

DESCRIPTION

ACCESS CONTROL AT AN INTERMEDIATE NETWORK ELEMENT
CONNECTING A PLURALITY OF DATA COMMUNICATIONS NETWORKS

5

Technical Field

The present invention relates to the use of access control in a plurality of data communications networks. An intermediate node controls access of edge nodes to the network resources in a singular or plurality of data communications networks. The grant of access to the network resources is decided by an external entity not co-located with the intermediate node. Such a deployment scenario is especially common in, but not limited to, a wireless data communications network where the intermediate node does not make a decision on access requests because of the need to reduce the processing load, or for ease of management.

20 Background Art

Information on documentation relating to prior arts referred to in this description will first be disclosed.

Non-Patent Document 1: IEEE 802.1 Working Group, "Port-Based Network Access Control", *IEEE 802.1X Standard*, June 2001.

Non-Patent Document 2: L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", *IETF RFC 2284*, March 1998.

Non-Patent Document 3: Basavaraj Patil and A. Yegin, "Charter of Protocol for carrying Authentication for Network Access", *IETF PANA WG Charter*, May 2002.

Non-Patent Document 4: C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", *IETF RFC 2865*, June 2000.

Non-Patent Document 5: P. R. Calhoun, J. Arkko, E. Guttman, G. Zorn, and J. Loughney, "Diameter Base Protocol", *IETF Internet Draft: draft-ietf-aaa-diameter-12.txt*, Work In Progress, July 2002.

Non-Patent Document 6: B. Aboba, "The Network Access Identifier", *IETF RFC 2486*, January 1999.

The Internet today has evolved to a stage where numerous peripheral data communications networks are deployed around a system of fixed network nodes. Most of these peripheral networks are controlled by different service providers or organizations. As such, these networks utilize different methods to implement access control. In addition, the underlying network infrastructures are vastly different between these peripheral networks (e.g. wireless networks versus wired-line networks). Possible access control methods are limited by the underlying network infrastructure used. As a result, there exist a wide range of access control methods.

For instance, the IEEE (Institute of Electrical and Electronics Engineers) 802.1x standard defines a network

access protocol for local area networks (Non-Patent Document 1). This standard defines an extension of the IETF (Internet Engineering Task Force) Extensible Authentication Protocol (EAP) (Non-Patent Document 2) for use in an IEEE 802 network, such as the IEEE 802.3 Ethernet or IEEE 802.11 Wireless network. Another example would be the ongoing effort of IETF in the Protocol for carrying Authentication for Network Access (PANA) Working Group (Non-Patent Document 3). Such network access protocols are usually deployed for local area networks, where the access control messages are limited to the local network.

In some situations, it might be necessary to transport the access control messages beyond the local area network. For instance, the server that grants access may be located in a different local area network. Such situations occur when a single administrative domain consists of a number of local area networks. A central access server is usually used to control these local area networks since it is easier to manage and maintain access information if it is collected in one central area, rather than being distributed to various local area networks. Furthermore, such a scenario is becoming more and more common with the widespread deployment of mobile network infrastructure, where a mobile terminal may be roaming in a plurality of wireless networks in one remote area, and authenticated by a server in its home area.

For these situations, a protocol capable of

traversing one or more packet switched networks is usually desired. Examples of such protocols are the widely deployed Remote Authentication Dial In User Service (RADIUS) protocol (Non-Patent Document 4), and the
5 Diameter (DIAMETER) Protocol (Non-Patent Document 5) of the IETF, which is currently being defined. These protocols are typically used to provide a backbone infrastructure for authentication, authorization, and accounting servers to communicate among each other.
10 Because these protocols are usually quite extensive, it is often considered too expensive (in both a computation and memory sense) to deploy in end terminals.

A typical deployment will be for terminals to use a local access protocol, such as IEEE 802.1x, to perform
15 access requests to a local intermediary. This intermediary then contacts a remote global server using RADIUS or DIAMETER that performs the actual authorization and authentication. Such an arrangement is most commonly seen in, but not limited to, a wireless network environment
20 where the wireless mobile node uses EAP to request access, and the wireless access point uses RADIUS or DIAMETER to verify the wireless user with a server on the wired network.

In a network access environment where the local nodes
25 uses one or more local access protocols such as PANA, IEEE 802.1x, or other EAP-based protocols, and the global authentication server uses another global access protocol such as DIAMETER or RADIUS, there is no efficient way

of maintaining the sessions between the two protocols at the intermediary. In addition, implementation of an intermediary is often tightly coupled to the access protocols, so that the change of an access protocol would
5 require substantial effort to modify the intermediary.

Of the studied prior arts, only DIAMETER (Non-Patent Document 5) specifies the possibility of an intermediary capable of linking two different protocols, known as a "translation agent". However, specification of such an
10 agent is absent. For 802.1x (Non-Patent Document 1), an intermediate "authenticator system" is defined. This, however, is confined to an intermediary using the same 802.1x protocol when communicating with both end-points of an authentication session. The charter of the PANA
15 working group (Non-Patent Document 3) specifically identifies the PANA protocol to be used within one hop, i.e. there can be no intermediary using a PANA protocol to communicate with both the local node and the global server. The intermediary, in such cases, will have to
20 use a different protocol to relay an authentication session to the global authentication server. Unfortunately, the architecture and operation of such an intermediary is not defined.

Furthermore, since many deployments of such an
25 intermediary are in a wireless environment, it is highly possible to envisage an intermediary which is itself mobile, such as a wireless access point in a train or aircraft. With such settings, there is a significant

possibility that the connection between the intermediate node and the global server may be momentarily down. This is especially true when there is a high frequency of handovers between base stations. Most implementations
5 of access control are not optimized for such a scenario. Often, access requests of local nodes are rejected or put on hold when the intermediate node cannot locate the global server. This is counter-productive if the local nodes just need to communicate with each other.

10

Disclosure of Invention

It is an object of the present invention to provide an access control method in a plurality of data communications networks that enables a plurality of local
15 nodes to communicate with each other even when connection between an intermediate node and global server is momentarily lost.

The present invention allows the intermediary to employ a high level state machine to synchronize between
20 two or more access protocols. In particular, the actual access protocols used are abstracted to a set of generic control messages for use in the state machine. As such, the problem of changing access protocols is limited to just the change in the affected protocol.

25 In addition, the invention disclosed in this description is designed with frequent temporary loss of connections taken into consideration. Thus, it has means of allowing local nodes to communicate with each other

even when the global server cannot be contacted.

The present invention involves operation of an intermediate node controlling access of local nodes in a singular or plurality of data communications networks.

5 When a local node requires network access, the intermediate node is configured to contact a global server to authorize the request. The protocols used by the local nodes and global server can be identical or different. When connection to the global server is momentarily lost,
10 the present invention allows the intermediary to temporarily grant network access to the local nodes, so that local nodes can still communicate with each other.

Brief Description of Drawings

15 FIG.1 is a drawing showing a communication network scenario, illustrating communication networks connected to an intermediate network node in a typical scenario. With the aid of the global server, the intermediate node controls access to local and global network resources
20 by the local nodes.

FIG.2 is a drawing showing a message flow sequence in access control, depicting a general flow sequence of control messages when performing access control of a local node by a global server. The intermediate node is
25 functioning as a relaying agent between the local node and the global server. Fourteen generic control messages are shown here.

FIG.3 is a state transition diagram showing state

transitions when the intermediate node receives a new data packet from a local node that has no active session associated with it.

FIG.4 is a state transition diagram showing state transitions when the intermediate node receives a new data packet from a local node that has no active session associated with it. This state diagram is simplified from FIG.3 when an acknowledgement for release of network resources is unnecessary.

FIG.5 is a flowchart for processing packets, depicting the algorithm employed by the intermediate node to process a packet received from a local node.

FIG.6 is a drawing showing the architecture of the intermediate node, consisting of local and global access protocol units to handle access protocol messages used by local nodes and the global server, a message mapping unit that maps the actual access protocol messages to one of the 15 generic control messages, and a state machine that implements the state transition diagram.

20

Best Mode for Carrying out the Invention

With reference now to the accompanying drawings, embodiments of the present invention will be explained in detail below.

25 An apparatus for controlling network resources at an intermediate network element is disclosed here. To help understand the present invention, the following definitions are used:

- A "packet" is a self-contained unit of data of any possible format that can be delivered on a data network.
- An "intermediary", an "intermediate network element", and an "intermediate node" are equivalent,
5 and are used interchangeably, unless otherwise specified, to refer to a gateway, an access router or an intelligent network hub to which the present invention applies.

In the following description, for the purpose of
10 explanation, specific numbers, times, structures, and other parameters are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to anyone skilled in the art that the present invention may be practiced without
15 these specific details.

The invention disclosed in this description is designed to be employed in an intermediate network node, which is connected to two or more data communications networks, as illustrated in FIG.1. The subject of the
20 present invention, the intermediate node (103) controls access to local networks (102) and a global network (104) by local nodes (101). Whenever there is a new local node (101) requesting network access, the intermediate node (103) will have to consult the global server (105), which
25 is the authority in granting network access to local nodes (101).

FIG.2 illustrates a typical flow sequence of control messages between the intermediate node (103), a local

node (101) and the global server (105).

Usually, the local node (101) will have to request access by sending the intermediate node (103) a local access request message, as signified by L-ACCESS-REQ
5 (202). This message will normally identify the local node (101), and state the network resources required. However, a local node (101) may assume that such a request is not necessary and directly attempt to use network resources, such as by sending data packets to a single or plural
10 number of nodes in other local networks (102) or the global network (104). When the intermediate node (103) receives such packets from a local node (101) that has not been previously granted access (or for which a previous grant has expired), the intermediate node (103) can notify the
15 local node (101) to send an L-ACCESS-REQ (202) message by sending an L-ACCESS-INIT (201) message.

When the intermediate node (103) receives an L-ACCESS-REQ (202), it then contacts the global server (105) with a G-ACCESS-REQ (203) message. This control
20 message informs the global server of the new access request from the local node (101). The global server (105) can then accept, reject, or authenticate the request. To accept the request, the global server (105) sends the intermediate node (103) a G-ACCESS-OK (208) message.
25 When the intermediate node (103) receives this, it grants access to the local node (101) by sending an L-ACCESS-OK (209) message to the local node (101). From this point on, the local node (101) can access the requested network

resource until it chooses to release it, or until the grant expires.

To release the network resource, the local node (103) can send the intermediate node (103) an L-LOGOFF (210) message. The intermediate node (103) will acknowledge the release by replying with an L-LOGOFF-ACK (211) message. At the same time, it will inform the global server (105) that the local node (103) has released the resource by sending a G-LOGOFF (212). The global server (105) acknowledges with a G-LOGOFF-ACK (213) control message. It must be noted that acknowledgement of the release of network resources is optional. In such cases, the L-LOGOFF-ACK (211) and G-LOGOFF-ACK (213) control messages are unnecessary.

When the global server (105) rejects the request, it sends the intermediate node (103) a G-ACCESS-REJ (214) control message. Upon receiving this, the intermediate node notifies the local node (101) with an L-ACCESS-REJ (215) message.

Alternatively, the global server (105) can choose to authenticate the local node (101) by sending the intermediate node (103) a G-AUTH-REQ (204) message. The intermediate node (103) relays this with an L-AUTH-REQ (205) message to the local node (101). The local node (101) will have to respond to the authentication with an L-AUTH-RES (206) message sent to the intermediate node (103). The intermediate node (103) forwards this to the global server (105) with a G-AUTH-RES (207) control

message. The global server (105) can then accept or reject the request based on the authentication response. In addition, it can choose to further authenticate the local node (101) with another G-AUTH-REQ (204) control
 5 message.

Due to the fact that L-LOGOFF-ACK (211) and G-LOGOFF-ACK (213) messages are optional, two sets of generic control messages can be identified: first, the full set consisting of all fifteen messages defined above,
 10 as cited in feature (3) described later herein, and second, a reduced set consisting of only thirteen messages, without the L-LOGOFF-ACK (211) and G-LOGOFF-ACK (213) messages, as cited in feature (2) described later herein.

As clearly shown in the above illustration, the
 15 intermediate node (103) will have to maintain states during an access request session to synchronize between the messages sent from and to the local node (101), and the messages sent to and from the global server (105). To facilitate this, the data structure shown in Data Format
 20 1 below, as cited in feature (8) described later herein, is defined.

```

                typedef struct __session_tag__ {
                                NODE_INFO    local_node_info;
25                                STATE      state;
                                BUFFER      packet[];
                } SESSION;
  
```

Data Format 1: The *SESSION* Structure.

The data format *SESSION* contains three major fields, *local_node_info*, *state*, and the *packet* array. The *local_node_info* field is used to store the identification information of the local node (101). This can include
5 user identification, network access identifier (Non-Patent Document 6), and some unique identifier of the network interface card. The *state* field is used to store the current status of the access request. Its usage will become apparent later in this description when the
10 operation of the intermediate node (103) is disclosed further. The *packet* array is used to temporarily store outgoing data packets sent from or to the local node (101) when the access request of the local node (101) is pending, or when there is a temporary loss of global network
15 connectivity. Use of the packet array will be disclosed further later in this description.

To successfully maintain the two sessions, one between the local node (101) and the intermediary, and the other between the intermediary and the global server
20 (105), a set of states and transitions among the states is needed. Features (11) and (12) described later herein specify the minimal set of states and state transitions that is crucial for the operation of the present invention. However, in order for the present invention to operate
25 correctly, a more complete set of states and state transitions is necessary. Two such complete sets are disclosed in this document, as described by the state transition diagrams shown in FIG.3 and FIG.4, with

reference to features (14), (15), (17) and (18) described later herein. It should be apparent to anyone skilled in the art that other sets of states and state transitions can be defined to implement the invention disclosed.

5 Nonetheless, such a set will incorporate in some form the minimal set cited in features (11) and (12) described later herein.

FIG.3 is the state diagram when the set of generic control messages includes the L-LOGOFF-ACK and
10 G-LOGOFF-ACK messages. When these messages are not necessary, the state diagram can be simplified to the one shown in FIG.4. A total of nine distinct states are defined, as follows:

- **S-INIT (301):**

15 The initial state when a new packet is received from a local node (101) that has not previously been granted access, and has no pending access grant. A new *SESSION* structure will be allocated and initialized for this local node (101). The *SESSION* structure will continue to exist
20 until the **S-DISCONN (307)** state is reached. Thus a method of checking if a local node (101) has any pending or granted access is to check if there is an active *SESSION* structure associated with the local node (101) by locating a *SESSION* structure that has similar *local_node_info*.

25 This state is a transient state in that it will always transit to a different state. The state it transits to depends on the received packet type. If the received data packet is an L-ACCESS-REQ (202) message, then the next

state will be **S-RES-WAIT** (303), as indicated by the transition denoted by literal 311. At this transition, the variable "try" is set to number n_{RES} , which defines the number of G-ACCESS-REQ (203) messages to be sent before
5 declaring that connection has failed. If the packet received is an ordinary data packet, then the next state will be S-ACC-WAIT (302), as indicated by the transition denoted by literal 310. At this transition, the variable "try" is set to number n_{ACC} , which defines the number of
10 L-ACCESS-INIT (201) messages to be sent before declaring that connection has failed.

- **S-ACC-WAIT** (302):

This state is entered when the intermediate node (103) receives an ordinary packet from a local node (101),
15 from which it has not received an L-ACCESS-REQ (202). This is the state in which the intermediate node (103) is waiting for the local node (101) to send an L-ACCESS-REQ (202) message. Once this state is entered, an L-ACCESS-INIT (201) message will be sent to the local
20 node (101), and the variable "try" will be decremented. At the same time, a timer of value t_{ACC} will be started. When this timer expires, a new state transition is triggered. If "try" is greater than zero, a self-transition takes place, i.e. the **S-ACC-WAIT** (302)
25 state is re-entered, as indicated by the transition denoted by literal 320.

On the other hand, if the timer expires with "try" equal to zero, the attempt at connection with the local

node (101) is deemed to have failed, and the next state of transit is **S-DISCONN** (307), as indicated by the transition denoted by literal 322. A state transition to **S-RES-WAIT** (303) can occur regardless of the timer
 5 when an L-ACCESS-REQ (202) message is received from the local node (101). This is the expected state transition. During this transition the variable "pkt" is set to G-ACCESS-REQ (203), and "try" is set to n_{RES} , as denoted by literal 321.

10 • **S-RES-WAIT** (303):

This state is entered when the intermediate node (103) receives an L-ACCESS-REQ (202) from the local node (101). This is the state in which the intermediate node (103) is waiting for the global server (105) to send back
 15 a response, in the form of a G-ACCESS-OK (208) to accept the access request, a G-ACCESS-REJ (214) to reject the access request, or a G-AUTH-REQ (204) to authenticate the access request.

Upon entering this state, the intermediate node
 20 (103) will send a G-ACCESS-REQ (203) or a G-AUTH-RES (207) to the global server (105) depending on the value of "pkt", decrement the variable "try", and start a timer of value t_{RES} . When this timer expires, a new state transition will be triggered. If "try" is greater than zero, a
 25 self-transition takes place, i.e. the **S-RES-WAIT** (303) state is re-entered, as indicated by the transition denoted by literal 330. If "try" is zero when the timer expires, the transition denoted by literal 332 will be

taken. Depending on the policy of intermediate node (103) as cited in features (9) and (10) described later herein, the next state will be either **S-CONN-LOST** (308) or **S-DISCONN** (307). If the policy is to assume that access
 5 is granted when the intermediate node (103) cannot contact the global server (105) (on-lost), the next state will be **S-CONN-LOST** (308), and an L-ACCESS-OK (209) message will be sent to the local node (101), as indicated by the transition denoted by literal 334. On the other hand,
 10 if the policy is to assume that access is denied when connection to global server (105) is lost (on-lost), then the next state will be **S-DISCONN** (307), and an L-ACCESS-REJ (215) message is sent to the local node (101), as indicated by the transition denoted by literal 333.

15 Transitions to other states from **S-RES-WAIT** (303) can occur even when the timer has not expired. This happens when the intermediate node (103) receives a message from the global server (105). If the received message is a G-ACCESS-REJ (214), transition to the state
 20 **S-DISCONN** (307) will occur, as denoted by literal 331. At the transition, an L-ACCESS-REJ (215) will be sent to the local node (101). If the received message is a G-ACCESS-OK (208), transition to the state **S-CONN** (305) will occur, as denoted by literal 336. During this
 25 transition, an L-ACCESS-OK (209) message is transmitted to the local node (101), and the variable "try" is set to n_{CONN} . Otherwise, if the received message is a G-AUTH-REQ (204), the next state will be **S-AUTH-WAIT** (304).

During this transition denoted by literal 335, the variable "try" is set to n_{AUTH} .

- **S-AUTH-WAIT (304):**

This state is entered when the intermediate node
5 (103) receives a G-AUTH-REQ (204) from the global server (105). This is the state in which the intermediate node (103) is waiting for the local node (101) to respond to the authentication with an L-AUTH-RES (206) message. When this state is entered, an L-AUTH-REQ (205) is sent
10 to the local node (101) and the variable "try" is decremented. In addition, a timer of value t_{AUTH} will be set.

When this timer expires or a response is received from the local node (101), a state transition will occur.
15 If the timer expires with "try" greater than zero, a self-transition will occur, as denoted by literal 340. If "try" is zero when the timer expires, it is assumed that connection with the local node (101) is lost, and the next state will be **S-LOGOFF** (306) if the full set
20 of generic control messages is used (FIG.3), as indicated by the transition denoted by literal 342. On the other hand, if the reduced set of generic control messages is used, the next state will then be **S-DISCONN** (307), as indicated by the transition denoted by literal 442.

25 State transitions can also occur when the intermediate node (103) receives an L-AUTH-RES (206) response from the local node (101). In this case the next state is **S-RES-WAIT** (303). The variable "try" is set to

`nRES` and the variable "`pkt`" set to G-AUTH-RES (207), as indicated by the transition denoted by literal 341.

- **S-CONN** (305):

This state is entered when the intermediate node
 5 (103) receives a G-ACCESS-OK (208) message indicating that the access request of the local node (101) is granted. Upon entering this state, the variable "`try`" will be decremented, and a timer of value `tCONN` will be set. When the timer expires, a state transition will occur. If
 10 "`try`" is greater than zero when the timer expires, a self-transition will occur, as denoted by literal 350. If "`try`" is zero when the timer expires, the connection with the local node (101) is assumed to be lost, since the intermediate node (103) has not received any packets
 15 from the local node (101).

When this happens, the transition denoted by literal 353 to the state **S-LOGOFF** (306) will be taken, when the full set of generic control messages is used (FIG.3). If the reduced set is used (FIG.4), a transition as denoted
 20 by literal 452 will be taken, which leads directly to the **S-DISCONN** (307) state. During the transition denoted by literal 452, a G-LOGOFF (212) message will be sent to the global server (105).

Even when the timer has yet to expire, state
 25 transitions can still occur when the intermediate node (103) receives packets from the local node (101). If the packet received is an L-LOGOFF (210) message to indicate the release of network resources, the next state will

be **S-LOGOFF** (306) for the full set of generic messages (FIG.3). During this transition denoted by literal 352, the intermediate node (103) will send an L-LOGOFF-ACK (211) message to the local node (101) and set the variable
 5 "try" to a variable of n_{OFF} .

On the other hand, if the reduced set is used (FIG.4), the transition denoted by literal 452 will be taken, leading to the state **S-DISCONN** (307). During the transition denoted by literal 452, a G-LOGOFF (212)
 10 message will be sent to the global server (105). However, if the packet is a normal data packet, a self-transition to **S-CONN** (305) will occur, and the variable "try" is reset to the value of n_{CONN} , as indicated by the transition denoted by literal 351.

15 • **S-LOGOFF** (306):

This state is entered when the intermediate node (103) receives an L-LOGOFF (210) message from the local node (101), and the full set of generic control messages is used (FIG.3). This is the state in which the
 20 intermediate node (103) sends the global server a G-LOGOFF (212) message, and waits for the G-LOGOFF-ACK (213) acknowledgement. Once this state is entered, a G-LOGOFF (212) message is sent to the global server, and the variable "try" is decremented. Furthermore, a timer of value t_{OFF}
 25 will be set. When the timer expires with "try" greater than zero, a self-transition occurs, as indicated by the state transition denoted by literal 360. If the timer expires with "try" equal to zero, or if a G-LOGOFF-ACK

(213) message is received from the global server (105), a state transition (361) to **S-DISCONN** (307) will occur.

- **S-DISCONN** (307):

This state is entered when the intermediate node
 5 (103) decides that the local node (101) no longer requires the network resources. Upon entering this state, the *SESSION* data structure associated with the local node (101) will be deleted. No more state transitions will occur.

- 10 • **S-CONN-LOST** (308):

This state is entered when the intermediate node (103) decides that connection to the global network (104) is lost, and the policy is to assume that an access request of the local node (101) is granted until connection to
 15 the global network (104) is restored. The session will always stay in this state until it receives an L-LOGOFF (210) message from the local node (101), or until connection to the global network (104) is restored.

In the former case, an L-LOGOFF-ACK (211) message
 20 is returned to the local node (101) and the next state is **S-DISCONN** (307), as indicated by the transition denoted by literal 381, if the full set of generic control messages is used (FIG.3). If the reduced set is used instead (FIG.4), the next state is **S-DISCONN** (307), as indicated
 25 by the transition denoted by literal 481. On the other hand, if connection to the global network (104) is restored, the state will be **S-RESET-WAIT** (309). During this transition denoted by literal 380, the variable "try"

is set to a value of n_{RST} .

- **S-RESET-WAIT (309):**

This state is entered when the intermediate node (103) has just regained connection to the global network.

5 This is the state in which it is waiting to receive a packet sent by the local node (101) to verify that the local node (101) is still active, before resuming the previous access request session. When this state is entered, the variable "try" is decremented and a timer
10 is set with value t_{RST} . When this timer expires and "try" is greater than zero, a self-transition (390) occurs.

Otherwise, if this timer expires with "try" equal to zero, the local node (101) is assumed to no longer need the network resources. In this case, a transition
15 as denoted by literal 391 to the state **S-DISCONN** (307) occurs. When a packet is received from the local node (101), the session will leave this state. If the packet is an L-LOGOFF (210) message, the next state will be **S-LOGOFF** (306), if the full set of generic control messages
20 is used (FIG.3).

Together with this state transition denoted by literal 392, the variable "try" is set to n_{OFF} and the local node is acknowledged with an L-LOGOFF-ACK (211) message. Otherwise, if the reduced set is used instead
25 (FIG.4), the next state will be **S-DISCONN** (309), as indicated by the transition denoted by literal 492. During this transition 492, a G-LOGOFF (212) control message will be sent to the global server (105).

On the other hand, if the packet received is not an L-LOGOFF (210) message, the local node is still actively using the network resource, and thus the access request session must be resumed. This is indicated by the state transition, denoted by literal 393, to the state **S-ACC-WAIT** (302). During this transition, the variable "try" is set to `nACC`.

In the above description of the state diagrams, a few references are made to `nACC`, `nRES`, `nAUTH`, `nRST`, `nCONN`, and `nOFF`. These are "retry parameters" employed to control the number of re-transmission attempts. It should be apparent to anyone skilled in the art that should re-transmission of any of the control packets not be desired, or be otherwise prohibited, the state transition diagram disclosed is still applicable by setting the corresponding "retry parameter" to a value of 1. In addition, a few references are made to `tACC`, `tRES`, `tAUTH`, `tCONN`, `tRST`, and `tOFF`. These are time-out parameters to control the re-transmission period and state transition timing.

The present invention allows the intermediate node (103) to temporarily grant access to local nodes (101) when the connection to the global network (104) is down. As cited in features (9) and (10) described later herein, this is a configurable option, depending on policy. Such a configuration option, in its simplest form, can manifest itself as a bit, where a bit value of zero implies that the policy is to temporarily reject access, and a bit

value of one implies that the policy is to temporarily grant access. It should be apparent to anyone skilled in the art that other forms of implementation are possible, such as using a string of bits to indicate the switching on or off of the configuration option.

During the period when connection to the global network (104) is down, if the policy is to grant the local node (101) access, all data packets sent to other local nodes (101) in the local networks (102) connected to the intermediate node (103) are forwarded. All data packets destined for the global network (104), however, cannot be forwarded. These are stored in a buffer associated with the local node (101), as cited in features (26) and (27) described later herein.

For this purpose, the *packet* array in the *SESSION* structure is used. This can be used to store data packets sent by the local node (101) destined for the global network (104) when connection to the global network (104) is down. When connection is restored and access has been granted by the global server (105), packets queued in the *packet* array are then processed as if they are received after access has been granted.

The *packet* array can also be used when connection to the global network (104) is alive. This is to store data packets sent by the local node (101) to any destination, including the local network (102), when the access request has yet to be granted by the global server (105), as cited in features (24) and (25) described later herein. For

instance, it is when the session is still in the state **S-RES-WAIT** (303) or **S-AUTH-WAIT** (304). Once the access has been granted, data packets queued in the *packet* array are then processed as if they are received after access
5 has been granted.

FIG.5 illustrates the algorithm used by the intermediate node (103) when a packet is received from the local node (101), with reference to features (22) and (23) described later herein. The list of *SESSION*
10 structures is first searched to locate a *SESSION* that is associated with the local node (101), as shown in the step denoted by literal 501. This search can be a simple search through all the *SESSION* structures, or a hash function on the *local_node_info* field can be used. If
15 no structure is found, a new state machine governed by the state machine shown in FIG.3 or 4 is instantiated, as shown in the steps denoted by literals 502 and 503.

If a *SESSION* structure is found, the packet is next checked to see if it is an L-ACCESS-REQ (202), L-AUTH-RES
20 (206), or L-LOGOFF (210) message, as indicated by the step denoted by literal 504. If it is, the message is processed as dictated by the state transition diagram, as shown in the step denoted by literal 505. Otherwise, the state is checked to see if it is **S-CONN** (305) or
25 **S-CONN-LOST** (308), as shown in the steps denoted by literals 506 and 508.

If the state is **S-CONN** (305), the packet is sent in the normal way and the state machine proceeds to the

next state, as indicated by the step denoted by literal 507. Otherwise, if the state is **S-CONN-LOST** (308), the packet is checked to see if it is destined for the global network (104) or local network (102). If the packet is
5 destined for the local network (102), it is sent and the state machine proceeds to the next state, as shown in the step denoted by literal 512. If the packet is destined for the global network (104), it is queued to the *SESSION* structure and the state machine proceeds to the next state,
10 as shown in the step denoted by literal 511. On the other hand, if the state is neither **S-CONN** (305) nor **S-CONN-LOST** (308), the step denoted by literal 509 is taken. In this step, the packet is queued to the *SESSION* structure and the state machine proceeds to the next state.

15 In any practical implementation of the disclosed invention, it is only reasonable to set a limit on the number of packets to be queued. If more packets need to be queued when the *packet* array is full, the incoming packets can be silently discarded. Furthermore, it
20 should be obvious to someone skilled in the art that by setting the size of the *packet* array to zero, the present invention is reduced to a system where no queuing of packets is performed.

With reference to feature (1) described later herein,
25 FIG. 6 depicts the architecture of the intermediate node (103). It consists of a singular or plurality of local access protocol units (601) that handle the access protocol used by local nodes (101) in the local networks

(102), and a singular or plurality of global access protocol units (602) that handle the access protocol used by the global server (105).

Messages to and from the local node (101) are handled
5 by the local access protocol unit (601) as indicated by the data path denoted by literal 611. Messages to and from the global server (105) are handled by the global access protocol unit (602) as indicated by the data path denoted by literal 612. The architecture shown in FIG.6
10 also contains a message mapping unit (603), which maps the messages used by the local and global access protocols to one of the fifteen control messages defined in FIG.2, and the state machine (604), which implements the state transition diagram described in FIG.3 or FIG.4.

15 Messages from the local access protocol unit (601) and global access protocol unit (602) are mapped to a generic control message, as shown by the data paths denoted by literals 613 and 614 respectively. The mapped messages are then passed to the state machine (604), as shown by
20 the data path denoted by literal 615. When the state machine (604) decides to transmit messages to the local node (101) or global server (105), these messages are passed to the message mapping unit (603) via the data path denoted by literal 615 to be mapped to the actual
25 control messages. The actual control messages are passed down to the local access protocol unit (601) or global access protocol unit (602) via the data paths denoted by literals 613 and 614 respectively, to be sent to the

local node (101) or global server (105).

It is up to implementers to use the full set of fifteen generic control messages, or the reduced set without L-LOGOFF-ACK (211) and G-LOGOFF-ACK (213). The message mapping unit (603) should work accordingly, as cited in features (4) and (5) described later herein. In fact, with reference to features (6) and (7) described later herein, a general solution is to use the full set, where the L-LOGOFF-ACK (211) generic message maps to a null message, i.e. no actual control message is sent by the local access protocol unit (601), and the G-LOGOFF-ACK (213) generic message maps to a virtual message, wherein the message is always implied to have been received whenever a G-LOGOFF message is sent.

Similarly, implementers can base the state machine (604) on the state transition diagram disclosed in FIG.3 or FIG.4, according to the choice of use of the full set of generic control messages, as cited in feature (17) described later herein, or use of the reduced set of generic control messages, as cited in feature (19) described later herein. In fact, a general solution is to use the state transition diagram depicted in FIG.3. When the reduced set of generic control messages is used, one can derive the operation of the state transition diagram illustrated in FIG.4 by setting n_{OFF} to one, and the timer value t_{OFF} to a very small value, such as one microsecond, as cited in features (21) and (22) described later herein.

The present invention allows an intermediary

controlling the network access of local network nodes in a singular or plurality of local data communications networks. It allows the decision to grant network access to be located in an external global server, so that the intermediary does not have to be overloaded with authentication and access issues. With the employment of the present invention, the intermediate node can easily synchronize the access request messages between the local node and the global server. In addition, the disclosed invention also allows intermediaries to temporarily grant access to local nodes when the global network is lost.

This allows the local nodes to continue to communicate with one another when global connection is temporarily down. Packets sent to the global network are also queued so that once global connection is restored (and access is granted), these packets can be transmitted immediately without having to wait for the local nodes to re-transmit.

Features of the present invention are listed below.

(1) A network access control framework apparatus for controlling access to resources in a plurality of packet-switched data communications networks, wherein network elements, hereafter known as local nodes, in one or more data communications networks, hereafter known as local networks, are access controlled, and one or more data communications networks, hereafter known as global networks, are not access controlled by the said access control framework, comprises:

i. a singular or plurality of local access protocol units, wherein a local access protocol unit services access requests from local nodes using a specific access protocol;

5 ii. a singular or plurality of global access protocol units, wherein a global access protocol unit services access responses from one or more network elements, hereafter known as global servers, in the global network, wherein the global servers provide authoritative
10 responses to access requests from the local nodes;

 iii. a message mapping unit that maps the control messages used in the said singular or plurality of local access protocol units, and control messages used in the said singular or plurality of global access protocol units,
15 to a generic set of control messages; and

 iv. a state machine to control the operation of the said network access control framework apparatus based on the said generic set of control messages.

(2) The set of generic control messages wherein the
20 message mapping unit maps to and from the control messages used by the singular or plurality of local access protocol units and the singular or plurality of global access protocol units, as cited in (1) above, comprises:

 i. an L-ACCESS-INIT generic control message that
25 is used to inform local nodes that access request is required;

 ii. an L-ACCESS-REQ generic control message that is sent from the local nodes to request access to the

controlled network resources;

iii. a G-ACCESS-REQ generic control message that is used to inform the global server that a local node is requesting access to the controlled network resources;

5 iv. a G-AUTH-REQ generic control message that is sent from the global server to request authentication information on the local node that is requesting access to the controlled network resources;

10 v. an L-AUTH-REQ generic control message that is sent to the local node that is requesting access to the controlled network resources to request authentication information from the said local node;

15 vi. an L-AUTH-RES generic control message that is sent from the local node to provide authentication information that is sent from the local nodes to request access to the controlled network resources;

20 vii. a G-AUTH-RES generic control message that is used to send authentication information from the local node that is requesting access to the controlled network resources to the global server;

viii. a G-ACCESS-OK generic control message that is sent from the global server to indicate that the request of access to the controlled network resources by the local node is granted;

25 ix. an L-ACCESS-OK generic control message that is used to inform the local node that the request to access the controlled network resources is granted;

x. an L-LOGOFF generic control message that is sent

from the local node to indicate the release of access to the controlled network resources;

xi. a G-LOGOFF generic control message that is sent to the global server to indicate the release of access
5 to the controlled network resources by the local node;

xii. a G-ACCESS-REJ generic control message that is sent from the global server to indicate that the request for access to the controlled network resources by the local node is rejected; and

10 xiii. an L-ACCESS-REJ generic control message that is used to inform the local node that the request to access the controlled network resources is rejected.

(3) The set of generic control messages as cited in (2) above wherein the message mapping unit maps to
15 and from the control messages used by the singular or plurality of local access protocol units and the singular or plurality of global access protocol units as cited in (1) above, whereas an acknowledgement is necessary when an indication of release of access to the controlled
20 network resources is required, further comprises the following additional control messages:

i. an L-LOGOFF-ACK generic control message that is used to acknowledge to the local node that the access to the controlled network resources is released; and

25 ii. a G-LOGOFF-ACK generic control message that is sent from the global server to acknowledge the release of the access to the controlled network resources by the local node.

(4) By means of the message mapping unit cited in (2) above, control messages used by the singular or plurality of local access protocol units and the singular or plurality of global access protocol units, as cited in (1) above, are mapped to one of the generic control messages as cited in (2) above.

(5) By means of the message mapping unit cited in (3) above, control messages used by the singular or plurality of local access protocol units and the singular or plurality of global access protocol units, as cited in (1) above, are mapped to one of the generic control messages as cited in (3) above.

(6) The method used in the message mapping unit of the network access control framework apparatus, as cited in (1) above, to generalize the set of fifteen generic control messages cited in (3) above to the reduced set of thirteen generic control messages cited in (2) above, comprises the steps of:

i. mapping the L-LOGOFF-ACK generic control message to a null message, wherein no actual message is sent by the local access protocol unit, when no acknowledgement is necessary for the release of the access to the controlled network resources; and

ii. mapping the G-LOGOFF-ACK generic control message to a virtual message, wherein the G-LOGOFF-ACK generic control message is assumed to have been received immediately after an indication of the release of the access to the controlled network resources is sent to

the global server, when no acknowledgement is necessary for the release of the access to the controlled network resources.

(7) The message mapping unit cited in (1) above, wherein control messages used by the singular or plurality of local access protocol units and the singular or plurality of global access protocol units, as cited in (1) above, are mapped to one of the generic control messages as cited in (3) above, utilizes the method as cited in (6) above to generalize the set of fifteen generic control messages cited in (3) above to the reduced set of thirteen generic control messages cited in (2) above.

(8) The data format used by the network access control framework apparatus, as cited in (1) above, wherein a structure of the said data format is associated with a local node throughout the session beginning from a request for access to network resources to the release of the network resource, comprises:

i. a field that stores information about the associated local node, wherein the said field stores a sufficient amount of information such that the associated local node can be identified using the information;

ii. a field that stores the current status of the state machine, as cited in (1) above; and

iii. a field that can be used to temporarily store data packets sent by the associated local node.

(9) The network access control framework apparatus for controlling access to resources in a plurality of

packet-switched data communications networks, as cited in (1) above, further comprises a mechanism to switch the policy of the said network access control framework apparatus to one of the following:

5 i. in the case where it is determined that the connection to the global server is lost, momentarily or otherwise, the policy is to reject all ongoing or newly initiated requests for access to the said network resources during the period of time for which it remains
10 so determined that the connection to the global server is lost; or

 ii. in the case where it is determined that the connection to the global server is lost, momentarily or otherwise, the policy is to accept all ongoing or newly
15 initiated requests for access to the said network resources during the period of time for which it remains so determined that the connection to the global server is lost.

(10) The mechanism to switch the policy of the
20 network access control framework apparatus for controlling access to resources in a plurality of packet-switched data communications networks, as cited in (1) above, switches to one of the following:

 i. in the case where it is determined that the
25 connection to the global server is lost, momentarily or otherwise, the policy is to reject all ongoing or newly initiated requests for access to the said network resources during the period of time for which it remains

so determined that the connection to the global server is lost; or

ii. in the case where it is determined that the connection to the global server is lost, momentarily or
5 otherwise, the policy is to accept all ongoing or newly initiated requests for access to the said network resources during the period of time for which it remains so determined that the connection to the global server is lost.

10 (11) The set of states used in the state machine that controls the operation of the network access control framework apparatus, as cited in (1) above, comprises:

i. an S-ACC-WAIT state, wherein a control message is sent to the local node indicating that an access request
15 is required, and the said state machine is waiting for an access request message to be sent by the local node;

ii. an S-RES-WAIT state, wherein a control message is sent to the global server indicating that an access request is made, and the said state machine is waiting
20 for a response to be sent by the global server;

iii. an S-CONN state, wherein access to the requested network resources is granted to the local node;

iv. an S-DISCONN state, wherein the access to all network resources by the local node is released, and the
25 structure with the data format specified in (8) above that is associated with the local node is deleted;

v. an S-CONN-LOST state, wherein the said state machine determines that connection to the global server

is lost, and the policy specified in (9) above is set to allow access temporarily when connection to the global server is lost; and

vi. an S-RESET-WAIT state, wherein the said state
5 machine determines that connection to the global server is regained, whereas the prior state is the S-CONN-LOST state.

(12) The set of transitions between the states cited
in (11) above, wherein these transitions are used in the
10 state machine that controls the operation of the network access control framework apparatus, as cited in (1) above, comprises:

i. the transition from the S-ACC-WAIT state to the S-RES-WAIT state, provided by the condition that the local
15 node has sent a control message to request access to the controlled network resource;

ii. the self-transition of the S-RES-WAIT state, provided by the condition that a control message in response to the request for access to the controlled
20 network resource has not been received from the global server after a specified time period, wherein the number of self-transitions performed has not exceeded a specified threshold;

iii. the transition from the S-RES-WAIT state to
25 the S-DISCONN state, provided by the condition that a control message in response to the request for access to the controlled network resource has not been received from the global server after a specified time period,

wherein the number of self-transitions performed has exceeded a specified threshold and the policy is configured to reject the access request as cited in (9) and (10) above;

5 iv. the transition from the S-RES-WAIT state to the S-CONN-LOST state, provided by the condition that a control message in response to the request for access to the controlled network resource has not been received from the global server after a specified time period,
10 wherein the number of self-transitions performed has exceeded a specified threshold and the policy is configured to accept the access request as cited in (9) and (10) above;

 v. the transition from the S-RES-WAIT state to the
15 S-CONN state, provided by the condition that the global server has sent a control message to accept the request for access to the controlled network resource, wherein during the said transition, a control message is sent to the local node indicating that the request for access
20 to the controlled network resource is accepted;

 vi. the transition from the S-RES-WAIT state to the S-DISCONN state, provided by the condition that the global server has sent a control message to accept the rejection of access to the controlled network resource, wherein
25 during the said transition, a control message is sent to the local node indicating that the request for access to the controlled network resource is rejected;

 vii. the transition from the S-CONN state to the

S-DISCONN state, provided by the condition that a packet has not been received from the local node after a specified time period, wherein the number of self-transitions performed has exceeded a specified threshold;

5 viii. the transition from the S-CONN state to the S-DISCONN state, provided by the condition that a control message is received from the local node to indicate the release of the controlled network resources, wherein during the said transition, a control message is sent
10 to the local node to acknowledge the release of the controlled network resources;

 ix. the transition from the S-CONN-LOST state to the S-DISCONN state, provided by the condition that a control message is received from the local node to indicate
15 the release of the controlled network resources, wherein during the said transition, a control message is sent to the local node to acknowledge the release of the controlled network resources;

 x. the transition from the S-CONN-LOST state to the
20 S-RESET-WAIT state, provided by the condition that the connection to the global server is determined to have been regained;

 xi. the self-transition of the S-RESET-WAIT state, provided by the condition that a packet sent from the
25 local node has not been received after a specified time period, wherein the number of self-transitions performed has not exceeded a specified threshold;

 xii. the transition from the S-RESET-WAIT state to

the S-DISCONN state, provided by the condition that a packet sent from the local node has not been received after a specified time period, wherein the number of self-transitions performed has exceeded a specified
5 threshold;

xiii. the transition from the S-RESET-WAIT state to the S-DISCONN state, provided by the condition that a control message is received from the local node to indicate the release of the controlled network resources,
10 wherein during the said transition, a control message is sent to the local node to acknowledge the release of the controlled network resources; and

xiv. the transition from the S-RESET-WAIT state to the S-ACC-WAIT state, provided by the condition that a
15 packet is received from the local node, whereas the said packet is not a control message to indicate the release of the controlled network resources.

(13) The state machine of the network access control framework apparatus, as cited in (1) above, utilizes the
20 set of states cited in (11) above and the set of transitions between the said states cited in (12) above, to control the operation of the said network access control framework apparatus.

(14) The set of states, as cited in (11) above, used
25 in the state machine that controls the operation of the network access control framework apparatus, as cited in (1) above, further comprises:

i. an S-INIT state, wherein a structure with the

data format specified in (8) above is initialized, wherein the said structure is associated with the local node initiating the said state machine;

ii. an S-ACC-WAIT state, wherein a control message
5 is sent to the local node indicating that an access request is required, and the said state machine is waiting for an access request message to be sent by the local node;

iii. an S-RES-WAIT state, wherein a control message
10 is sent to the global server indicating that an access request is made, and the said state machine is waiting for a response to be sent by the global server;

iv. an S-AUTH-WAIT state, wherein a control message
15 is sent to the local node indicating that authentication information is required, and the said state machine is waiting for an authentication response message to be sent by the local node;

v. an S-CONN state, wherein access to the requested network resources is granted to the local node;

vi. an S-LOGOFF state, wherein a control message
20 is sent to the global server indicating the release of requested network resources, and the said state machine is waiting for an acknowledgement message to be sent by the global server;

vii. an S-DISCONN state, wherein the access to all
25 network resources by the local node is released, and the structure with the data format specified in (8) above that is associated with the local node is deleted;

viii. an S-CONN-LOST state, wherein the said state

machine determines that connection to the global server is lost, and the policy specified in (9) above is set to allow access temporarily when connection to the global server is lost; and

- 5 ix. an S-RESET-WAIT state, wherein the said state machine determines that connection to the global server is regained, whereas the prior state is the S-CONN-LOST state.

10 (15) The set of transitions between the states cited in (14) above, wherein these transitions are used in the state machine that controls the operation of the network access control framework apparatus, as cited in (1) above, comprises:

- 15 i. the transition from the S-INIT state to the S-ACC-WAIT state, provided by the condition that the local node has not sent a control message to request access to the controlled network resource;

- 20 ii. the transition from the S-INIT state to the S-RES-WAIT state, provided by the condition that the local node has sent a control message to request access to the network resource;

- 25 iii. the self-transition of the S-ACC-WAIT state, provided by the condition that a control message to request access to the controlled network resource has not been received from the local node after a specified time period, wherein the number of self-transitions performed has not exceeded a specified threshold;

- iv. the transition from the S-ACC-WAIT state to the

S-DISCONN state, provided by the condition that a control message to request access to the controlled network resource has not been received from the local node after a specified time period, wherein the number of self-transitions performed has exceeded a specified threshold;

v. the transition from the S-ACC-WAIT state to the S-RES-WAIT state, provided by the condition that the local node has sent a control message to request access to the controlled network resource;

vi. the self-transition of the S-RES-WAIT state, provided by the condition that a control message in response to the request for access to the controlled network resource has not been received from the global server after a specified time period, wherein the number of self-transitions performed has not exceeded a specified threshold;

vii. the transition from the S-RES-WAIT state to the S-DISCONN state, provided by the condition that a control message in response to the request for access to the controlled network resource has not been received from the global server after a specified time period, wherein the number of self-transitions performed has exceeded a specified threshold and the policy is configured to reject the access request as cited in (9) and (10) above;

viii. the transition from the S-RES-WAIT state to the S-CONN-LOST state, provided by the condition that

a control message in response to the request for access to the controlled network resource has not been received from the global server after a specified time period, wherein the number of self-transitions performed has
5 exceeded a specified threshold and the policy is configured to accept the access request as cited in (9) and (10) above;

ix. the transition from the S-RES-WAIT state to the S-CONN state, provided by the condition that the global
10 server has sent a control message to accept the request for access to the controlled network resource, wherein during the said transition, a control message is sent to the local node indicating that the request for access to the controlled network resource is accepted;

15 x. the transition from the S-RES-WAIT state to the S-DISCONN state, provided by the condition that the global server has sent a control message to accept the rejection of access to the controlled network resource, wherein during the said transition, a control message is sent
20 to the local node indicating that the request for access to the controlled network resource is rejected;

xi. the transition from the S-RES-WAIT state to the S-AUTH-WAIT state, provided by the condition that the global server has sent a control message to request
25 authentication information from the local node;

xii. the self-transition of the S-AUTH-WAIT state, provided by the condition that a control message in response to the request for authentication information

has not been received from the local node after a specified time period, wherein the number of self-transitions performed has not exceeded a specified threshold;

xiii. the transition from the S-AUTH-WAIT state to
5 the S-LOGOFF state, provided by the condition that a control message in response to the request for authentication information has not been received from the local node after a specified time period, wherein the number of self-transitions performed has exceeded
10 a specified threshold;

xiv. the transition from the S-RES-WAIT state to the S-AUTH-WAIT state, provided by the condition that the global server has sent a control message to request authentication information from the local node;

15 xv. the self-transition of the S-CONN state, provided by the condition that a packet has not been received from the local node after a specified time period, wherein the number of self-transitions performed has not exceeded a specified threshold;

20 xvi. the transition from the S-CONN state to the S-LOGOFF state, provided by the condition that a packet has not been received from the local node after a specified time period, wherein the number of self-transitions performed has exceeded a specified threshold;

25 xvii. the self-transition of the S-CONN state, provided by the condition that a packet has been received from the local node, wherein the packet is not a control message to indicate the release of the controlled network

resources;

xviii. the transition from the S-CONN state to the S-LOGOFF state, provided by the condition that a control message is received from the local node to indicate the release of the controlled network resources, wherein
5 during the said transition, a control message is sent to the local node to acknowledge the release of the controlled network resources;

xix. the self-transition of the S-LOGOFF state,
10 provided by the condition that an acknowledgement of the release of the controlled network resources has not been received from the global server after a specified time period, wherein the number of self-transitions performed has not exceeded a specified threshold;

15 xx. the transition from the S-LOGOFF state to the S-DISCONN state, provided by the condition that an acknowledgement of the release of the controlled network resources has not been received from the global server after a specified time period, wherein the number of
20 self-transitions performed has exceeded a specified threshold;

xxi. the transition from the S-LOGOFF state to the S-DISCONN state, provided by the condition that an acknowledgement of the release of the controlled network
25 resources has been received from the global server;

xxii. the transition from the S-CONN-LOST state to the S-DISCONN state, provided by the condition that a control message is received from the local node to indicate

the release of the controlled network resources, wherein during the said transition, a control message is sent to the local node to acknowledge the release of the controlled network resources;

5 xxiii. the transition from the S-CONN-LOST state to the S-RESET-WAIT state, provided by the condition that the connection to the global server is determined to have been regained;

 xxiv. the self-transition of the S-RESET-WAIT state,
10 provided by the condition that a packet sent from the local node has not been received after a specified time period, wherein the number of self-transitions performed has not exceeded a specified threshold;

 xxv. the transition from the S-RESET-WAIT state to
15 the S-DISCONN state, provided by the condition that a packet sent from the local node has not been received after a specified time period, wherein the number of self-transitions performed has exceeded a specified threshold;

20 xxvi. the transition from the S-RESET-WAIT state to the S-LOGOFF state, provided by the condition that a control message is received from the local node to indicate the release of the controlled network resources, wherein during the said transition, a control message
25 is sent to the local node to acknowledge the release of the controlled network resources; and

 xxvii. the transition from the S-RESET-WAIT state to the S-ACC-WAIT state, provided by the condition that

a packet is received from the local node, whereas the said packet is not a control message to indicate the release of the controlled network resources.

(16) The state machine of the network access control framework apparatus, as cited in (1) above, utilizes the set of states cited in (14) above and the set of transitions between the said states cited in (15) above, to control the operation of the said network access control framework apparatus.

(17) The set of states, as cited in (11) above, used in the state machine that controls the operation of the network access control framework apparatus, as cited in (1) above, further comprises:

i. an S-INIT state, wherein a structure with the data format specified in (8) above is initialized, wherein the said structure is associated with the local node initiating the said state machine;

ii. an S-ACC-WAIT state, wherein a control message is sent to the local node indicating that an access request is required, and the said state machine is waiting for an access request message to be sent by the local node;

iii. an S-RES-WAIT state, wherein a control message is sent to the global server indicating that an access request is made, and the said state machine is waiting for a response to be sent by the global server;

iv. an S-AUTH-WAIT state, wherein a control message is sent to the local node indicating that authentication information is required, and the said state machine is

waiting for an authentication response message to be sent by the local node;

v. an S-CONN state, wherein access to the requested network resources is granted to the local node;

5 vi. an S-DISCONN state, wherein the access to all network resources by the local node is released, and the structure with the data format specified in (8) above that is associated with the local node is deleted;

vii. an S-CONN-LOST state, wherein the said state
10 machine determines that connection to the global server is lost, and the policy specified in (9) above is set to allow access temporarily when connection to the global server is lost; and

viii. an S-RESET-WAIT state, wherein the said state
15 machine determines that connection to the global server is regained, whereas the prior state is the S-CONN-LOST state.

(18) The set of transitions between the states cited in (17) above, wherein these transitions are used in the
20 state machine that controls the operation of the network access control framework apparatus, as cited in (1) above, comprises:

i. the transition from the S-INIT state to the S-ACC-WAIT state, provided by the condition that the local
25 node has not sent a control message to request access to the controlled network resource;

ii. the transition from the S-INIT state to the S-RES-WAIT state, provided by the condition that the local

node has sent a control message to request access to the network resource;

iii. the self-transition of the S-ACC-WAIT state, provided by the condition that a control message to request
5 access to the controlled network resource has not been received from the local node after a specified time period, wherein the number of self-transitions performed has not exceeded a specified threshold;

iv. the transition from the S-ACC-WAIT state to the
10 S-DISCONN state, provided by the condition that a control message to request access to the controlled network resource has not been received from the local node after a specified time period, wherein the number of self-transitions performed has exceeded a specified
15 threshold;

v. the transition from the S-ACC-WAIT state to the S-RES-WAIT state, provided by the condition that the local node has sent a control message to request access to the controlled network resource;

20 vi. the self-transition of the S-RES-WAIT state, provided by the condition that a control message in response to the request for access to the controlled network resource has not been received from the global server after a specified time period, wherein the number
25 of self-transitions performed has not exceeded a specified threshold;

vii. the transition from the S-RES-WAIT state to the S-DISCONN state, provided by the condition that a

control message in response to the request for access to the controlled network resource has not been received from the global server after a specified time period, wherein the number of self-transitions performed has exceeded a specified threshold and the policy is configured to reject the access request as cited in (9) and (10) above;

viii. the transition from the S-RES-WAIT state to the S-CONN-LOST state, provided by the condition that a control message in response to the request for access to the controlled network resource has not been received from the global server after a specified time period, wherein the number of self-transitions performed has exceeded a specified threshold and the policy is configured to accept the access request as cited in (9) and (10) above;

ix. the transition from the S-RES-WAIT state to the S-CONN state, provided by the condition that the global server has sent a control message to accept the request for access to the controlled network resource, wherein during the said transition, a control message is sent to the local node indicating that the request for access to the controlled network resource is accepted;

x. the transition from the S-RES-WAIT state to the S-DISCONN state, provided by the condition that the global server has sent a control message to accept the rejection of access to the controlled network resource, wherein during the said transition, a control message is sent

to the local node indicating that the request for access to the controlled network resource is rejected;

xi. the transition from the S-RES-WAIT state to the S-AUTH-WAIT state, provided by the condition that the
5 global server has sent a control message to request authentication information from the local node;

xii. the self-transition of the S-AUTH-WAIT state, provided by the condition that a control message in response to the request for authentication information
10 has not been received from the local node after a specified time period, wherein the number of self-transitions performed has not exceeded a specified threshold;

xiii. the transition from the S-AUTH-WAIT state to the S-DISCONN state, provided by the condition that a
15 control message in response to the request for authentication information has not been received from the local node after a specified time period, wherein the number of self-transitions performed has exceeded a specified threshold;

20 xiv. the transition from the S-RES-WAIT state to the S-AUTH-WAIT state, provided by the condition that the global server has sent a control message to request authentication information from the local node;

xv. the self-transition of the S-CONN state,
25 provided by the condition that a packet has not been received from the local node after a specified time period, wherein the number of self-transitions performed has not exceeded a specified threshold;

xvi. the transition from the S-CONN state to the S-DISCONN state, provided by the condition that a packet has not been received from the local node after a specified time period, wherein the number of self-transitions performed has exceeded a specified threshold, wherein
5 during the said transition, a control message is sent to the global server to indicate the release of the access to the controlled network resources;

xvii. the self-transition of the S-CONN state,
10 provided by the condition that a packet has been received from the local node, wherein the packet is not a control message to indicate the release of the controlled network resources;

xviii. the transition from the S-CONN state to the
15 S-DISCONN state, provided by the condition that a control message is received from the local node to indicate the release of the controlled network resources, wherein during the said transition, a control message is sent to the global server indicating the release of the access
20 to the controlled network resources;

xix. the transition from the S-CONN-LOST state to the S-DISCONN state, provided by the condition that a control message is received from the local node to indicate the release of the controlled network resources;

25 xx. the transition from the S-CONN-LOST state to the S-RESET-WAIT state, provided by the condition that the connection to the global server is determined to have been regained;

xxi. the self-transition of the S-RESET-WAIT state, provided by the condition that a packet sent from the local node has not been received after a specified time period, wherein the number of self-transitions performed
5 has not exceeded a specified threshold;

xxii. the transition from the S-RESET-WAIT state to the S-DISCONN state, provided by the condition that a packet sent from the local node has not been received after a specified time period, wherein the number of
10 self-transitions performed has exceeded a specified threshold;

xxiii. the transition from the S-RESET-WAIT state to the S-DISCONN state, provided by the condition that a control message is received from the local node to
15 indicate the release of the controlled network resources, wherein during the said transition, a control message is sent to the global server indicating the release of the access to the controlled network resources; and

xxiv. the transition from the S-RESET-WAIT state
20 to the S-ACC-WAIT state, provided by the condition that a packet is received from the local node, whereas the said packet is not a control message to indicate the release of the controlled network resources.

(19) The state machine of the network access control
25 framework apparatus, as cited in (1) above, utilizes the set of states cited in (17) above and the set of transitions between the said states cited in (18) above, to control the operation of the said network access control framework

apparatus.

(20) The method used in the network access control framework apparatus as cited in (1) above, to generalize the set of states as cited in (14) above and the set of transitions between the said states cited in (15) above, to the set of states as cited in (17) above and the set of transitions between the said states cited in (18) above, comprises the steps of:

i. configuring the parameters of the said network access control framework apparatus such that for the self-transition of the S-LOGOFF state, provided by the condition that an acknowledgement of the release of the controlled network resources has not been received from the global server after a specified time period, wherein the number of self-transitions performed has not exceeded a specified threshold, the said specified time period is so small a value that it is negligible with respect to the processing cycle of the said network access control framework apparatus, and the said specified threshold is set to a value of zero so that no self-transition can occur; and

ii. configuring the parameters of the said network access control framework apparatus such that for the transition from the S-LOGOFF state to the S-DISCONN state, provided by the condition that an acknowledgement of the release of the controlled network resources has not been received from the global server after a specified time period, wherein the number of self-transitions performed

has exceeded a specified threshold, the said specified time period is so small a value that it is negligible with respect to the processing cycle of the said network access control framework apparatus, and the said
5 specified threshold is set to a value of zero so that a transition to the S-DISCONN state must occur when the said specified time period elapses.

(21) The state machine of the network access control framework apparatus, as cited in (1) above, utilizes the
10 set of states cited in (14) above, the set of transitions between the said states cited in (15) above, and the method cited in (20) above to generalize the set of states cited in (14) above to the set of states cited in (17) above, and the set of transitions between the said states cited
15 in (15) above to the set of transitions between the said states cited in (18) above, to control the operation of the said network access control framework apparatus.

(22) The method used in the network access control framework apparatus as cited in (1) above, to process
20 a data packet sent by a local node, comprises the steps of:

i. searching for a structure with the data format as cited in (8) above that is associated with the local node, and if not found, instantiating a new instance of
25 the state machine as cited in (1) above to process the said packet;

ii. when the said structure is found, having the said packet processed by the state machine as cited in

(1) above if it contains a control message that corresponds to one of the generic control messages cited in (2) and (3) above;

iii. when the said packet does not contain any
5 control messages that correspond to one of the generic control messages cited in cited in (2) and (3) above, and the state of the state machine as cited in (1) above is the state in which access to the controlled network resources is granted, forwarding the said packet to its
10 intended recipient;

iv. when the said packet does not contain any control messages that correspond to one of the generic control messages cited in (2) and (3) above, and the state of the state machine as cited in (1) above is not the state
15 in which access to the global server is determined to be lost, nor the state in which access to the controlled network resources is granted, queuing the said packet in the said structure associated with the local node;

v. when the said packet does not contain any control
20 messages that correspond to one of the generic control messages cited in (2) and (3) above, and the state of the state machine as cited in (1) above is the state in which access to the global server is determined to be lost, and the policy as cited in (9) above is configured
25 to accept access requests, and the intended recipient of the said packet is in a data communications network that is controlled by the said network access control framework apparatus, forwarding the said packet to its

intended recipient; and

vi. when the said packet does not contain any control messages that correspond to one of the generic control messages cited in (2) and (3) above, and the state of
5 the state machine as cited in (1) above is the state in which access to the global server is determined to be lost, and the policy as cited in (9) above is configured to accept access requests, and the intended recipient of the said packet is in a data communications network
10 that is not controlled by the said network access control framework apparatus, queuing the said packet in the said structure associated with the local node.

(23) The network access control framework apparatus, as cited in (1) above utilizes the method cited in (22)
15 above to process data packets that are sent by a local node.

(24) The mechanism utilized in the network access control framework apparatus, as cited in (1) above, wherein the said mechanism allows the network access
20 control framework to temporarily store packets sent by a local node intended for some other node when the said local node has not yet been granted access to the controlled network resources, comprises the step of, when the said packet does not contain any control messages that
25 correspond to one of the generic control messages cited in (2) and (3) above, and the state of the state machine as cited in (1) above is not the state in which access to the global server is determined to be lost, nor the

state in which access to the controlled network resources is granted, queuing the said packet in a structure with the data format cited in (8) above, wherein the said structure is associated with the local node.

5 (25) The network access control framework apparatus, as cited in (1) above, wherein the said network access control framework utilizes the mechanism cited in (24) above to temporarily store packets sent by a local node intended for some other node when the said local node
10 has not yet been granted access to the controlled network resources, comprises the step of, when the said packet does not contain any control messages that correspond to one of the generic control messages cited in (2) and (3) above, and the state of the state machine as cited
15 in (1) above is not the state in which access to the global server is determined to be lost, nor the state in which access to the controlled network resources is granted, queuing the said packet in a structure with the data format cited in (8) above, wherein the said structure is
20 associated with the local node.

 (26) The mechanism utilized in the network access control framework apparatus as cited in (1) above, wherein the said mechanism allows the network access control framework to temporarily store packets sent by a local
25 node when the connection to the said local node has not yet been granted access to the controlled network resources by the global server cited in (1) above, wherein the said data packet is intended for some other node in

a data communications network that is not controlled by the said network access control framework apparatus, comprises the step of, when the said packet does not contain any control messages that correspond to one of the generic control messages cited in (2) and (3) above, and the state of the state machine as cited in (1) above is the state in which access to the global server is determined to be lost, and the policy as cited in (9) above is configured to accept access requests, and the intended recipient of the said packet is in a data communications network that is not controlled by the said network access control framework apparatus, queuing the said packet in the said structure associated with the local node.

(27) The network access control framework apparatus as cited in (1) above, wherein the said network access control framework apparatus utilizes the mechanism cited in (26) above to temporarily store packets sent by a local node when the connection to the said local node has not yet been granted access to the controlled network resources by the global server cited in (1) above, wherein the said data packet is intended for some other node in a data communications network that is not controlled by the said network access control framework apparatus, comprises the step of, when the said packet does not contain any control messages that correspond to one of the generic control messages cited in (2) and (3) above, and the state of the state machine as cited in (1) above is the state in which access to the global server is determined to

be lost, and the policy as cited in (9) above is configured to accept access requests, and the intended recipient of the said packet is in a data communications network that is not controlled by the said network access control
5 framework apparatus, queuing the said packet in the said structure associated with the local node.

This application is based on Japanese Patent Application No.2002-276195 filed on September 20, 2002, the entire content of which is expressly incorporated
10 by reference herein.

Industrial Applicability

The present invention is applicable to access control in an intermediate network element connecting
15 a plurality of data communications networks.

CLAIMS

1. An access control method in an intermediate network element for connecting a plurality of data communication networks including a local network and a global network,
5 comprising the steps of:

determining whether or not a connection from a local node in the local network to a global node in the global network is disconnected; and

accepting an access from the local node to the global
10 node when the connection from the local node to the global node is determined to be disconnected in the step of determining.

2. The access control method according to claim 1,
15 further comprising the step of:

rejecting an access from the local node to the global node when the connection from the local node to the global node is determined to be disconnected in the step of determining,

20 wherein the step of accepting and the step of rejecting are switched according to a course of action of the intermediate network element.

3. The access control method according to claim 1,
25 further comprising the step of:

transmitting a message to the local node which indicates that an access to the global node is accepted when an access from the local node to the global node

is accepted in the step of accepting.

4. The access control method according to claim 2, further comprising the step of:

5 transmitting a message to the local node which indicates that an access to the global node is rejected when an access from the local node to the global node is rejected in the step of rejecting.