EXHIBIT G

US006874090B2

(12) **United States Patent**
See et al.

(10) **Patent No.: US 6,874,090 B2**
(45) **Date of Patent: *Mar. 29, 2005**

(54) **DETERMINISTIC USER AUTHENTICATION SERVICE FOR COMMUNICATION NETWORK**

(75) Inventors: **Michael E. See**, Chapel Hill, NC (US); **John W. Bailey**, Agoura Hills, CA (US); **Charles L. Panza**, Park City, UT (US); **Yuri Pikover**, Malibu, CA (US); **Geoffrey C. Stone**, Malibu, CA (US)

(73) Assignee: **Alcatel**, Paris (FR)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 506 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **09/886,930**

(22) Filed: **Jun. 21, 2001**

(65) **Prior Publication Data**

US 2002/0040441 A1 Apr. 4, 2002

Related U.S. Application Data

(63) Continuation of application No. 09/525,506, filed on Mar. 15, 2000, now Pat. No. 6,339,830, which is a continuation of application No. 08/874,754, filed on Jun. 13, 1997, now Pat. No. 6,070,243.

(51) **Int. Cl.**[7] **G06F 11/30**; G06F 12/14; H04L 9/00; H04L 9/32

(52) **U.S. Cl.** **713/202**; 713/200; 713/201; 713/151; 713/150

(58) **Field of Search** 713/200, 201, 713/151, 155, 168, 202

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,896,319 A 1/1990 Lidinsky et al.
4,922,486 A 5/1990 Lidinsky et al.

(Continued)

OTHER PUBLICATIONS

Estrin, Deborah, et al. "Visa Protocols for Controlling Inter–Organizational Datagram Flow: Extended Description," WRL Research Report 88/5, Western Research Laboratory, The University of Southern California, Dec. 1988, 41 Pages.

Xylan and Checkpoint Develop First Secure Virtual LANs and User Authenticated Virtual LANs; Business Wire, Inc.; Calabasas, California; 4 Pages; Jun. 11, 1996.

Stoneburner, Gary R., et al.; The Boeing MLS LAN: Headed Towards an Infosec Security Solution; Boeing Aerospace and Electronics; pp. 254–265; (Undated).

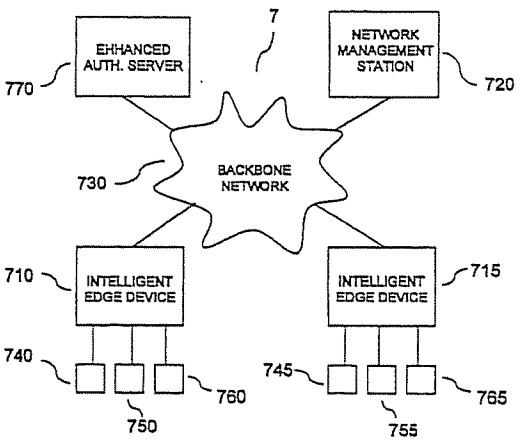
(Continued)

Primary Examiner—Kim Wu
Assistant Examiner—Allen S. Wu
(74) *Attorney, Agent, or Firm*—Scot A. Reader

(57) **ABSTRACT**

A user authentication service for a communication network authenticates local users before granting them access to personalized sets of network resources. Authentication agents on intelligent edge devices present users of associated end systems with log-in challenges. Information supplied by the users is forwarded to an authentication server for verification. If successfully verified, the authentication server returns to the agents authorized connectivity information and time restrictions for the particular authenticated users. The agents use the information to establish rules for filtering and forwarding network traffic originating from or destined for particular authenticated users during authorized time periods. An enhanced authentication server may be engaged if additional security is desired. The authorized connectivity information preferably includes identifiers of one or more virtual local area networks active in the network. Log-in attempts are recorded so that the identity and whereabouts of network users may be monitored from a network management station.

33 Claims, 8 Drawing Sheets



U.S. PATENT DOCUMENTS

4,962,449	A	10/1990	Schlesinger	
5,191,613	A	3/1993	Graziano et al.	
5,249,230	A	9/1993	Mihm, Jr.	
5,272,754	A	12/1993	Boerbert	
5,311,593	A	5/1994	Carmi	
5,343,529	A	8/1994	Goldfine et al.	
5,414,844	A	5/1995	Wang	
5,469,576	A	11/1995	Dauerer et al.	
5,499,297	A	3/1996	Boebert	
5,502,766	A	3/1996	Boebert et al.	
5,564,016	A	10/1996	Korenshtein	
5,657,388	A	8/1997	Weiss	
5,671,354	A	9/1997	Ito et al.	
5,678,004	A	10/1997	Thaweethai	
5,684,951	A	11/1997	Goldman et al.	
5,696,898	A	12/1997	Baker et al.	
5,721,779	A	2/1998	Funk	
5,721,780	A	2/1998	Ensor et al.	
5,761,309	A	6/1998	Ohashi et al.	
5,774,525	A	6/1998	Kanevsky et al.	
5,774,551	A	6/1998	Wu et al.	
5,774,650	A	6/1998	Chapman et al.	
5,778,065	A	7/1998	Hauser et al.	
5,784,566	A	7/1998	Viavant et al.	
5,796,942	A	8/1998	Esbensen	
5,852,714	A	12/1998	Tseng et al.	
5,889,958	A	3/1999	Willens	
5,968,126	A	10/1999	Ekstrom et al.	
6,021,495	A	2/2000	Jain et al.	
6,055,638	A	4/2000	Pascal et al.	
6,061,790	A	5/2000	Bodnar	
6,070,240	A	5/2000	Xydis	
6,070,243	A	5/2000	See et al.	
6,212,191	B1 *	4/2001	Alexander et al.	370/401
6,233,686	B1 *	5/2001	Zenchelsky et al.	713/201
6,311,218	B1	10/2001	Jain et al.	

OTHER PUBLICATIONS

Weiss, Howard; Verdix Secure LAN & Boeing MLS LAN Product Bulletins, Sparta, Inc.; 5 Pages; Sep. 4, 1990.

Microsoft SNA Server; Microsoft Corporation; 6 Pages, 1993.

Microsoft® SNA Server for Windows NT™ Fact Sheet; Microsoft Corporation; 3 Page; 1994.

Microsoft SNA Server Evaluation Guide; Microsoft Corporation; 28 Pages; Jan. 1994.

Cover letter for Microsoft SNA Server Fact Sheet and Evaluation Guide, Microsoft Corporation; 1 Page; (Undated).

Guideline for the Analysis of Local Area Network Security; Federal Information Processing Standards Publication 191; http://www.itl.nist.gov/fipspubs/fip191.htm; 43 Pages, Nov. 9, 1994.

McNealis, Martin; New Cisco IOS VLAN Service Make "Virtual" a Reality; Cisco Systems Software Engineering; pp. 1–5; Jun. 6, 1995.

Blunk, L.J., et al., PPP Extensible Authentication Protrocol (EAP) IETF Internet Draft draft–ietf–pppext–eap–auth–02.txt; http://www.waterspring.org/pub/id/draft–ietf–pppext–eap–auth–02.txt; 20 Pages; Jun. 1996.

Cisco IOS Lock and Key Security; Cisco Systems, Inc., pp. 1–6; 1996.

Cisco Announces Advanced Security Access Control Servers; Cisco Systems, Inc.; http://www.cisco.com/warp/public/146/pressroom/1997/apr97/1853.html; 3 Pages; Apr. 15, 1997.

Passmore, David, et al.; The Virtual LAN Technology Report; Decisys, Inc., 22 Pages; May 1996.

Symantec pcANYWHERE 32 Version 7.5 Packaging; Symantec Corporation; 4 Pages; 1996.

Symantec pcANYWHERE–Creating Scripts; Symantec Corporation, 254 Pages; 1993–1996.

Symantec pcANYWHERE 32 Version 7.5 User's Guide; Symantec Corporation, 261 Pages, 1993–1996.

Ascend Max/Pipeline Software Version 4.6 Dictionary Definitions, 9 Pages, Oct. 18, 1996.

Livingston Enterprises, Inc., "Remote Authetication Dial In User Service (RADIUS) Ascend Definitions," Jul. 25, 1995.

Rigney, C., "RADIUS Accounting," IETF RFC 1035, pp. 1–37, Jan. 1996, http://www.ietf.org/rfc/rfc2059.txt?number=2059.

Rigney, C., et al, "Remote Authentication Dial In User Service (RADIUS)," IETF RFC 2058, Network Working Group Internet, pp. 1–64, Jan. 1997, http://www.ietf.org.rfc/rfcw058.txt?number=2058.

Hamzeh, K., "Ascend Tunnel Management Protocol – ATMP," IETF RFC 2107, Network Working Group Internet, pp. 1–19, Feb. 1997, ftp://ftp.isi.edu/in–notes/rfc2107.txt.

Rigney, C., et al., "Remote Authentication Dial In User Service (RADIUS)," IETF RFC 2138, pp. 1–65, Apr. 1997, http://www.ietf.org/rfc/rfc2138.txt?number–2138.

Rigney, C., "RADIUS Accounting," IETF RFC 2139, pp. 1–37, Apr. 1997, http://www.ietf.org/rfc/rfc2139.txt?number=2139.

Claassen et al., "Secure Communication Procedure For ISDN," IEEE Trans. on Computers, pp. 165–170, Jun. 1998.

Benhanmou, Eric, "Integrating Bridges and Routers in a Large Internetwork," IEEE Network, pp. 65–71, Jan. 1998.

Weaver, et al., "A Real–Time Monitor for Token Ring Networks," IEEE Trans. on Computers, pp. 0784–0798, May 1989.

Karri, Ramesh, "A Security Imbedded Authentication Protocol," IEEE Trans. on Computers, pp. 1105–1109, Jun. 1988.

Cole, et al., "An Architecture for a Mobil OSI Mail Access System," IEEE Journal on Selected Areas in Communications, vol. 7, No. 2, pp. 249–256, Feb. 1989.

Nakeo, et al., "Proposal on a Secure Communications Service Element in the OSI Application Layer," IEEE Journal on Selected Areas on Communications, vol. 7, No. 4, pp. 505–516, May 1989.

Ciminiera, et al., "Authentication Mechanism in Microprocessor–Based Local Area Networks," IEEE Trans. on Software Engineering, Col. 15, No. 5, pp. 654–658, May 1989.

Lu, et al., "Secure Communication in Internet Environments: A Hierarchical Key Management Scheme for end–to–end Encryption," IEEE Trans. on Communications, vol. 37, No. 10, pp. 1014–1023, Oct. 1989.

Lloyd, B., et al., "PPP Authentication Protocols," Network Working Group, http://www.ietf.org/rfc/rfc1334.txt?number=1334, pp. 1–16, Oct. 1992.

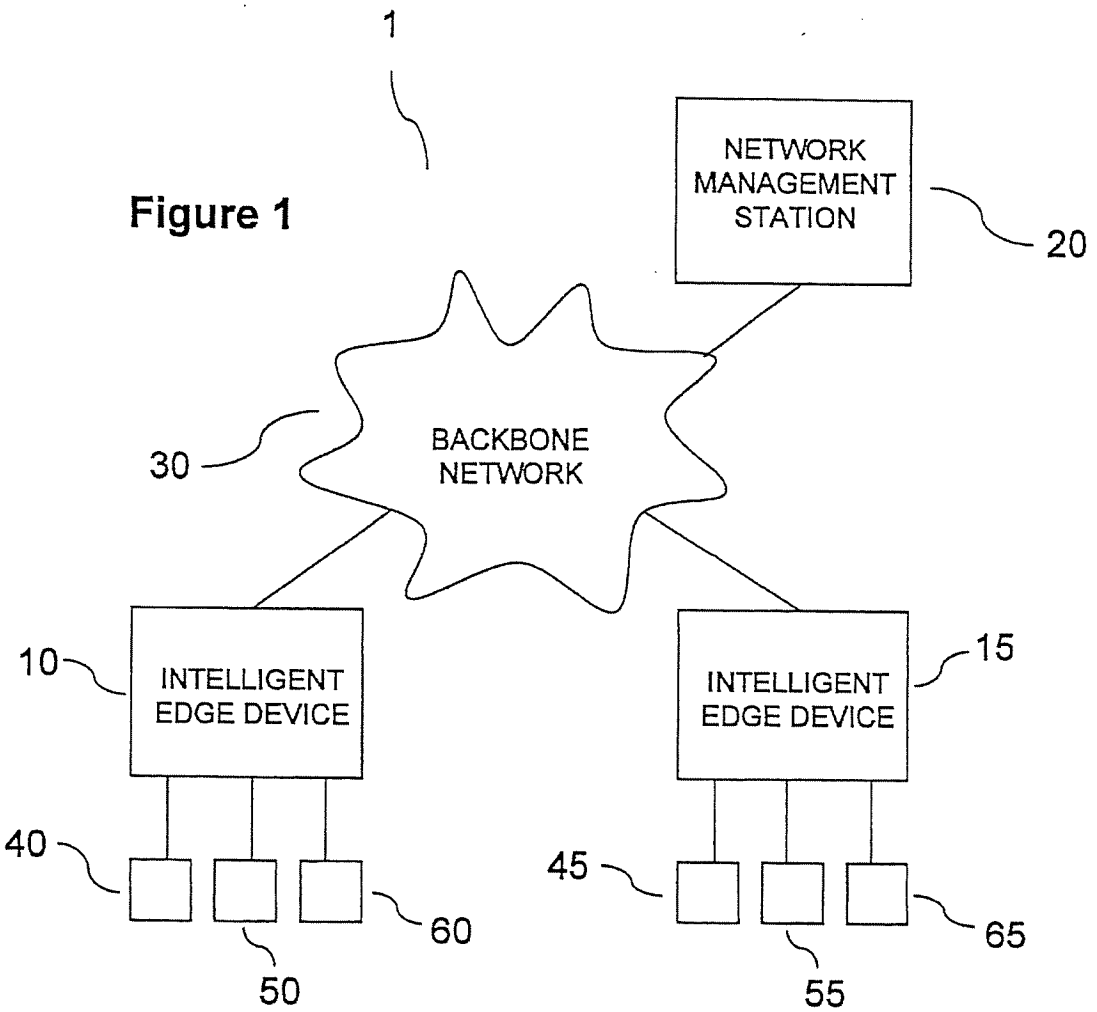
Haller, N., "The S/Key One–Time Password System," Network Working Group, http://www.ietf.org/rfc/rfc1760.txt?number=1760, pp. 1–12, Feb. 1995.

Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP),", Network Working Group, http://www.ietf.org/rfc/rfc1994.txt?number=1994, pp. 1–12, Aug. 1996.

Blunk, L.J., et al., "PPP Extensible Authentication Protocol (EAP)," Network Working Group, http://www.waterspring-s.org/pub/id/draft-ietf-pppext-eap-auth-02.txt, pp. 1–18, Jun. 1996.

* cited by examiner

Figure 1


1
NETWORK MANAGEMENT STATION
20
BACKBONE NETWORK
30
INTELLIGENT EDGE DEVICE
10
INTELLIGENT EDGE DEVICE
15
40
45
60
65
50
55

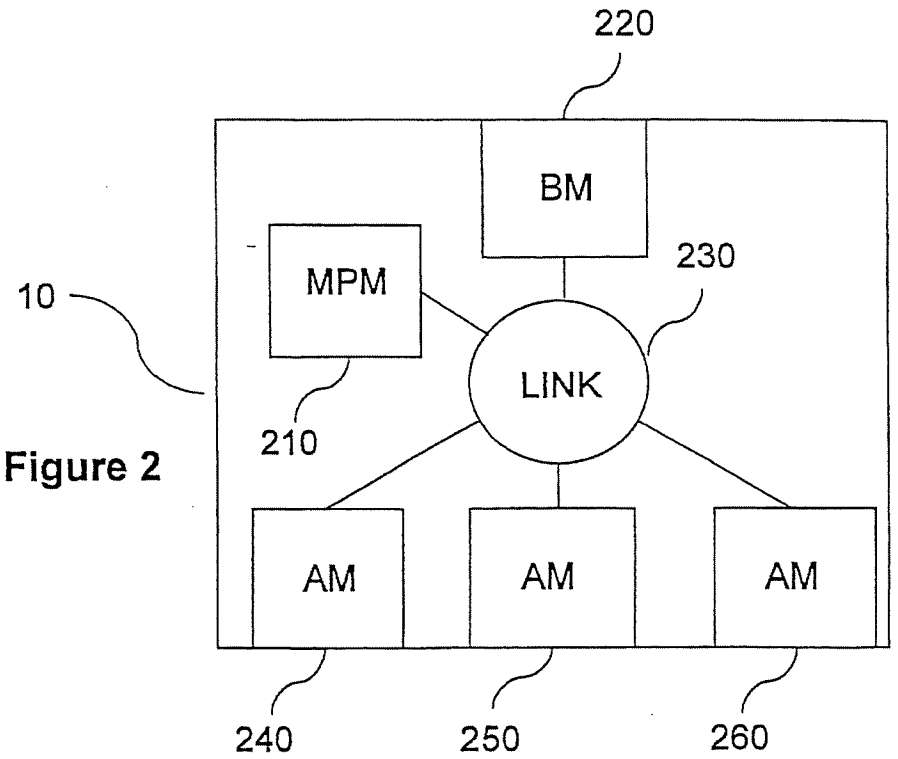


Figure 2

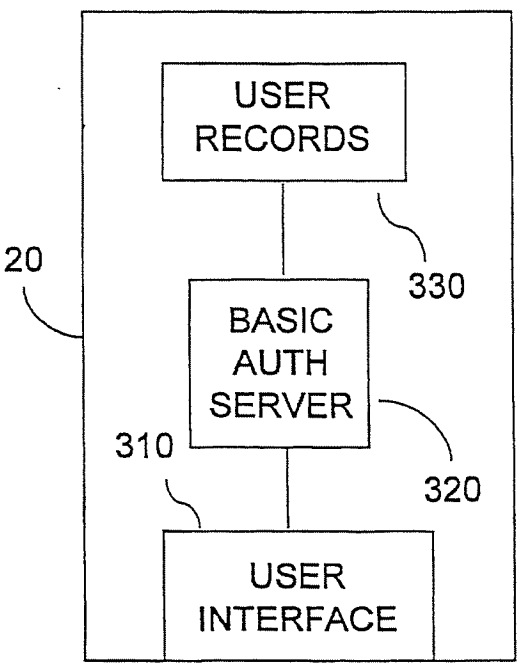


Figure 3A

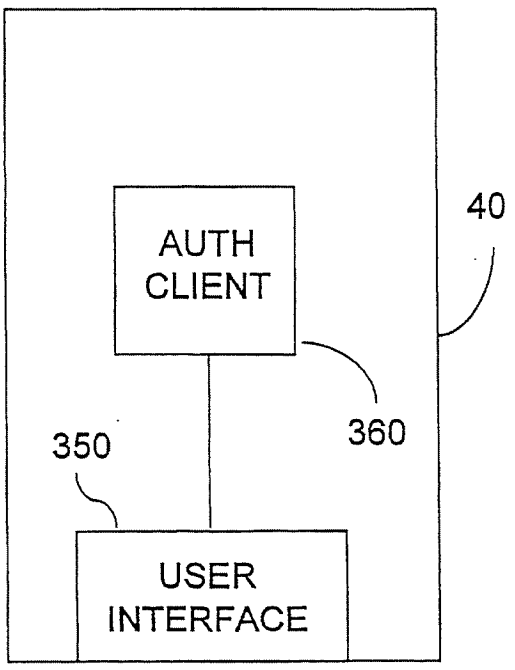


Figure 3B

Figure 4

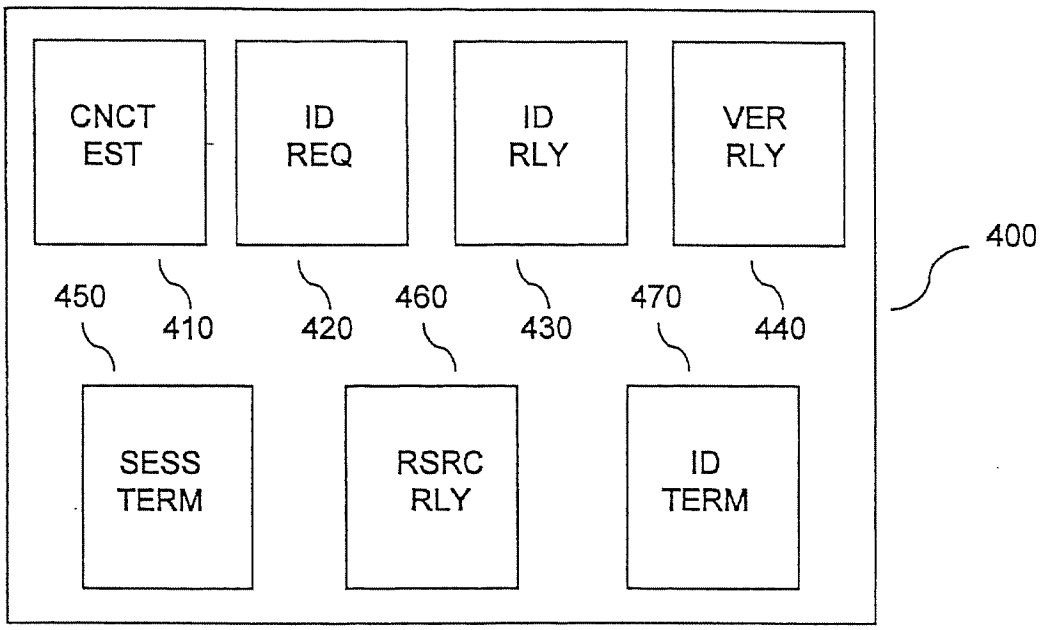
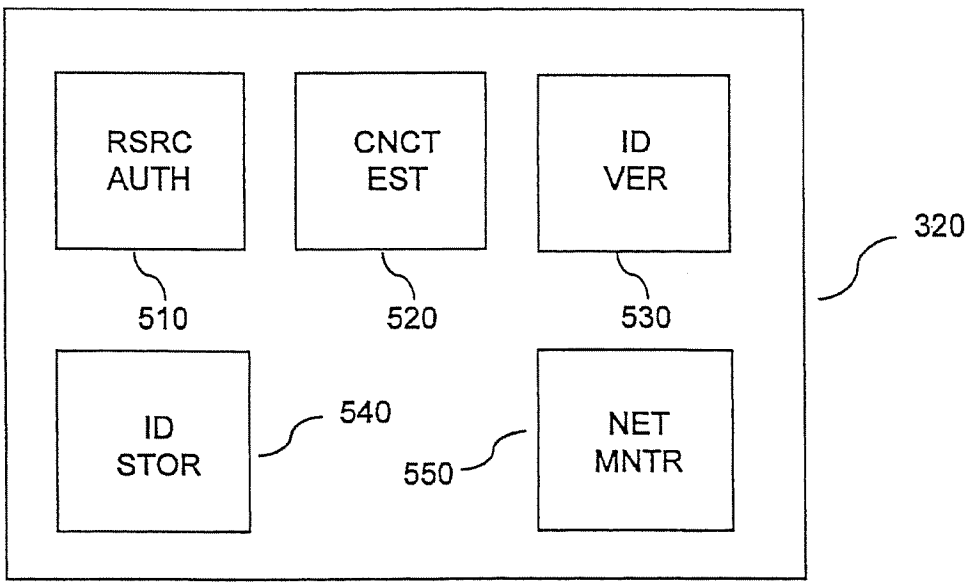


Figure 5



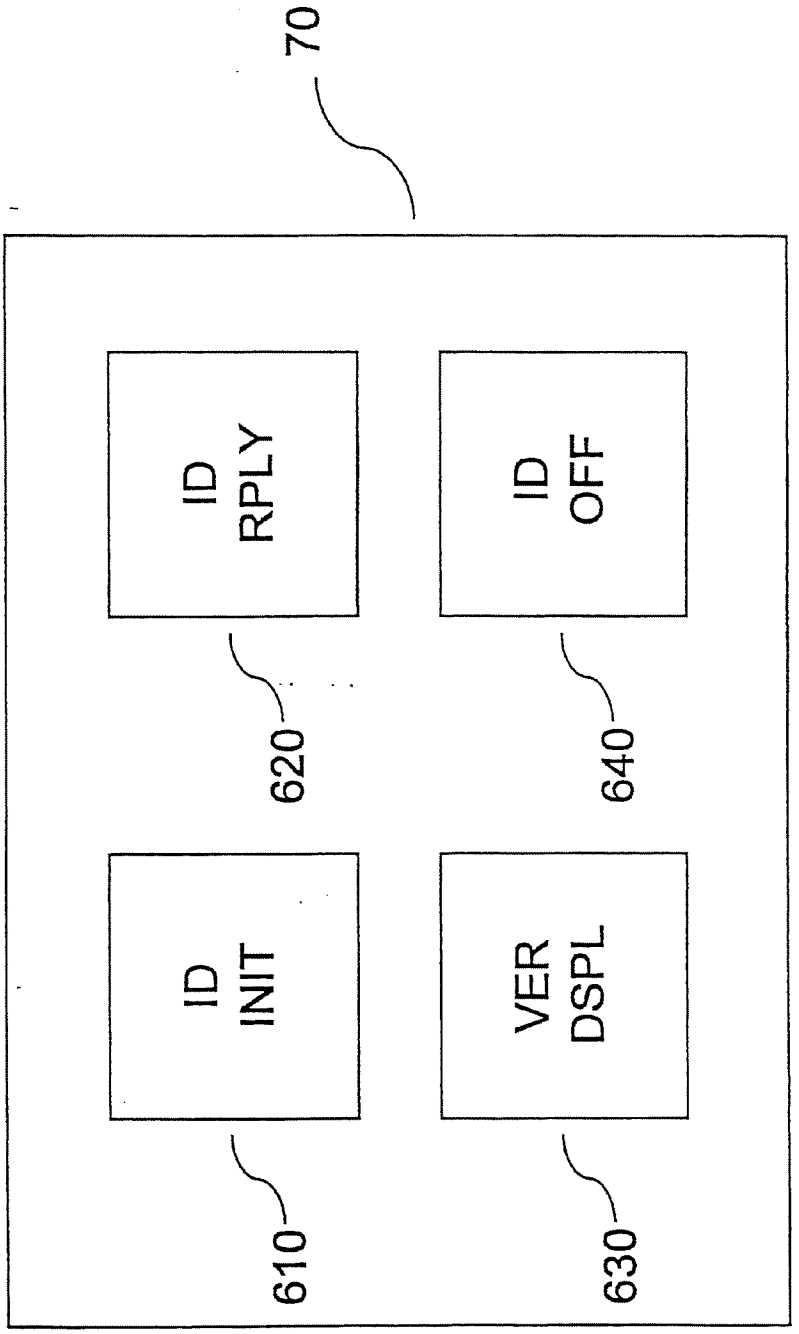


Figure 6

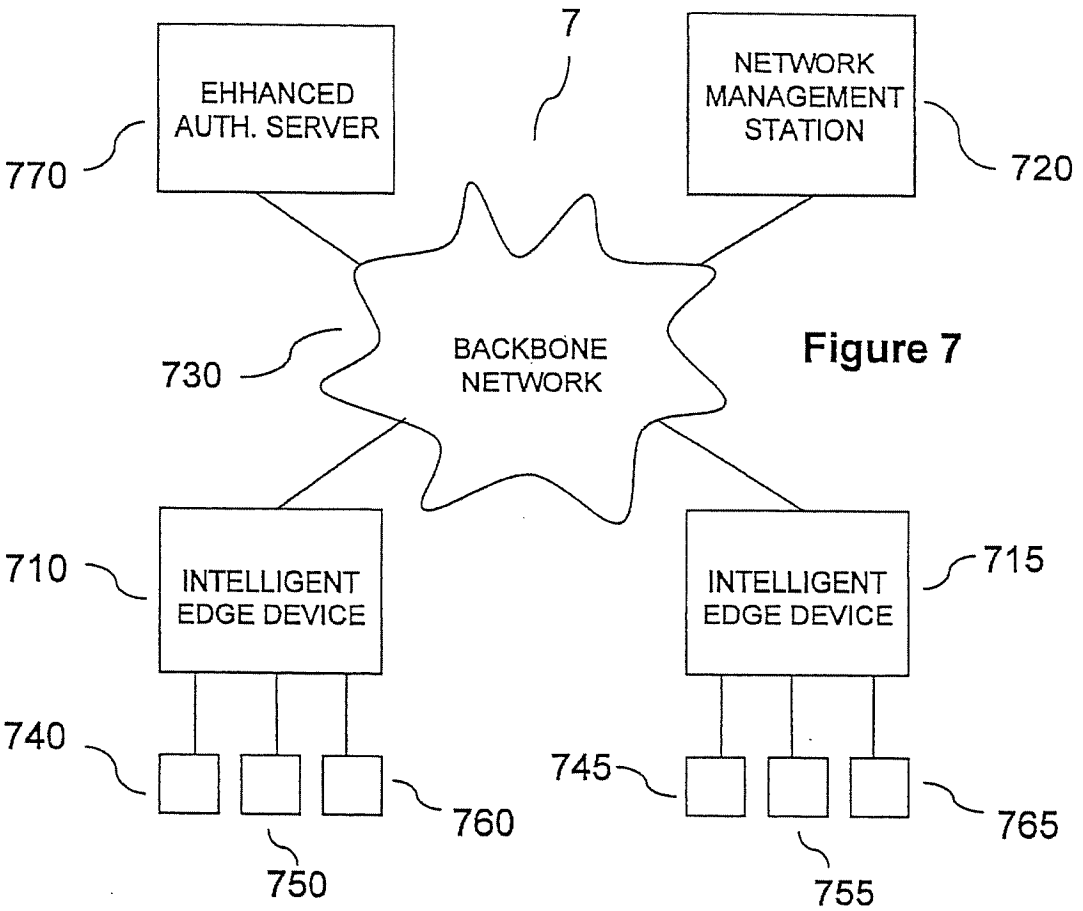

7
EHHANCED AUTH. SERVER
770
NETWORK MANAGEMENT STATION
720
BACKBONE NETWORK
730
INTELLIGENT EDGE DEVICE
710
INTELLIGENT EDGE DEVICE
715
740
760
750
745
765
755

Figure 7

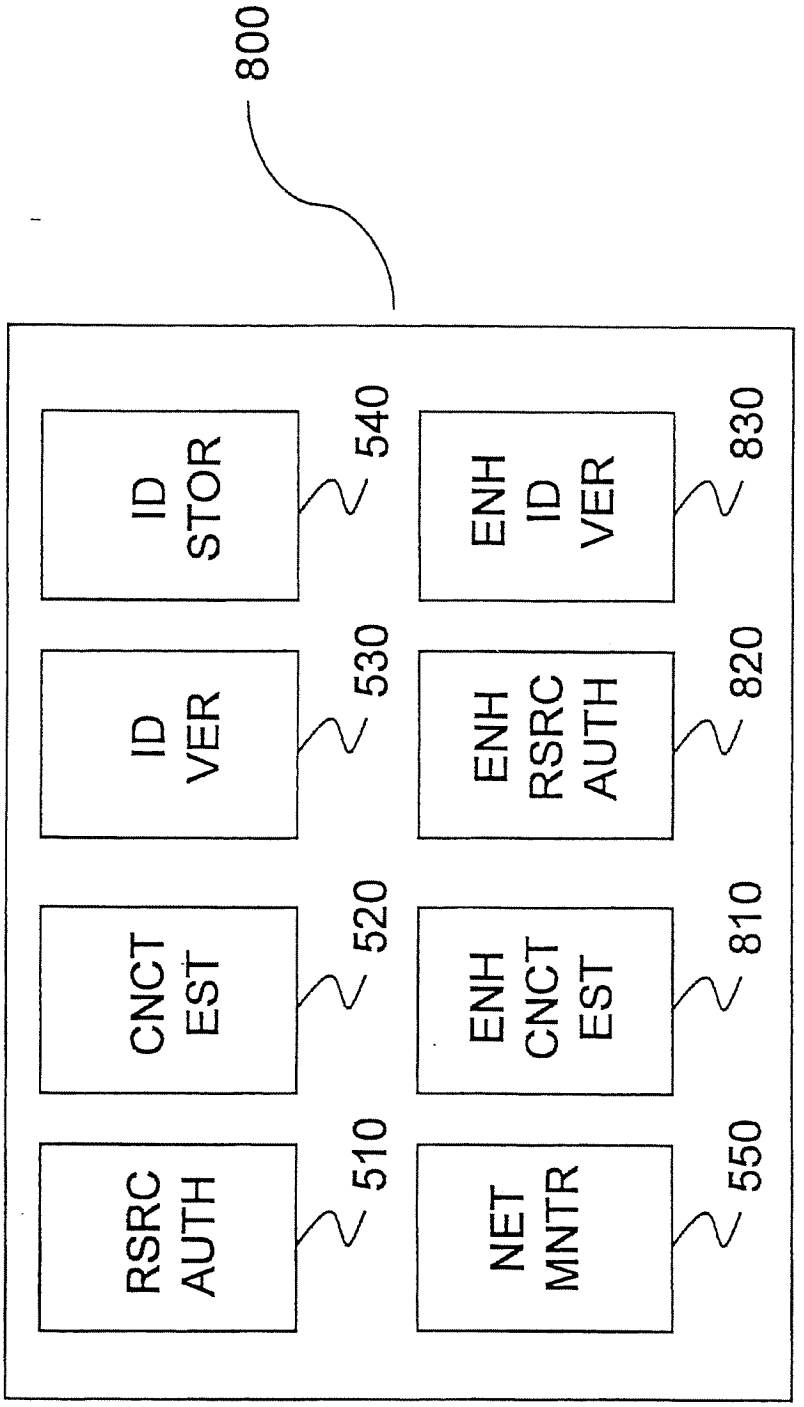

800
RSRC AUTH
510
CNCT EST
520
ID VER
530
ID STOR
540
NET MNTR
550
ENH CNCT EST
810
ENH RSRC AUTH
820
ENH ID VER
830

Figure 8

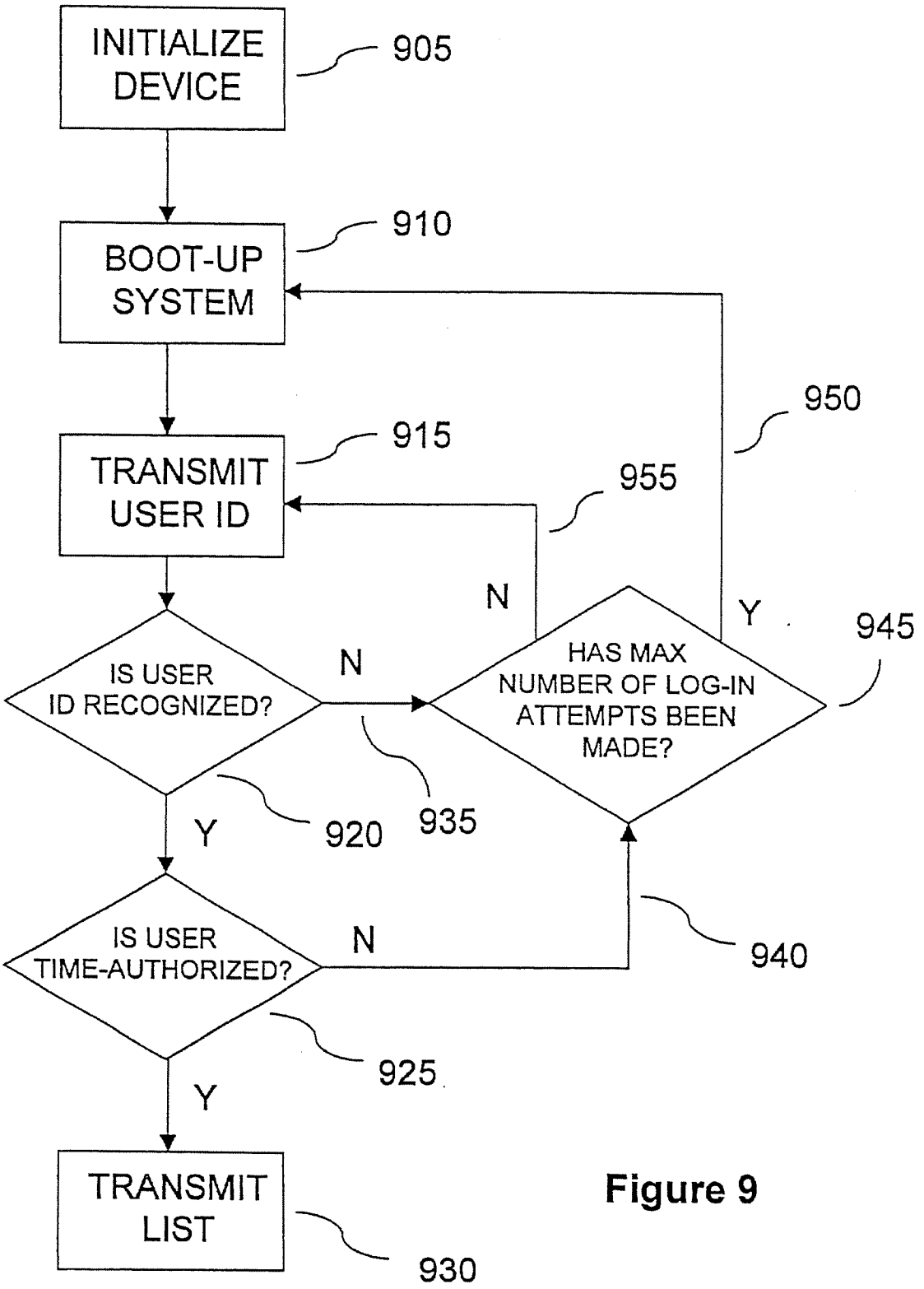

INITIALIZE DEVICE
905
BOOT-UP SYSTEM
910
TRANSMIT USER ID
915
IS USER ID RECOGNIZED?
N
HAS MAX NUMBER OF LOG-IN ATTEMPTS BEEN MADE?
Y
945
950
955
935
Y
920
IS USER TIME-AUTHORIZED?
N
940
925
Y
TRANSMIT LIST
930

Figure 9

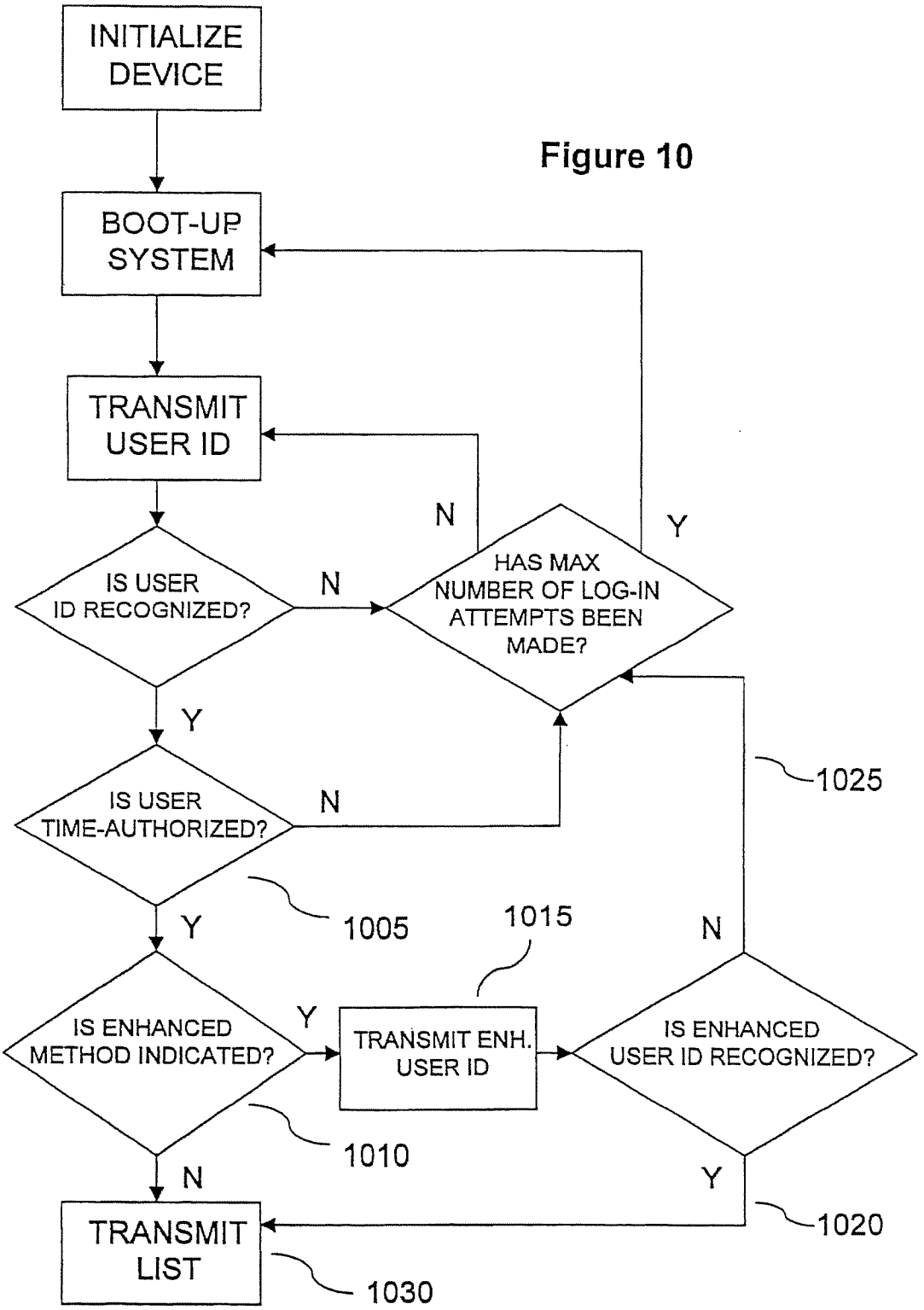

INITIALIZE DEVICE
BOOT-UP SYSTEM
TRANSMIT USER ID
IS USER ID RECOGNIZED?
N
HAS MAX NUMBER OF LOG-IN ATTEMPTS BEEN MADE?
N
Y
Y
IS USER TIME-AUTHORIZED?
N
1025
Y
1005
1015
N
IS ENHANCED METHOD INDICATED?
Y
TRANSMIT ENH. USER ID
IS ENHANCED USER ID RECOGNIZED?
1010
N
Y
TRANSMIT LIST
1020
1030

Figure 10

DETERMINISTIC USER AUTHENTICATION SERVICE FOR COMMUNICATION NETWORK

CROSS REFERENCE TO RELATED APPLICATIONS

This application is a continuation of U.S. patent application Ser. No. 09/525,504; filed Mar. 15, 2000, now U.S. Pat. No. 6,339,830 which is a continuation of U.S. patent application Ser. No. 08/874,054, filed Jun. 13, 1997, now U.S. Pat. No. 6,070,243.

FIELD OF THE INVENTION

The present invention relates to regulating connectivity to and within communicability networks. More specifically, the present invention relates to a authenticating and establishing personalized network connectivity for local users of institutional communication networks.

BACKGROUND OF THE INVENTION

Institutions are relying increasingly on their data communication network infrastructures for efficient communication and data transfer. With this increasing reliance on network computing has arisen a significant need for mechanisms to regulate connectivity and communicability to and within such networks. This need has been partially filled by interact protocol (IP) firewalls. IP firewalls typically restrict access to fixed sets of network resources by applying a set of protocol level filters on a packet-by-packet basis or by requiring prospective users to become authenticated before gaining access to the resources. Authentication has generally required users to supply certain signature information, such as a password. While this requirement of signature information has reduced the risk of unauthorized access to firewall-protected resources, firewalls have proven an imperfect and inflexible regulatory solution. Because firewalls are protocol-specific, firewalls have not provided a means for regulating network connectivity in a multi-protocol environment. Moreover, because firewalls regulate access to particular network resources, they have failed to provide a means for regulating access to sets of network resources which can vary as a function of user identity.

Protocol-independent mechanisms have also been deployed for authenticating users of the resources of institutional networks. However, such authentication mechanisms are only known to have been deployed to challenge remote users attempting to log-in over dial-up phone lines. Such mechanisms are not known to regulate the network access of local users logging-in over a LAN interfaces, such as Ethernet or Token Ring interfaces. Moreover, such mechanisms have, like firewalls, provided an inflexible solution which is unable to regulate access to customized or personalized sets of resources within the network based on user identity.

The flexibility limitations of the foregoing log-in challenge mechanisms have been partially overcome by independently implementing virtual local area networks (VLANs) within institutional networks. VLANs are sub-networks which typically include a plurality of network devices, such as servers, workstations and PCs, that together form a logical work group within a larger network. Because VLAN membership is assigned based on policies rather than physical location in the network, network bandwidth has been conserved and network security enhanced by assigning VLAN membership based on considerations of efficiency and need and restricting the flow of network traffic across VLAN boundaries.

While significant security and efficiency gains have been realized by policy-based VLANs, the solution they have offered is far from complete. VLAN membership has generally been assigned to end systems without reference to the identity of the users of such systems. In the current technology, for instance, VLAN membership is typically assigned by comparing network traffic with a configured set of rules which classify the traffic, and by inference the system which originated the traffic, into one or more VLANs. The identity of the user who sent the traffic is not considered in the assignment process. The failure to consider user identity leaves some network security issues unaddressed. Particularly, a person not authorized to use the resources of a VLAN may be able to gain access to its resources by transmitting data packets which the configured rules will classify into the VLAN, either by communicating over a member end system or by spoofing the required identifiers. Known VLAN assignment methods have also failed to contemplate providing conditional access to users based on the day of the week, the time of day, the length of access or a combination of such factors. Furthermore, current networking equipment and policy-based VLANs in particular have not offered collateral functionality, such as the ability to dynamically track where local users are connected to the network. Such a tracking mechanism would greatly simplify tasks such as network troubleshooting by allowing the network location of a user requesting technical support to be easily determined.

Accordingly, there is a need for comprehensive services for regulating communicablility in institutional networks which are not subject to the inflexibility of conventional user log-in mechanisms or the lack of consideration for user identity of conventional VLAN assignment techniques. There is also a need for services which authenticate local users of institutional networks before establishing network communicability. There is a further need for user authentication services which provide collateral functionality, such as the ability to dynamically track the whereabouts of network users.

SUMMARY OF THE INVENTION

In accordance with its basic feature, the present invention combines the user-specific advantages of log-in challenges and the flexibility of VLANs into a deterministic user-based authentication and tracking service for local users of institutional communication networks.

It is therefore one object of the present invention to provide a service which authenticates local users before establishing network communicability.

It is another object of the present invention to provide a service which assigns and regulates user access to personalized sets of network resources.

It is another object of the present invention to provide a service which grants user access to personalized sets of network resources upon verifying signature information.

It is another object of the present invention to provide a service which conditions user access to personalized sets of network resources on one or more time-dependent variables.

It is another object of the present invention to provide a service which tracks user identity and network location.

These and other objects of the present invention are accomplished by a service which requires that local users be authenticated before gaining access to personalized sets of

network resources. User identification information, time restrictions and authorized lists of resources for particular users are entered and stored in the network. Prior to authentication, packets from an end system being used by a prospective user of network resources are transmitted to an authentication agent operative on an intelligent edge ociated with the system. The agent relays log-in responses received from the system to a basic authentication server in the network for verification of the user. Verification is made by comparing log-in responses with the user identification information stored in the network and determining whether time restrictions associated with the user identification information are applicable. If the basic authentication server is able to verify from the log-in response that the user is an authorized user of network resources, and that the user is authorized to use the network resources at the time of the log-in attempt, the basic authentication server transmits to the agent the list of network resources for which the user is authorized, along with any time restrictions. The agent forwards the list of authorized network resources and time restrictions for storage and use on the edge device. The edge device uses the authorized list of resources and time restrictions to establish network communicability rules for the user. Preferably, the authorized list of network resources is a list of one or more VLANs.

If the basic authentication server is unable to verify from the log-in response that the user is an authorized user of network resources and authorized to use network resources at the time of the log-in attempt, the basic authentication server communicates that information to the agent. Packets from the user continue to be directed to the agent or, alternatively, are dropped. Preferably, the number of log-in attempts users are granted before packets are dropped is configurable.

In another aspect of the invention, the basic authentication server records information relating to the identity and network location of users learned from log-in attempts. The information is accessible by a network administrator tracking network activity from a network management station.

In another aspect of the invention, when the basic authentication server successfully verifies that the user is an authorized user of network resources, and that the user is authorized to use the network resources at the time of the log-in attempt, the basic authentication server, in lieu of transmitting to the agent the list of authorized network resources and time restrictions, initiates an enhanced authentication method for the user. The enhanced authentication method is preferably conducted by an enhanced authentication server within the network.

In another aspect of the invention, when an authenticated user logs-off the network, or fails to transmit packets for a predetermined time, or if the system being used by the authenticated user is disconnected from the network, or if the authorized communicability period expires, or if the basic authentication server or other management entity instructs the agent to abolish the authenticated user's network communicability, the authenticated user's network communicability is deactivated.

The present invention can be better understood in reference to the following detailed description, taken in conjunction with the accompanying drawings which are briefly described below. Of course, the actual scope of the invention is defined by the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a schematic of a network in which a preferred embodiment of the present invention is operative;

FIG. **2** is a schematic of an intelligent edge device operative in the network according to FIG. **1**;

FIG. **3**A is a schematic of a network management station operative in the network according to FIG. **1**;

FIG. **3**B is a schematic of a end system operative in the network according to FIG. **1**;

FIG. **4** is a functional diagram of an authentication agent operative in the network according to FIG. **1**;

FIG. **5** is a functional diagram of a basic authentication server operative in the network according to FIG. **1**;

FIG. **6** is a functional diagram of an authentication client operative in the network according to FIG. **1**;

FIG. **7** is a schematic of an LAN in which a more preferred embodiment of the present invention is operative;

FIG. **8** is a functional diagram of a basic authentication server operative in the network according to FIG. **7**;

FIG. **9** is a flow diagram of a preferred method for authenticating users within network **1**; and

FIG. **10** is a flow diagram of a preferred method for authenticating users within network **7**.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring to FIG. **1**, a network **1** operating in accordance with a preferred embodiment of the present invention is shown. Network **1** includes intelligent edge devices **10**, **15** and a network management station **20** interconnected over a backbone network **30**, such as an asynchronous transfer mode (ATM) or fiber distributed data interface (FDDI) network. Devices **10**, **15** and station **20** are interconnected using cables, which may be fiber optic, unshielded twisted pair, or other form. Devices **10**, **15** are associated with end systems **40**, **50**, **60**, and **45**, **55**, **65**, respectively, which are operative in local area network (LAN) communication media, such as Ethernet or Token Ring. It will be appreciated that Ethernet as used herein is not limited to 10 megabit Ethernet, but includes other Ethernet varieties, such as Fast Ethernet and Gigabit Ethernet. Systems **40**, **50**, **60** and **45**, **55**, **65** may be workstations, PCs, or other systems having a user interface. Although the illustrated network **1** is shown to include two edge devices each associated with multiple end systems, it will be appreciated that a network operating in accordance with the present invention may include one or more edge devices interconnected across a backbone network, and that each edge device may be associated with one or more end systems or servers. It will also be appreciated that, in networks operating in accordance with the present invention, every edge device preferably has common operational capabilities.

Turning to FIG. **2**, device **10** is shown in greater detail. Device **10** is preferably representative of devices **10**, **15**. Device **10** includes a management processor module **210**, backbone module **220** and authentication modules **240**, **250**, **260** interconnected over a switching link **230**. Modules **220**, **240**, **250**, **260** are preferably implemented using custom logic, e.g., application specific integrated circuits (ASICs), while management processor module **210** is preferably software-implemented. Authentication modules **240**, **250**, **260** each include a LAN interface interconnecting systems **40**, **50**, **60**, respectively, and switching link **230**. In contradistinction to hubs which indiscriminately forward packets in unmodified form to all associated end systems, device **10** includes means on each of modules **220**, **240**, **250**, **260** for interpreting, modifying, filtering and forwarding packets.

Preferably, modules **220, 240, 250, 260** are also operative to perform necessary LAN media translations so that device **10** is able to support end stations operating using disparate LAN media. Thus, for example, system **40** utilizing an Ethernet communication protocol may communicate through device **10** with system **50** utilizing Token Ring. LAN switches marketed by the assignee hereof under the federally registered trademarks OmniSwitch® and PizzaSwitch®, implemented with appropriate switching modules available from the assignee, may advantageously be implemented as devices **10, 15** in the performance of the above-described functionality.

Turning to FIG. **3A**, a schematic diagram of network management station **20** is shown. Preferably, station **20** includes a user interface **310**, a software-implemented basic authentication server **320** and user records **330**. Although server **320** and user records **330** are shown operative on station **20**, server **320** and user records **330**, or either one, may be operative on another device in network **1** accessible by station **20**. Although network **1** is illustrated to include a single basic authentication server **320**, a network operating in accordance with the present invention may include one or more basic authentication servers. Server **320** is preferably configured with an address of each of devices **10, 15** and an associated authentication key for the authentication agent active on each of devices **10, 15**. The addresses are preferably IP addresses.

Turning to FIG. **3B**, a schematic diagram of system **40** is shown. System **40** is representative of systems **40, 50, 60** and **45, 55, 65**. System **40** has a user interface **350** and an authentication client **360**. Authentication client **360** is software used during the authentication process. This is preferably a software application installed on system **40** but may also take the form of a standard software application such as Telnet. Client **360** is configured with an address of an authentication agent on associated device **10**, which may be an IP address or a reserved media access control (MAC) address.

An authentication agent is deployed on each of devices **10, 15**. Turning to FIG. **4**, a functional diagram of an authentication agent **400** residing on device **10** is shown. Agent **400** is preferably a software module implemented by management processor module **210**. Agent **400** is configured with an address of device **10**, an address of basic server **320** and an authentication key for server **320**. The configured addresses are preferably IP addresses.

Agent **400** includes CNCT EST means **410**. Means **410** serves, upon initialization of device **10**, to establish a secure connection with server **320**. Means **410** requests a connection to server **320** using the known address of server **320** and acknowledges a response from server **320** to such a request. Means **410** also transmits and receives information from and to server **320** sufficient to allow agent **400** and server **320** to authenticate one another. Preferably, mutual authentication is accomplished through exchange of authentication keys configured on agent **400** and server **320**. Means **410** may encrypt information and decipher encrypted information transmitted during the secure connection establishment process. TCP/IP based flows between agent **400** and server **320** are contemplated. Although network **1** is shown to include only one basic server **320**, it will be appreciated that a network may include more than one basic server. If an agent is configured with the address of more than one basic server in the network, and an attempt to establish a secure connection with a particular server fails, the agent may implement the foregoing process using the known address of another basic server until a secure connection is established.

Agent **400** also includes ID REQ means **420**. Means **420** serves to obtain log-in responses from users of associated systems **40, 50, 60** by communicating with authentication clients operative on systems **40, 50, 60**. Means **420** acknowledges requests received from clients to establish an authentication session. Means **420** responds to the requests by transmitting a log-in prompt to the requesting one of clients. IP-based flows using an application, such as Telnet, or MAC-based flows between agent **400** and clients are contemplated. Flows are initiated by clients using a reserved MAC address or IP address of agent **400** configured on clients.

Agent **400** also includes ID RLY means **430**. Means **430** serves to relay to server **320** for verification log-in responses received from users in response to log-in prompts. Means **430** associates the known address of device **10**, the identifier of the authentication module (i.e., **240, 250** or **260**) associated with the one of systems **40, 50, 60** being used by a user and the log-in response. Means **430** transmits the associated authentication information to server **320** for verification.

Agent **400** also includes VER RLY means **440**. Means **440** serves to relay user status information received from server **320** to users. Means **440** transmits user status information to the one of systems **40, 50, 60** being used by a user. User status information preferably includes a log-in valid or log-in invalid message, depending on whether server **320** was able to successfully verify the log-in response. IP-based flows using an application such as Telnet or MAC-based flows are contemplated for transmission of user status information between agent **400** and clients.

Agent **400** also includes RSR.C RLY means **460**. Means **460** serves to forward for storage and use on device **10** authorized communicability information received from server **320** for authenticated users of systems **40, 50, 60**. Authorized communicability information may advantageously be transmitted by server **320** to agent **400** in the same data packet as user status information. Authorized communicability information includes, for the particular one of the systems **40, 50, 60**, a list of authorized network resources. Authorized communicability information may also include time restrictions, if any. Time restrictions preferably define times during which the particular user is authorized to use the network resources, such as the day of the week, the time of day, and the length of permitted access. The list of authorized network resources is preferably a list of VLAN identifiers. Authorized communicability information is preferably forwarded by agent **400** to management processor module **210** along with the authentication module identifier. Management processor module **210** preferably associates the authorized communicability information with a known address of the one of the systems **40, 50, 60** being used by the authenticated user and stores the pair in device records. The address is preferably a MAC address.

Device records are advantageously used on device **10** to make filtering and forwarding decisions on packets received from and destined for authenticated users. Packets transmitted by an unauthenticated one of systems **40, 50, 60**, unless addressed to authentication agent **400**, are dropped by the receiving one of modules **240, 250, 260**. Packets addressed to an unauthenticated one of systems **40, 50, 60** are also dropped. Packets transmitted by one of authenticated systems **40, 50, 60** addressed to another authenticated one of systems **40, 50, 60** are selectively forwarded according to the following rules:

1. If the destination address is the address of another one of systems **40, 50, 60** associated with device **10**, resort

is made to device records on device **10** to verify that the source and destination systems share a common VLAN. If a VLAN is shared, the packet is forwarded to the destination system. If a VLAN is not shared, the packet is dropped.

2. If the destination address is not the address of another one of systems **40, 50, 60** associated with device **10**, resort is made to device records on device **10** to retrieve the VLAN identifiers associated with the source system. The VLAN identifiers are appended to the packet and the packet is transmitted by backbone module **220** for transmission on backbone network **30**. When the packet arrives on the edge device (e.g., **15**) associated with the destination system (e.g., **45**), resort is made to device records on the edge device to verify that the source and destination systems share a common VLAN. If a VLAN is shared, the packet is forwarded to the destination system. If a VLAN is not shared, the packet is dropped.

Packets addressed to unauthenticated systems in network **1** continue to be dropped. The foregoing rules may be implemented using various known protocols. It will be appreciated that any addressable core, edge, or end devices, stations and systems in network **1** which are not subject to authentication requirements may be treated as authenticated systems for purposes of transmitting and receiving packets under the foregoing rules.

Agent **400** also includes ID TERM means **470**. Means **470** serves, upon receipt of log-off commands from authenticated users, or upon expiration of the authorized communicability period, or when one of authenticated systems **40, 50, 60** is physically disconnected from network **1**, or when one of authenticated systems **40, 50, 60** fails to send traffic for a prescribed length of time, or upon receipt of instruction from server **320**, to deactivate the established network communicability. Means **460** forwards to management processor module **210** a request to remove from device records the address-authorized connectivity information entry for the user whose connectivity is to be deactivated. Upon receipt of such a request, management processor module **210** preferably removes the entry from device records and the authenticated one of systems **40, 50, 60** reverts to the unauthenticated state.

Turning to FIG. **5**, a functional diagram of basic authentication server **320** is shown. Server **320** includes RSRC AUTH means **510**. Means **510** serves to enable network administrators to define, on an individualized basis, authorized communicability information for users of the network **1**. Means **510** enables a network administrator to input user-specific entries. Means **510** supplies a textual or graphical display to user interface **310** operative to accept user-specific entries. Means **510** stores each user-specific entry as a related pair in user records **330**. Each user-specific entry preferably includes user identifier information and a list of authorized network resources. User-specific entries may also include time restrictions for the particular user. User identification information preferably includes signature information for the user, such as a password. Means **510** also enables a network administrator to input device-specific entries. Device-specific entries preferably includes, for each edge device in network **1** having an authentication agent, a device address and an authentication key. Device addresses are preferably IP addresses. Means **510** stores each device-specific entry as a related pair in network management records (not shown). Each device address is preferably uniquely assigned to a particular edge device operative within network **1**.

Server **320** also includes CNCT EST means **520**. Means **520** serves, upon receipt of a request from an authentication agent, to establish a secure connection with the agent. Means **520** acknowledges receipt from the agent of a request to establish a secure connections and to respond to the request. Means **520** also transmits and receives information sufficient to allow the agent and server **320** to authenticate one another. Preferably, authentication is established through exchange of authentication keys. Means **520** may encrypt information and decipher encrypted information transmitted during the secure connection establishment process. TCP/IP based flows between the agent and server **320** are contemplated.

Server **320** also includes ID VER means **530**. Means **530** serves to subject to a verification process authentication information received from users via agent **400**. Means **530**, upon receipt of authentication information from agent **400**, determines if the log-in response matches the user identification information associated with a user-specific entry in user records **330**. If a match is found, and there are time restrictions associated with the user-specific entry, means **530** determines from the time restrictions if the user is authorized to use network **1** at the particular time. If the user is time-authorized or there are no time restrictions, means **530** generates authorized communicability information. Means **530** retrieves the list of authorized network resources associated with the matching user identification information in the generation of authorized communicability information. Authorized communicability information may also include anytime restrictions. Means **530** also generates user status information. User status information is information sufficient to communicate to agent **400** whether user identification information was successfully verified. User status information is preferably either a log-in valid or log-in invalid message. Means **530** transmits authorized communicability information and user status information to agent **400**. Preferably, authorized communicability information and user status information are transmitted as part of the same data packet. If no match for user identification information is found, or if the user is not time-authorized, means **530** generates and transmits to agent **400** user status information, preferably in the form of a log-in invalid message, but does not generate or transmit authorized communicability information. Although the above described means operative on server **320** are described to be interoperative in conjunction with agent **400**, it will be appreciated that the means are fully interoperative with other authentication agents residing on edge devices in network **1**.

Server **320** also includes ID STOR means **540**. Means **540** serves to forward for storage and use by a network administrator user tracking information. User tracking information is preferably retained for all log-in attempts made by prospective users, whether successful or unsuccessful. User tracking information may include, for each log-in attempt, any information learned from one or more of the following: user identification information, authentication information, user status information, authorized communicability information. User tracking information also may include the time of day the log-in attempt was made. The time of day may be kept on and obtained from server **320**. Server **320** preferably associates the user tracking information and stores the information as an entry in a network activity database (not shown) that is accessible by or resides on station **20**. Network activity database entries are accessible by a network administrator using interface **310**.

Server **320** also includes NET MNTR means **550**. Means **550** serves to enable a network administrator to access and

use user tracking information. Means 550 supplies a textual or graphical display to interface 310 operative to display user tracking information. Means 550 also enables a network administrator to generate user tracking information reports consisting of related information from one or more user tracking information entries.

Client 360 further includes ID OFF means 640. Means 640 serves to initiate the log-off process by which authenticated users log-off the network 1. Means 640 supplies a textual or graphical display to user interface 350 operative to accept log-off commands. Means 640 transmits log-off commands to agent 400 for deactivation of established network connectivity.

Turning to FIG. 6, a functional diagram of client 360 is shown. Client 360 is representative of clients residing on systems 40, 50, 60 and 45, 55, 65. Client 360 includes ID INIT means 610. Means 610 serves, when system 40 is booted-up by a user, to request and establish an authentication session with agent 400. Alternatively, means 610 can be activated by a direct action of the user of system 40. Means 610 transmits to agent 400 a request to establish an authentication session using a known address of agent 400. Client 360 preferably transmits requests periodically until agent 400 responds. A MAC-based flow is contemplated. Alternatively, an IP-based flow using an application such as Telnet may be used.

Client 360 also includes ID RPLY means 620. Means 620 serves to enable users to reply to log-in prompts received from agent 400. Means 620 supplies a textual or graphical display to a user interface of system 40 operative to accept log-in responses. Means 620 also transmits log-in responses to agent 400.

Client 360 also includes VER DSPL means 630. Means 630 serves to convey to users whether log-in attempts were successful or unsuccessful. Means 630 supplies a textual or graphical display to a user interface of system 40 operative to display user status information, preferably a log-in valid message or a log-in invalid message, received from agent 400.

Client 360 further includes ID OFF means 640. Means 640 serves to initiate the log-off process by which authenticated users log-off the network 1. Means 640 supplies a textual or graphical display to user interface 350 operative to accept log-off commands. Means 640 transmits log-off commands to agent 400 for deactivation of established network connectivity.

Referring to FIG. 7, a network 7 operating in accordance with an alternative embodiment of the present invention is shown. In the alternative embodiment, an enhanced authentication method is conducted before network communicability is granted. Network 7 includes intelligent edge devices 710, 715 and a network management station 720 interconnected over a backbone network 730 by means similar to those described in relation to network 1. Bridges 710, 715 are associated with end systems 740, 750, 760 and 745, 755, 765, respectively, which utilize LAN communication media, such as Ethernet or Token Ring. Network 7 also includes enhanced authentication server 770 interconnected over backbone network 730. It will be appreciated that, as in the previous preferred embodiment, a network operating in accordance with the alternative embodiment may include one or more edge devices having common operational capabilities and associated with one or more end systems. In network 7, devices 710, 715 station 720 and systems 740, 750, 760 and 745, 755, 765 have operational capabilities common to their counterparts in network 1, plus additional operational capabilities hereafter described.

Turning to FIG. 8, a functional diagram of a basic authentication server 800 preferably operable on station 720 is shown. Server 800 is preferably interoperative with devices 710, 715 and systems 740, 750, 760 and 745, 755, 765 and associated modules, agents and clients to perform the functionality of server 320 described above, including RSRC AUTH means 510, CNCT EST means 520, ID VER means 530, ID STOR means 540 and NET MNTR means 550.

Server 800 also includes ENH CNCT EST means 810. Means 810 serves to establish and maintain a secure connection with enhanced authentication server 770. A TCP/IP based flow is contemplated. Server 800 also includes ENH RSRC AUTH means 820. Means 820 serves to enable network administrators to define, on an individualized basis, an enhanced authentication method for each prospective user of network 7. Means 820 enables a network administrator to enter user-specific entries which additionally include enhanced authentication method information. Enhanced authentication method information includes information sufficient to enable basic server 800 to identify a device, station, or system within network 7 which will conduct the enhanced authentication session, if any, the prospective user must successfully complete to become authenticated. Preferably, enhanced authentication method information includes an IP address of enhanced authentication server 770. Enhanced authentication methods may include one of various security methods implemented on enhanced authentication server 770. Authentication methods marketed under the trade names Secure ID™ by Security Dynamics, Inc. and methods that comply with Internet Engineering Task Force (IETF) RFC 2058 Remote Authentication Dial-in User Service (RADIUS) are referenced herein by way of example.

Server 800 also includes ENH ID VER means 830. Means 830 serves, upon verifying log-in responses received from a user and that the user is authorized to use the network 7 at the time of the log-in attempt, to initiate an enhanced authentication method, if indicated. Means 830, upon determining that the log-in response matches user identification information associated with a user-specific entry in user records, and upon determining that the user is time-authorized if time restrictions are indicated, checks whether there is an enhanced authentication method associated with the matching user-specific entry. If an enhanced authentication method is indicated, means 820, before transmitting authorized communicability information and user status information to the agent on the appropriate one of devices 710, 715, transmits a request to enhanced authentication server 770 to conduct an enhanced authentication session with the user. The enhanced authentication session is preferably conducted between enhanced server 770 and the user transparently to basic server 800. Enhanced server 770 instructs basic server 800 of the results of the enhanced authentication session. If the user was successfully authenticated, means 830 transmits to the agent authorized communicability information and user status information, preferably in the form of a log-in valid message. If the user was not successfully authenticated, means 830 transmits user status information, preferably a log-in invalid message, but no authorized communicability information. If an enhanced authentication method is not indicated when the check for an enhanced authentication method is performed, means 830 transmits to the agent authorized communicability information and user status information, in the form of a log-in valid message, without engaging server 770. If a matching entry for user identification information is not

found in user records, or if the user is not time-authorized, means **830** transmits to the agent user status information, in the form of a log-in invalid message, without transmitting authorized communicability information.

Referring now to FIG. **9**, a flow diagram illustrates a preferred method for implementing the invention within network **1**. When device **10** is initialized (**905**), agent **400** attempts to establish a secure connection with server **320** using the known address of server **320**. Once a TCP session is successfully established, agent **400** and server **320** authenticate one another by exchanging authentication keys.

When a user boots-up device **40** (**910**), client **360** activates. Client **360** sends an authentication request to agent **400** using a known address of agent **400**. Authentication requests are transmitted to agent **400** periodically until agent **400** responds. When agent **400** receives a request, agent **400** responds by transmitting a log-in prompt to client **360**.

The user enters a log-in response and the response is transmitted to agent **400** (**915**). Agent **400** transmits authentication information to server **320**. Authentication information preferably includes an address of device **10**, an identifier of authentication module **240** associated with system **40**, and the log-in response.

Server **320** determines whether the log-in response is recognized on station **20** (**920**). Server **320** checks user records **330** for a user-specific entry having user identification information matching the log-in response. If a matching entry is found, server **320** checks any time restrictions associated with the entry to determine if the user is authorized to use the network resources at the particular time (**925**). If the prospective user is time-authorized, server **320** retrieves the list of authorized network resources and any time restrictions associated with the matching user identification information. The information is transmitted to agent **400** (**930**) along with user status information, preferably a log-in valid message. If no matching entry is found (**935**), or if the user is not time-authorized (**940**), user status information, preferably a log-in invalid message, is returned to the user via agent **400**. Agent **400** also in that instance determines if user has made the configurable number of failed log-in attempts (**945**). If the configurable number of failed log-in attempts has been reached (**950**), agent **400** terminates the authentication session with client **360**. The user is denied network access until such time as the user reboots system **40**. If the configurable number of failed log-in attempts has not been reached (**955**), agent **400** presents the user with another log-in prompt.

Turning to FIG. **10**, a flow diagram illustrates a preferred method for implementing the invention within network **7**. The method proceeds generally as in FIG. **9**, except that an enhanced authentication method is performed, if indicated.

Accordingly, once a determination is made that the user is time-authorized (**1005**), basic server **800** checks whether there is an enhanced authentication method associated with the matching entry (**1010**). If an enhanced authentication method is indicated, server **800** transmits a request to enhanced authentication server **770** to conduct an enhanced authentication session with the user (**1015**). Enhanced server **770** informs basic server **800** of the results of the enhanced authentication session. If the session was successfully completed (**1020**), basic server **800** transmits authorized communicability information and user status information, in the form of a log-in valid message, to the agent (**1030**). If enhanced session was not successfully completed (**1025**), basic server **800** transmits a log-in invalid message to user and does not transmit authorized communicability information to agent. Agent also in that instance determines if user has made a configurable number of failed log-in attempts. The authentication session either continues or terminates as discussed depending on the outcome of that inquiry. If an enhanced authentication method is not indicated when the check for an enhanced authentication method is performed (**1010**), server **800** transmits authorized communicability information and user status information, in the form of a log-in valid message, without requesting server **770** to conduct an enhanced authentication session.

It will be appreciated by those of ordinary skill in the art that the invention can be embodied in other specific forms without departing from the spirit or essential character hereof. The present description is therefore considered in all respects to be illustrative and not restrictive. The scope of the invention is indicated by the appended claims, and all changes that come within the meaning and range of equivalents thereof are intended to be embraced therein.

We claim:

1. A user authentication method for a communication network having a plurality of nodes, the method comprising:

entering on a first node first user identification information;

transmitting to an authentication agent on a second node communicating with the first node over a LAN link the first user identification information;

relaying from the authentication agent to an authentication server the first user identification information;

comparing on the authentication server the first user identification information with user identification information in a database of user identification information; and

transmitting from the authentication server to the authentication agent, if the first user identification information matches user identification information in the database of user identification information, notification information notifying the authentication agent that a user on the first node has been authenticated whereupon the authentication agent authorizes transmission on the second node of packets in data flows involving the first node, wherein the first user identification information is transmitted to the authentication agent as part of a MAC-based authentication flow between an authentication client on the first node and the authentication agent.

2. The method of claim **1**, further comprising relaying from the authentication agent to the authentication client as part of the MAC-based authentication flow the notification information.

3. The method of claim **1**, further comprising, prior to transmitting the first user identification information to the authentication agent, transmitting from the authentication client to the authentication agent as part of the MAC-based authentication flow a request to establish an authentication session.

4. The method of claim **1**, further comprising transmitting from the authentication client to the authentication agent as part of the MAC-based authentication flow a logoff request, whereupon the authentication agent revokes the authorization.

5. The method of claim **1**, further comprising transmitting from the authentication server to the authentication agent, if the first user identification information does not match user identification information in the database, second notification information notifying the authentication agent that the user on the first node has failed to become authenticated, whereupon the authentication agent fails to authorize trans-

mission on the second node of packets in data flows involving the first node and relays to the authentication client as part of the MAC-based authentication flow the second notification information.

6. The method of claim 5, wherein if the authentication agent determines that the user has made a predetermined number of failed authentication attempts, the authentication agent transmits to the authentication client as part of the MAC-based authentication flow information notifying the authentication client that further authentication attempts will be inhibited.

7. The method of claim 1, wherein the packets transmitted pursuant to the authorization are neither encrypted nor decrypted by the second node.

8. A user authentication method for a communication network having a plurality of nodes, the method comprising:

entering on a first node first user identification information;

transmitting to an authentication agent on a second node communicating with the first node over a LAN link the first user identification information;

relaying from the authentication agent to an authentication server the first user identification information;

comparing on the authentication server the first user identification information with user identification information in a database of user identification information; and

transmitting from the authentication server to the authentication agent, if the first user identification information matches user identification information in the database of user identification information, information notifying the authentication agent that a user on the first node has been authenticated whereupon the authentication agent authorizes transmission on the second node of packets in data flows involving the first node, wherein the authorization comprises authorizing an interface to the LAN link to allow packets in data flows.

9. The method of claim 8, wherein the interface is on the second node.

10. The method of claim 8, wherein the LAN link is an Ethernet link.

11. The method of claim 8, wherein the authentication server is a RADIUS server.

12. The method of claim 8, wherein the authentication server is on a third node.

13. The method of claim 8, wherein prior to the authorization, the second node drops all packets received from the first node that are not part of an authentication flow.

14. The method of claim 8, wherein prior to the authorization, the second node drops all packets received from the first node that are not addressed to the authentication agent.

15. A user authentication method for a communication network having a plurality of nodes, the method comprising:

entering on a first node first user identification information;

transmitting to an authentication agent on a second node communicating with the first node over a LAN link the first user identification information;

relaying from the authentication agent to an authentication server the first user identification information;

comparing on the authentication server the first user identification information with user identification information in a database of user identification information; and

transmitting from the authentication server to the authentication agent, if the first user identification information matches user identification information in the database of user identification information, notification information notifying the authentication agent that a user on the first node has been authenticated whereupon the authentication agent authorizes transmission on the second node of packets in data flows involving the first node and one or more nodes reachable by the first node via the second node and relays to the first node the notification information.

16. The method of claim 15, wherein prior to the authorization, the second node inhibits transmission to any nodes reachable by the first node via the second node of all packets received from the first node that are not part of an authentication flow.

17. The method of claim 15, wherein prior to the authorization, the second node inhibits transmission to any nodes reachable by the first node via the second node of all packets received from the first node that are not addressed to the authentication agent.

18. The method of claim 15, further comprising, prior to transmitting the first user identification information to the authentication agent, transmitting from the first node to the authentication agent a request to establish an authentication session.

19. The method of claim 15, further comprising transmitting from the first node to the authentication agent a logoff request, whereupon the authentication agent revokes the authorization.

20. The method of claim 15, further comprising transmitting from the authentication serve to the authentication agent, if the first user identification information does not match user identification information in the database, second notification information notifying the authentication agent that the user on the first node has failed to become authenticated, whereupon the authentication agent fails to authorize transmission on the second node of packets in data flows involving the first node and any nodes reachable by the first node via the second node and relays to the first node the second notification information.

21. The method of claim 20, wherein upon receipt of the second notification information, the authentication agent determines the number of failed authentication attempts made by the user.

22. The user authentication method of claim 21, wherein if the authentication agent determines that the user has made a predetermined number of failed authentication attempts, the authentication agent inhibits further authentication attempts.

23. The user authentication method of claim 21, wherein if the authentication agent determines that the user has made a predetermined number of failed authentication attempts, the authentication agent transmits to the first node information notifying the first node that further authentication attempts will be inhibited.

24. A user authentication method for a communication network having a plurality of nodes, the method comprising:

entering on a first node first user identification information;

transmitting to an authentication agent on a second node communicating with the first node over a LAN link the first user identification information;

relaying from the authentication agent to an authentication server the first user identification information;

comparing on the authentication server the first user identification information with user identification information in a database of user identification information; and

transmitting from the authentication server to the authentication agent, if the first user identification information matches user identification information in the database of user identification information, information notifying the authentication agent that a user on the first node has been authenticated whereupon the authentication agent authorizes transmission on the second node of packets in data flows involving the first node, wherein the packets that are transmitted pursuant to the authorization bypass the authentication agent.

25. A user authentication method for a communication network having a plurality of nodes, the method comprising:

entering on a first node first user identification information;

transmitting to an authentication agent on a second node communicating with the first node over a LAN link the first user identification information;

relaying from the authentication agent to an authentication server the first user identification information;

comparing on the authentication server the first user identification information with user identification information in a database of user identification information; and

transmitting from the authentication server to the authentication agent, if the first user identification information matches user identification information in the database of user identification information, information notifying the authentication agent that a user on the first node has been authenticated and information identifying a VLAN for which the user has been authenticated whereupon the authentication agent authorizes transmission on the second node of packets in data flows that involve the first node and are within the VLAN.

26. The method of claim 25, wherein the information notifying the authentication agent that the user on the first node has been authenticated and the information identifying the VLAN for which the user has been authenticated are transmitted from the authentication server to the authentication agent in a single packet.

27. The method of claim 25, wherein one or more of the packets that are transmitted pursuant to the authorization are appended on the second node and transmitted from the second node to a backbone network with an identifier of the VLAN.

28. The method of claim 25, further comprising dropping on the second node of packets in data flows involving the first node and other nodes that are not within the VLAN.

29. The method of claim 25, further comprising, before the authorization, dropping on the second node of packets in data flows involving the first node.

30. The method of claim 25, further comprising, after the authorization, forwarding on the second node of packets in data flows involving the first node and other nodes that are within the VLAN.

31. The method of claim 25, wherein the first user identification information is transmitted front the first node to the authentication agent as part of a MAC-based authentication flow between an authentication client on the first node and the authentication agent.

32. The method of claim 25, wherein the authorization comprises authorizing an interface to the LAN link to allow packets in data flows.

33. The method of claim 25, wherein the packets that are transmitted pursuant to the authorization bypass the authentication agent.

* * * * *