- 19 - wherein the first entity is further configured to cause establishment of a
- 20 configuration session between the second entity and the communication device;
- 21 - wherein the first entity is further configured to provide the logical identifier to the
- 22 second entity further to identification thereof based on the first credentials;
- 23 - wherein the third entity is further configured to transmit the account credentials over
- 24 the configuration session;
- 25 - wherein the first entity is further configured to receive the account credentials from
- 26 the communication device;
- 27 - wherein the first entity is further configured to obtain an identity of a fourth entity
- 28 based on the account credentials;
- 29 - wherein the account credentials are received in association with a second access
- 30 request by the communication device;

86503-295

- 1 - wherein the first entity is further configured to cause establishment of a
- 2 communication session between the fourth entity and the communication device;
- 3 and
- 4 - wherein the first entity is further configured to select a new logical identifier for use
- 5 by the communication device.

6

1/10

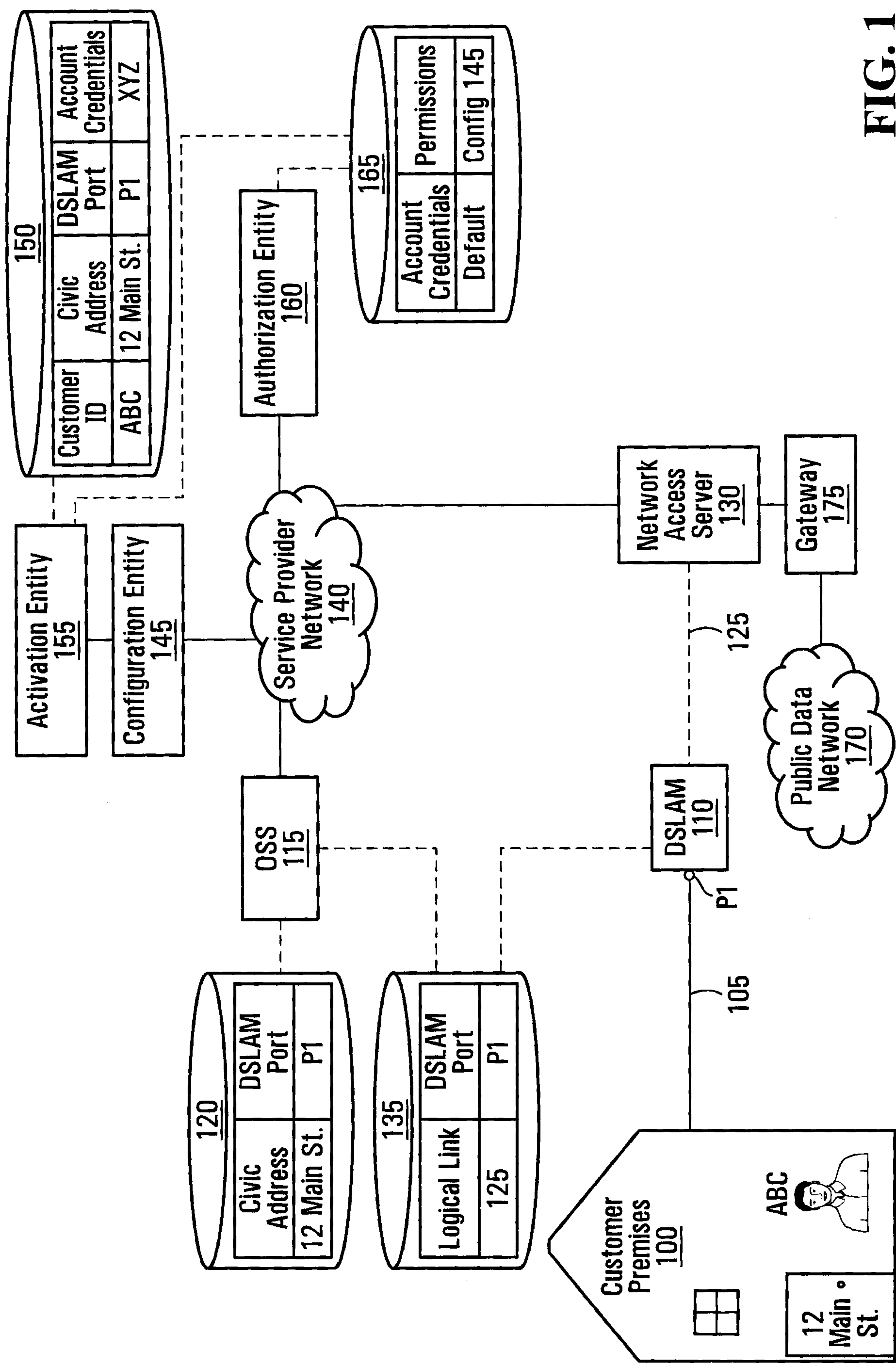


FIG. 1

2/10

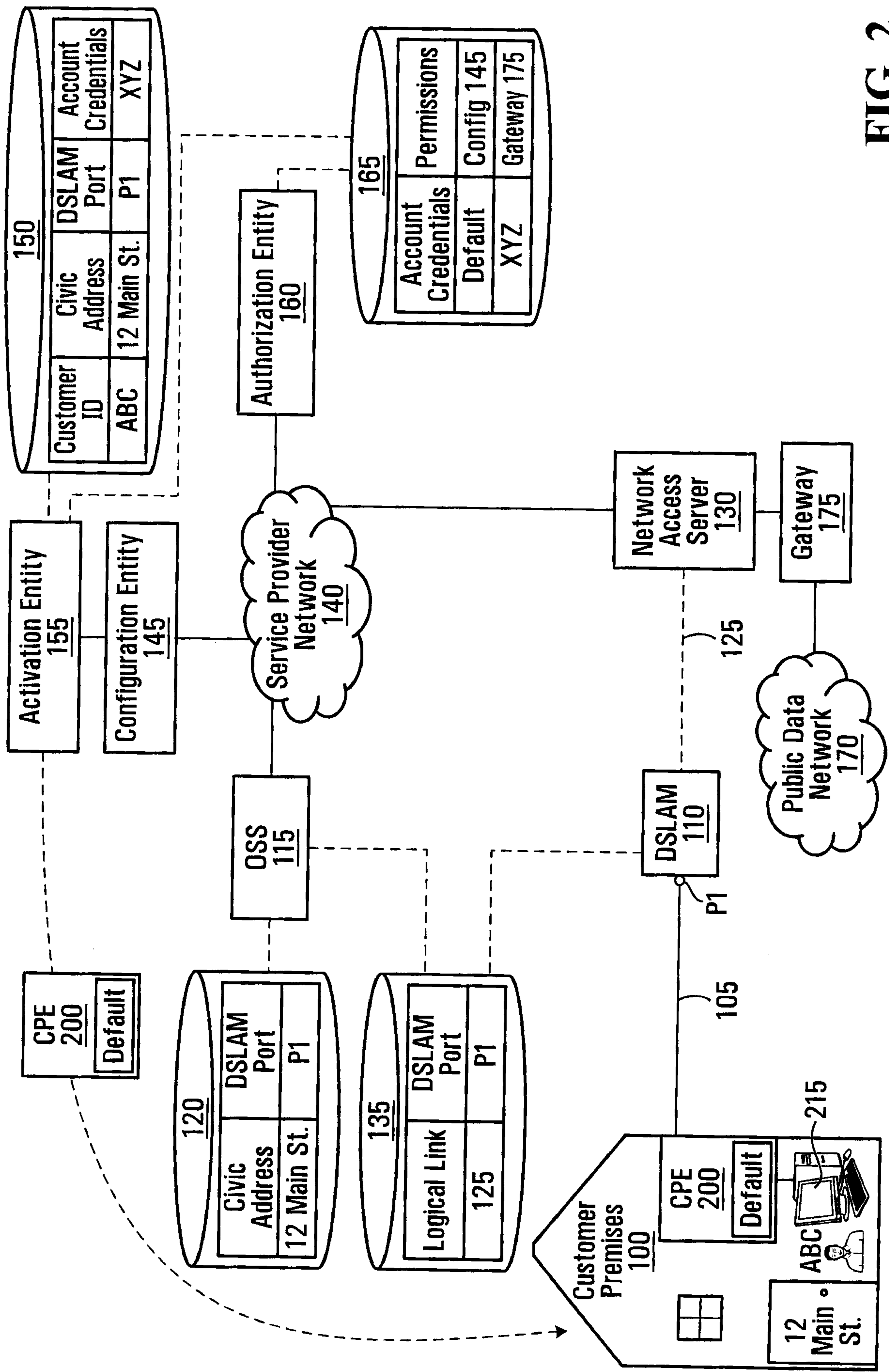


FIG. 2

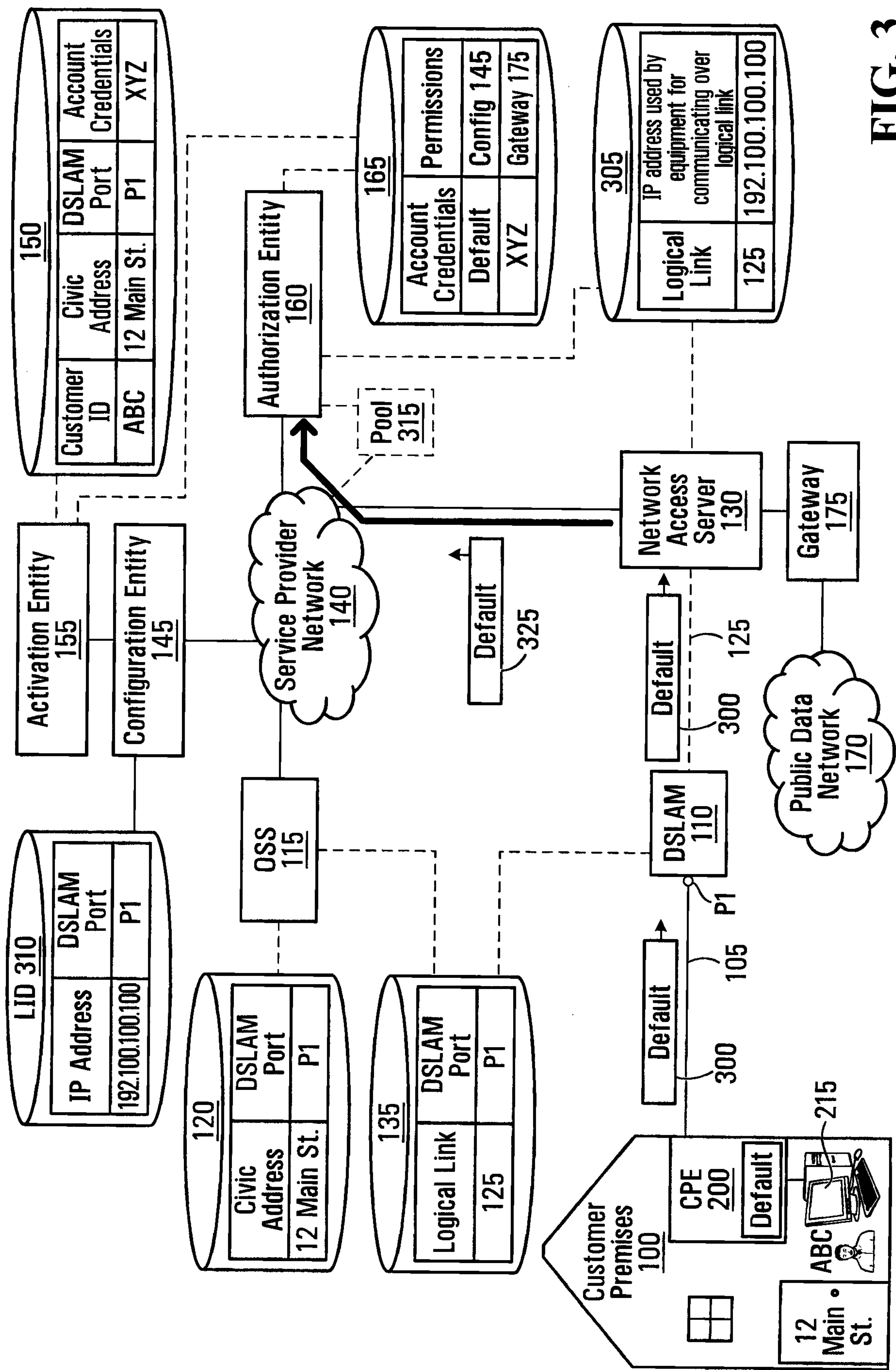


FIG. 3

4/10

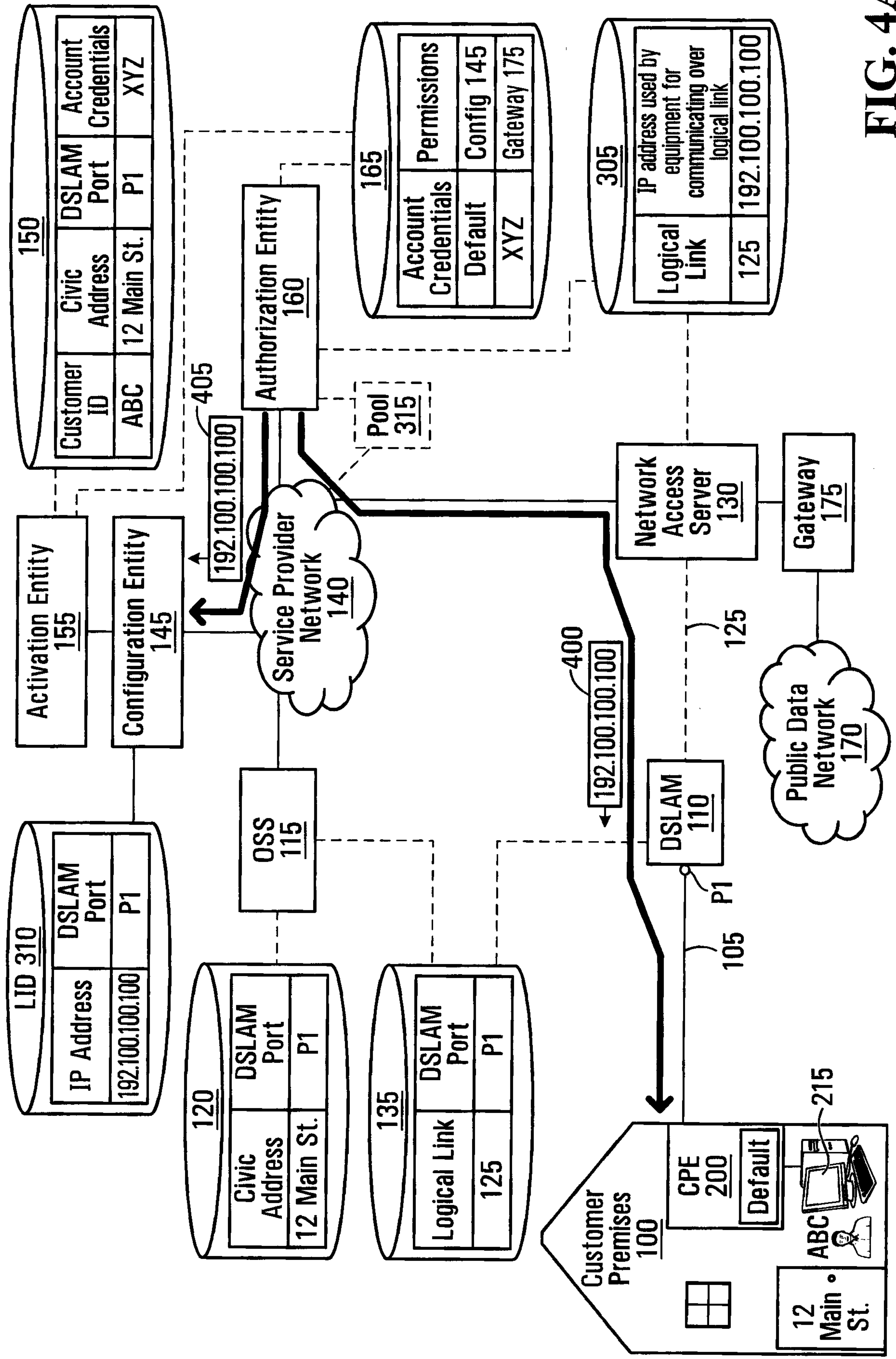


FIG. 4A

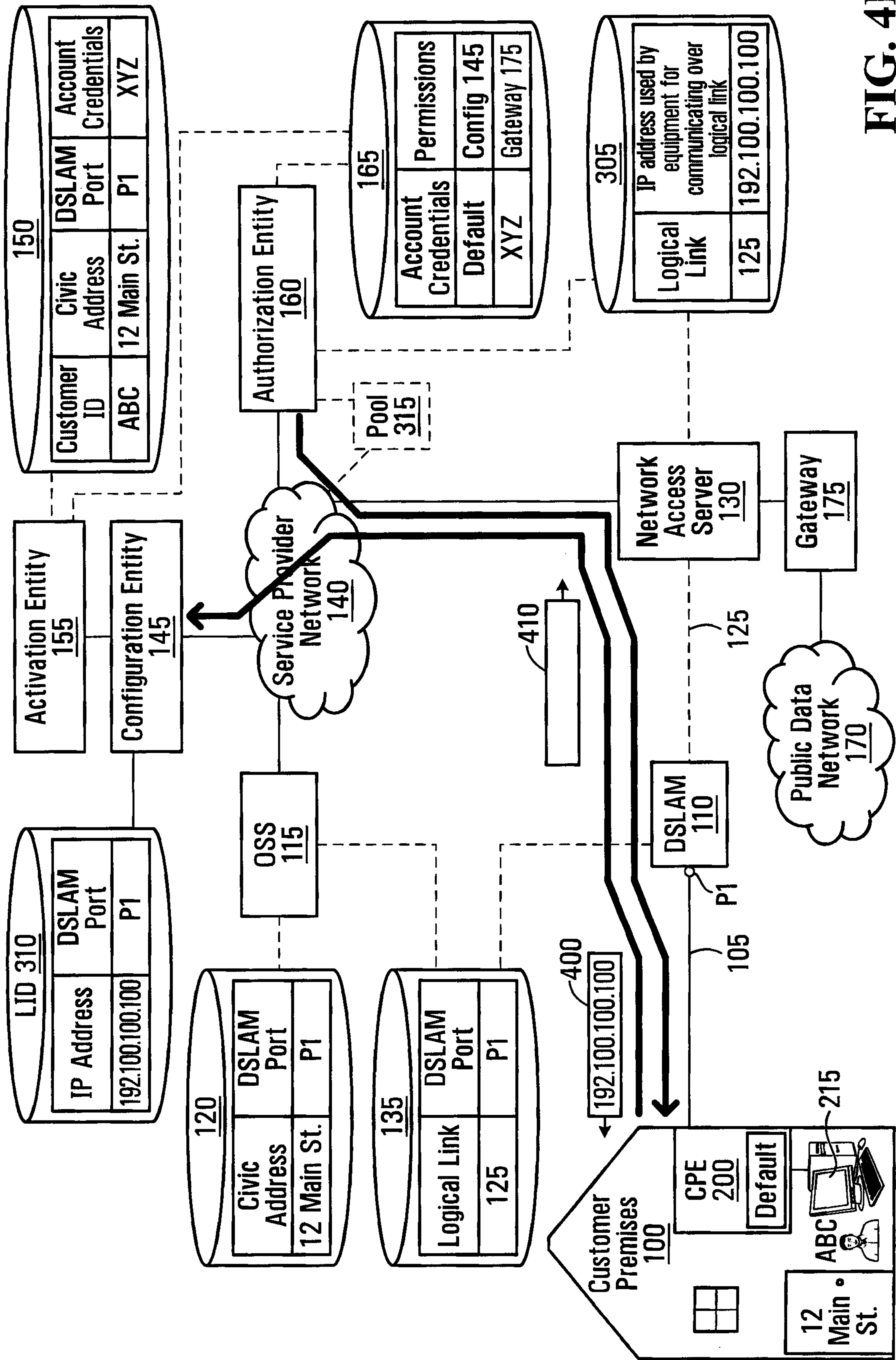


FIG. 4B

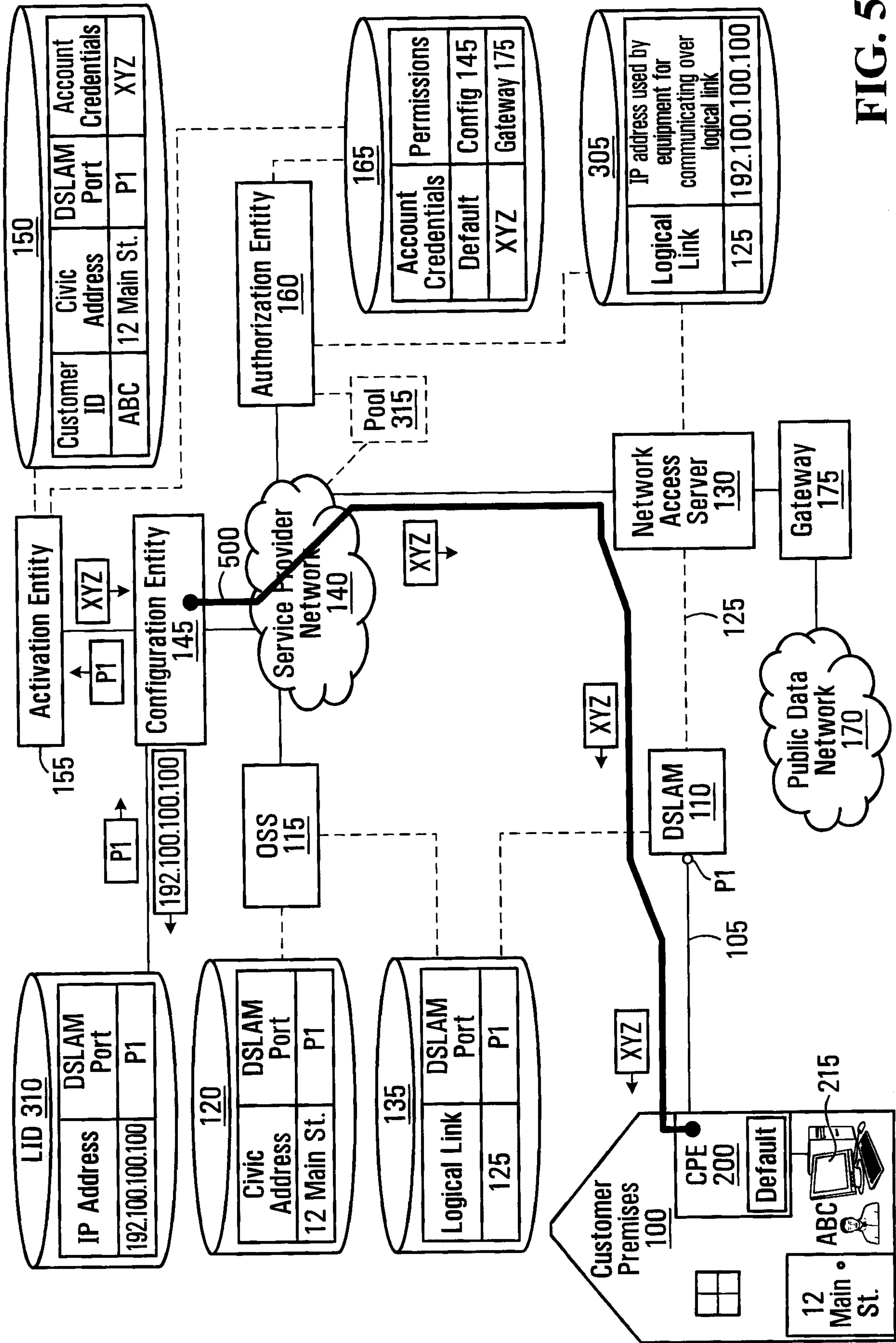


FIG. 5

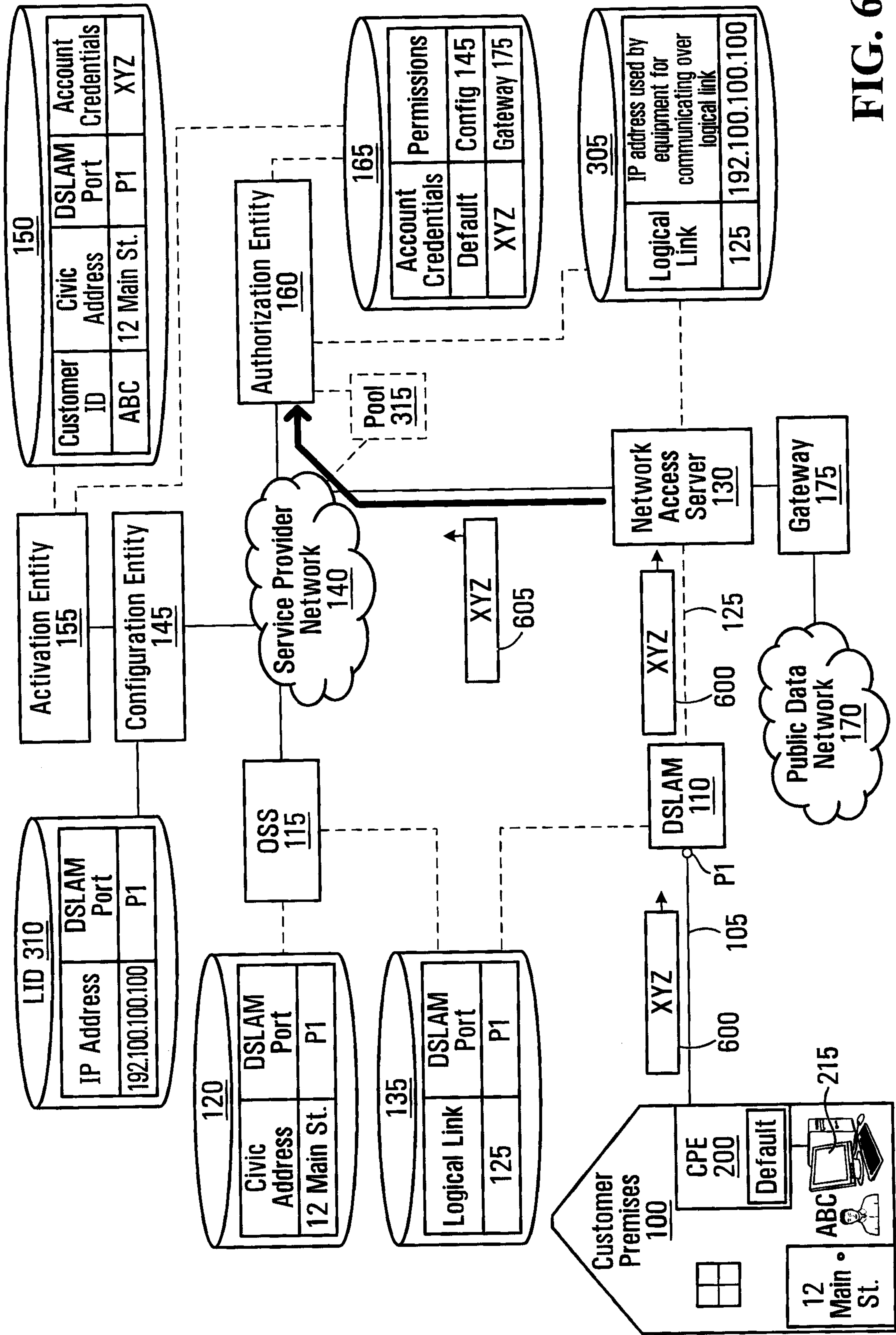


FIG. 6

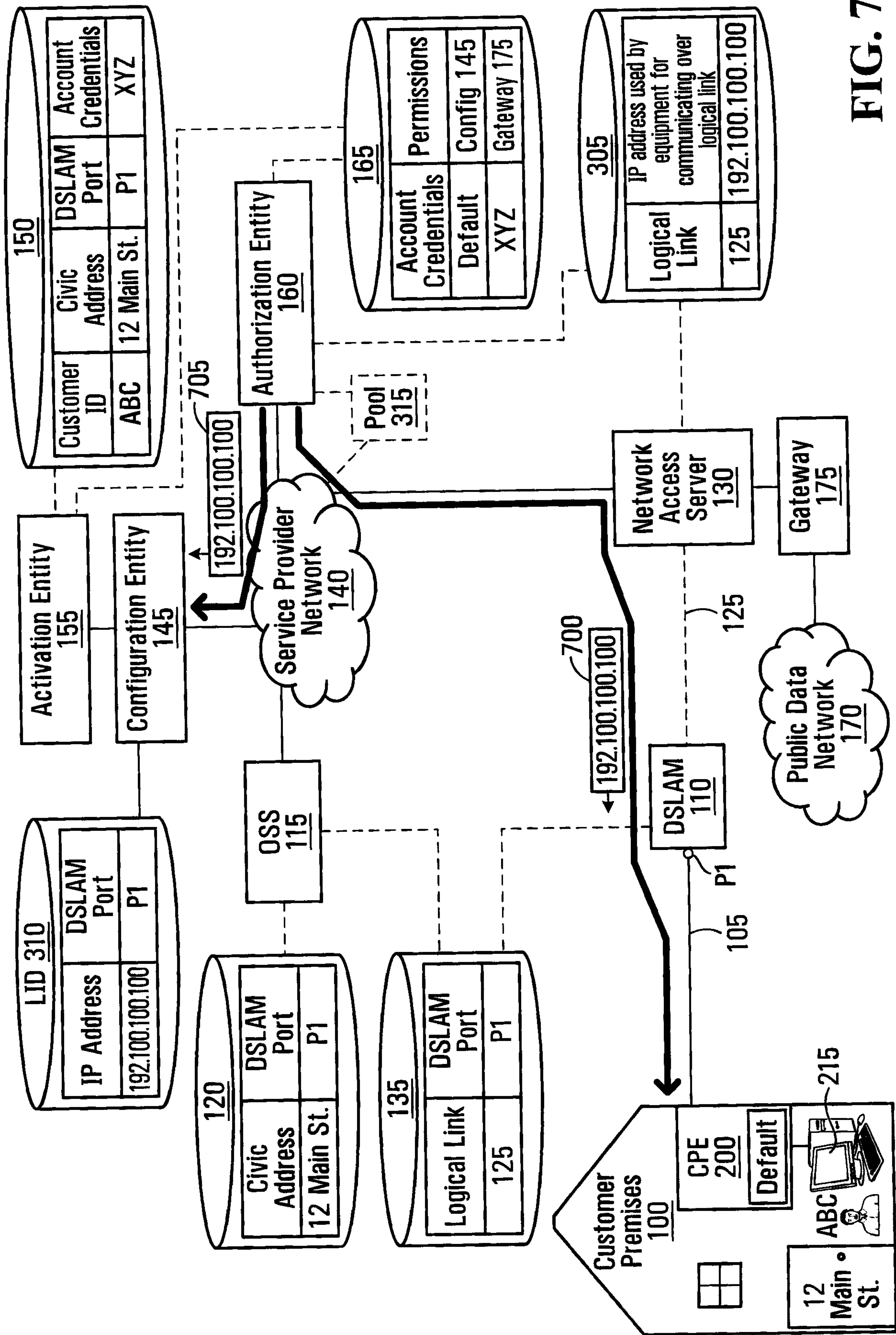


FIG. 7A

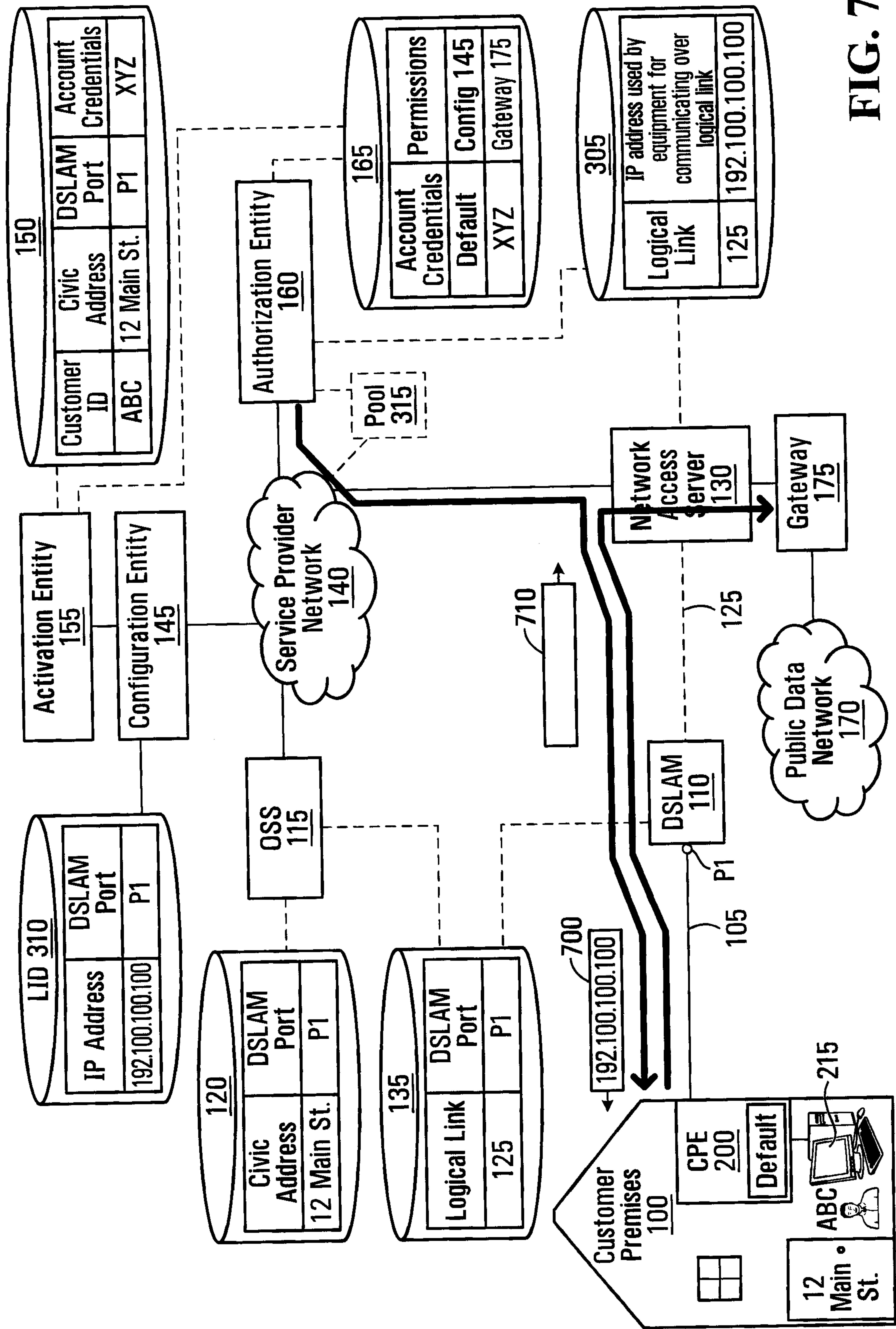


FIG. 7B

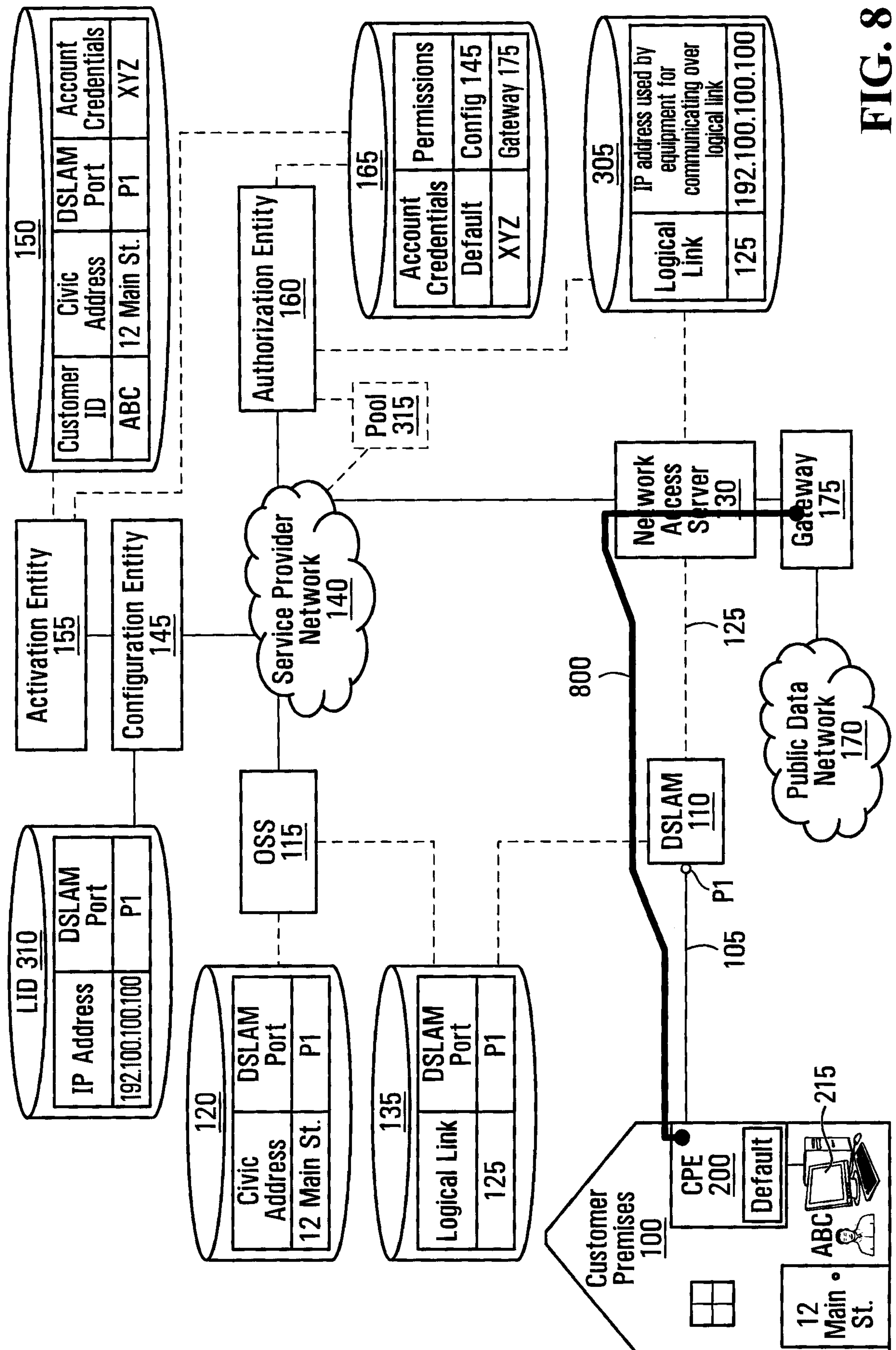


FIG. 8