

United States District Court,
E.D. Texas, Tyler Division.

ALCATEL USA SOURCING, INC,
Plaintiff.

v.

MICROSOFT CORPORATION,
Defendant.

No. 6:06 CV 499

Aug. 21, 2008.

Carl J. Blickle, Eric D. Hayes, Kirkland & Ellis LLP, Chicago, IL, James E. Marina, Jennifer J. Schmidt, Paul A. Bondor, Robert A. Appleby, Tamir Packin, Todd M. Friedman, William C. Mercer, Kirkland & Ellis, LLP, New York, NY, Scott F. Partridge, Bradley Bowling, Larry Gene Spears, Lisa Catherine Kelly, Michael A. Hawes, Baker Botts, Houston, TX, Charles Ainsworth, Robert Christopher Bunt, Robert M. Parker, Tammy M. Pennington, Parker Bunt & Ainsworth, Tyler, TX, Jonathan Bell Rubenstein, Timothy S. Durst, Baker Botts, Dallas, TX, for Plaintiffs.

Roger A. Denning, Fish & Richardson, San Diego, CA, Thomas M. Melsheimer, Decker A. Cammack, Matthew Kenton Wernli, Fish & Richardson, Dallas, TX, Alan D. Albright, Barry Kenneth Shelton, Christopher Ryan Johnson, Steven Joel Lauff, Ross S. Garsson, Fish & Richardson, Austin, TX, Andrew C. Warnecke, Fish & Richardson PC, Washington, DC, Melissa Richards Smith, Gillam & Smith, LLP, Marshall, TX, Robert M. Parker, Parker, Bunt & Ainsworth, P.C., Tyler, TX, for Defendants.

MEMORANDUM OPINION

LEONARD DAVIS, District Judge.

This Memorandum Opinion construes the disputed terms in U.S. Patent Nos. 6,339,830 (the "'830 Patent"), 6,661,799 (the "'799 Patent"), 6,674,767 (the "'767 Patent"), 6,874,090 (the "'090 Patent"), and 6,944,273 (the "'273 Patent").

BACKGROUND

This case involves five patents. The '830 and '090 Patents are directed to an authentication service for authenticating users who log on from a client through an authentication agent that operates on an intelligent edge device. The application that became the '090 Patent is a continuation of the application that became the '830 Patent. The intelligent edge device and the client are located on a local area network (LAN). The service allows authenticated users access to a personalized subset of computing resources on the interconnected networks. The authentication agents establish rules to filter and forward network traffic that originates from or is destined to particular authenticated users during authorized time periods.

The '799 Patent discloses a system for performing network address translations between internal and external address realms. The system allows applications running to host computers within a network to request information about address translations to be performed by a network address translation device. With this information, applications may send useful information to other applications to enable applications to communicate through the network address translation device in the absence of statically defined translations rules for a particular communications channel. Alcatel USA Sourcing, Inc. ("Alcatel") alleges Microsoft Corporation ("Microsoft") infringes various claims of the '830, '799, and '090 Patents.

The '767 Patent is directed to a flexible gateway that determines the necessary conversions to transfer a message or data from an originating device located on a network that uses one protocol to a destination device located on a different network that uses another protocol. After the gateway receives information from the originating device, the gateway identifies the specific device type and the specific network type to which the information is bound. The gateway subsequently calls the device and network drivers associated with the destination device and associated network. These drivers manipulate the message or data into a format recognized by the destination device and provide the manipulated data or message to the destination device using the compatible protocol.

The '273 Patent is directed to a messaging system that sends messages to a receiving device at a future delivery time, where the receiving device is coupled to a data-centric network or a telephony-centric network. The messaging system permits seamless messaging at a future delivery time to a receiving device located on either network such that the message format and transmission network are transparent to the message originator. Thus, the message originator need not retain a messaging service or acquire special-purpose hardware or software to obtain future messaging capabilities. Microsoft alleges Alcatel infringes various claims of the '767 and '273 Patents.

APPLICABLE LAW

"It is a 'bedrock principle' of patent law that 'the claims of a patent define the invention to which the patentee is entitled the right to exclude.'" Phillips v. AWH Corp., 415 F.3d 1303, 1312 (Fed.Cir.2005) (en banc) (quoting Innova/Pure Water Inc. v. Safari Water Filtration Sys., Inc., 381 F.3d 1111, 1115 (Fed.Cir.2004)). In claim construction, courts examine the patent's intrinsic evidence to define the patented invention's scope. *See id.*; C.R. Bard, Inc. v. U.S. Surgical Corp., 388 F.3d 858, 861 (Fed.Cir.2004); Bell Atl. Network Servs., Inc. v. Covad Commc'ns Group, Inc., 262 F.3d 1258, 1267 (Fed.Cir.2001). This intrinsic evidence includes the claims themselves, the specification, and the prosecution history. *See Phillips*, 415 F.3d at 1314; C.R. Bard, Inc., 388 F.3d at 861. Courts give claim terms their ordinary and accustomed meaning as understood by one of ordinary skill in the art at the time of the invention in the context of the entire patent. Phillips, 415 F.3d at 1312-13; Alloc, Inc. v. Int'l Trade Comm'n, 342 F.3d 1361, 1368 (Fed.Cir.2003).

The claims themselves provide substantial guidance in determining the meaning of particular claim terms. Phillips, 415 F.3d at 1314. First, a term's context in the asserted claim can be very instructive. *Id.* Other asserted or unasserted claims can also aid in determining the claim's meaning because claim terms are typically used consistently throughout the patent. *Id.* Differences among the claim terms can also assist in understanding a term's meaning. *Id.* For example, when a dependent claim adds a limitation to an independent claim, it is presumed that the independent claim does not include the limitation. *Id.* at 1314-15.

"[C]laims 'must be read in view of the specification, of which they are a part.' " *Id.* (quoting *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed.Cir.1995) (en banc)). "[T]he specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.' " *Id.* (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed.Cir.1996)); *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1325 (Fed.Cir.2002). This is true because a patentee may define his own terms, give a claim term a different meaning than the term would otherwise possess, or disclaim or disavow the claim scope. *Phillips*, 415 F.3d at 1316. In these situations, the inventor's lexicography governs. *Id.* Also, the specification may resolve ambiguous claim terms "where the ordinary and accustomed meaning of the words used in the claims lack sufficient clarity to permit the scope of the claim to be ascertained from the words alone ." *Teleflex, Inc.*, 299 F.3d at 1325. But, "[a]lthough the specification may aid the court in interpreting the meaning of disputed claim language, particular embodiments and examples appearing in the specification will not generally be read into the claims." *Comark Commc'ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed.Cir.1998) (quoting *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1571 (Fed.Cir.1988)); *see also Phillips*, 415 F.3d at 1323. The prosecution history is another tool to supply the proper context for claim construction because a patent applicant may also define a term in prosecuting the patent. *Home Diagnostics, Inc., v. Lifescan, Inc.*, 381 F.3d 1352, 1356 (Fed.Cir.2004) ("As in the case of the specification, a patent applicant may define a term in prosecuting a patent.").

Although extrinsic evidence can be useful, it is " 'less significant than the intrinsic record in determining the legally operative meaning of claim language.' " *Phillips*, 415 F.3d at 1317 (quoting *C.R. Bard, Inc.*, 388 F.3d at 862). Technical dictionaries and treatises may help a court understand the underlying technology and the manner in which one skilled in the art might use claim terms, but technical dictionaries and treatises may provide definitions that are too broad or may not be indicative of how the term is used in the patent. *Id.* at 1318. Similarly, expert testimony may aid a court in understanding the underlying technology and determining the particular meaning of a term in the pertinent field, but an expert's conclusory, unsupported assertions as to a term's definition is entirely unhelpful to a court. *Id.* Generally, extrinsic evidence is "less reliable than the patent and its prosecution history in determining how to read claim terms." *Id.*

The patents in suit also contain means-plus-function limitations that require construction. Where a claim limitation is expressed in "means plus function" language and does not recite definite structure in support of its function, the limitation is subject to 35 U.S.C. s. 112, para. 6. *Braun Med., Inc. v. Abbott Labs.*, 124 F.3d 1419, 1424 (Fed.Cir.1997). In relevant part, 35 U.S.C. s. 112, para. 6 mandates that "such a claim limitation 'be construed to cover the corresponding structure ... described in the specification and equivalents thereof.' " *Id.* (citing 35 U.S.C. s. 112, para. 6). Accordingly, when faced with means-plus-function limitations, courts "must turn to the written description of the patent to find the structure that corresponds to the means recited in the [limitations]." *Id.*

Construing a means-plus-function limitation involves multiple inquiries. "The first step in construing [a means-plus-function] limitation is a determination of the function of the means-plus-function limitation." *Medtronic, Inc. v. Advanced Cardiovascular Sys., Inc.*, 248 F.3d 1303, 1311 (Fed.Cir.2001). Once a court has determined the limitation's function, "the next step is to determine the corresponding structure disclosed in the specification and equivalents thereof." *Id.* A "structure disclosed in the specification is 'corresponding' structure only if the specification or prosecution history clearly links or associates that structure to the function recited in the claim." *Id.* Moreover, the focus of the "corresponding structure" inquiry is not merely whether a structure is capable of performing the recited function, but rather whether the corresponding structure is "clearly linked or associated with the [recited] function." *Id.*

CLAIM TERMS

'830 and '090 Patents

Virtual Local Area Network / VLAN

Claims 12, 25, 26, and 27 of the '830 Patent and claim 27 of the '090 Patent contain the term "virtual local area network [VLAN]." Alcatel contends the term means "a subset of nodes on a local area network." Microsoft contends the term means "group of nodes or network resources on the communications network." The parties dispute whether the nodes or network resources must reside on a LAN.

The intrinsic record does not require the nodes or network resources to reside on a particular type of network. The specification defines a "virtual local area network" as "subnetworks 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." '830 Patent, col. 1:58-61. FN1 The specification does not limit the backbone of the network that connects the intelligent edge devices to a LAN medium. Id. at col. 4:24-32.

FN1. The '830 and '090 Patents' specifications contain nearly identical disclosures. The Court will cite to the '830 Patent, though the '090 Patent contains the same propositions.

Alcatel claims the applicants disclaimed a VLAN comprised of nodes connected through dial-up networks. During prosecution of the application that became the '830 Patent, the applicants, in response to an obviousness-type double patenting rejection, filed a terminal disclaimer. Alcatel's Opening Claim Construction Brief, Ex. G, at 16. The applicants also submitted a supplemental disclosure statement to disclose certain documents related to Remote Authentication Dial In User Service (RADIUS). Id. at 16-17.

The applicants described RADIUS as "characteristic of a system that enables remote users to log-in over dial up phone line connections, which Applicants expressly distinguished in the Background section of the application." Id. at 17. The relevant portion of the Background of the Invention states:

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.

'830 Patent, col. 1:43-54.

In response to the Examiner's rejection, the applicants subsequently stated "RADIUS does not disclose or suggest user access to a group of nodes represented by a VLAN or VLAN identifier." Alcatel's Opening Claim Construction Brief, Ex. G, at 17. With respect to claims that did not include a VLAN limitation, the applicants amended the claims to add a "second node communicating with a first node over a LAN link" limitation to further distinguish those claims over dial-up phone line connections. Id.

The applicants distinguished RADIUS on the basis that RADIUS disclosed a system where the remote user to be authenticated logged-in over a dial-up connection. The VLAN limitations go to relationship between nodes the user has access to and not the connection between the user and the intelligent edge device. '830 Patent, col. 13:17-27 (claiming method step of "associating ... each [user] with a group of nodes represented by a virtual local area network selected for the user"); id. at col. 14:49-65 (claiming a user authentication system that comprises a first node for entering user identification information, a second node for receiving the user identification information, and a port on the second node that allows communication between the "first node and a group of nodes associated with the user identification information, ... wherein the group of nodes is associated with a virtual local area network"). To the extent the applicants' statements disclaim dial-up connections, the statements only disclaim a dial-up connection between the remote user and the authentication agent and do not limit the VLAN terms.

For the abovementioned reasons, "virtual local area network [VLAN]" means "subnetworks 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."

LAN Link

Claims 17 and 37 of the '830 Patent and claims 1 and 25 of the '090 Patent contain the term "LAN link." Alcatel argues "LAN link" means "a local area network interface, such as Ethernet or Token Ring, as opposed to a dial-up phone line connection." Microsoft argues "LAN link" means "a permanent wired communication channel between the first node and second node using LAN transmission protocols." The parties dispute whether the "LAN link" is limited to a permanent, wired connection.

The "LAN link" is not limited to a permanent, wired connection. The claimed methods transfer user identification information over a "LAN link." '830 Patent, col. 13:66-col. 14:20, col. 16:11-30; '090 Patent, col. 12:19-45, col. 15:11-34. The specification does not limit the LAN link to a permanent wired connection, but describes the devices and end systems associated with the "LAN link" as operable in LAN communication media. '830 Patent, col. 4:32-40. At the time of the invention that matured into the '830 and '090 Patents, wireless LANs, while not in widespread usage, were known by those in the art, which Microsoft agrees with. *See Alcatel USA Sourcing, Inc. v. Microsoft Corp.*, Cause No. 6:06cv499, Transcript of *Markman* hearing held on 7/8/2008, 9 ("Certainly wireless networks existed at the time of the patent, but conventional local area networks were not considered to be wireless at that time."); U.S. Pat. No. 5,487,069, col. 1:58-62 (describing the state of wireless LAN technology in November 23, 1993 and stating "[o]ne wireless LAN which is commercially available is that sold by Motorola under the trade name ALTAIR. This system operates at approximately 18 GHz, however, the maximum data transmission rate is limited to approximately 3-6 Mbit/s."); U.S. Pat. No. 5,852,405, col. 1:4-col. 2:34 (describing wireless LAN technology as of October 26, 1995).

During prosecution, the applicants added the "LAN Link" limitation to distinguish over RADIUS, which the applicants characterized as enabling remote users to log-in over dial-up phone line connections. Alcatel's Opening Claim Construction Brief, Ex. G, at 16-17; *see also* '830 Patent, col. 1:43-54. The applicants did not disclaim connections to wireless LANs.

Nothing in the intrinsic record limits a "LAN link" to a permanently wired communications channel. From the intrinsic record, a "LAN link" is the communications channel that connects two nodes of a LAN. Thus,

"LAN link" means "a connection, other than a dial-up phone connection, to a local area network (LAN)."

MAC-Based Authentication Flow

Claims 1, 3, 4, and 5 of the '090 Patent contain the term "MAC-based authentication flow." Alcatel contends the term means "information exchange taking place via the Media Access Control sublayer of the Data Link layer of the OSI reference model for authentication." Microsoft argues "MAC-based authentication flow" means "user authentication communication between the authentication client and the authentication agent in which the authentication client is configured with the MAC address of the authentication agent and the authentication client addresses communication to the authentication agent using the MAC address."

MAC is an acronym for "media access control." '090 Patent, col. 5:35-38. Network technology is often explained in terms of different functional layers. One sublayer is the MAC sublayer. Additionally, a network device has a MAC address. '830 Patent, col. 1:26-27; '090 Patent, col. 5:35-38, col. 5:43-46. Thus, the parties dispute whether "MAC-based authentication flow" is authentication flow addressed using the MAC address or if the term refers to information exchanged at the MAC sublayer.

The "MAC-based authentication flow" refers to the authentication data-flow between the authentication client and authentication agent. '090 Patent, col. 12:19-45, col. 12:50-55, col. 12:56-60, col. 12:61-col. 13:4. The claims cover information transmitted to the authentication agent or the authentication client as part of a "MAC-based authentication flow." *Id.* at col. 12:19-45 (claiming user authentication method 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"); *id.* at col. 12:61-col. 13:4 (claiming user authentication method wherein the authentication agent, if the user fails to become authenticated, "relays to the authentication client as part of the MAC-based authentication flow the second notification information").

The specification discloses exchanges of authentication information between authentication agents and authentication clients. The specification describes MAC-based flows as data flows between the authentication agent and client initiated by the client using the reserved MAC address of the authentication agent. *Id.* at col. 6:12. The MAC-based flow may travel to the authentication agent or the authentication client. *Id.* at col. 6:6-10, col. 12:61-col. 13:4. The specification does not specify which particular layer or sublayer the information travels.

The authentication agent contains the address of the intelligent edge device, the basic server, and the authentication key for the server. *Id.* at col. 5:43-46. The intelligent edge device may contain the MAC addresses of the systems that contain authentication clients; however, the specification indicates these MAC addresses are used to forward data packets to systems with authenticated users and not for the purposes of authentication. *See id.* at col. 6:50-col. 7:27.

The intrinsic record indicates "MAC-based authentication flow" relates to the authentication client's use of the MAC address of the authentication agent to initiate authentication flow between the authentication agent and the client. Thus, "MAC-based authentication flow" means "information exchange in which the authentication client uses the MAC address of the authentication agent for the purposes of authentication."

Comparing on the Authentication Server the First User Identification Information with User Identification Information in a Database of User Identification Information

Claims 17 and 37 of the '830 Patent and claims 1 and 25 of the '090 Patent contain the term "comparing on the authentication server the first user identification information with user identification information in a database of user identification information." Alcatel argues the term does not require construction. Microsoft argues the term means "determining on the authentication server if the user identification information input on the first node matches the user identification information contained in one of the user-specific entries." The parties dispute whether the "comparing" step determines whether the first user identification information matches user identification information in a database of user identification information.

The claims provide the context such that construction of the "comparing" step is not necessary. The asserted method claims contain a separate step of transmitting information if the first user identification information matches the user identification information located in the database. '830 Patent, col. 13:66-col. 14:20 (claiming method that comprises step of "transmitting [notification information] 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"); *id.* at col. 16:10-30 (claiming method that comprises steps of "transmitting from the authentication server to the authentication agent, the result of the comparison" and "transmitting from the authentication server to the authentication agent a list of network resources for which the user is authorized if the result is a match"); '090 Patent, col. 12:19-45, col. 15:11-34 (claiming method that comprises step of "transmitting [notification information] 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"). Thus, the conditional transmitting steps determine whether the result of the "comparing" step is that the first identification information matches user identification information in the database of user identification information.

The specifications disclose an identification verification process where the authentication server receives authentication information from an authentication agent. '830 Patent, col. 8:20-22. The authentication server then determines if the authentication information matches user identification information associated with a user-specific entry in user records. *Id.* at col. 8:22-26. If the authentication server finds a match, the authentication server may authorize the user if other conditions are met. *Id.* at col. 8:26-54. If the authorization server does not find a match, the authorization server does not authorize the user. *Id.* at col. 8:45-49.

The description in the specifications conflates the "comparing" and "transmitting" steps and does not limit the "comparing" step to determining whether the first user identification information matches user identification information in a database of user identification information. The determining, or finding, step in the specifications describes the "comparing" and conditional "transmitting" steps in the claims, as determination of a match requires the authentication server to compare data and, based on the result of the comparison, conclude whether the data matches. *See id.* at col. 8:20-29, col. 13:66-col. 14:20, col. 16:10-30. If the authentication server concludes the data matches, it transmits notification information to the authentication agent. *See id.* Thus, the specification does not redefine "comparing" as "determining [a] match[]."

In light of the foregoing, a lay jury will understand the term "comparing on the authentication server the first user identification information with user identification information in a database of user identification information." The Court has resolved the parties' claim-scope dispute and will not further define the term. *See* O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co., 521 F.3d 1351, 1362 (Fed.Cir.2008).

Entering on a First Node First User Identification Information

Claims 17 and 37 of the '830 Patent and claims 1 and 25 of the '090 Patent contain the term "entering on a first node first user identification information." Alcatel argues the term does not require construction. Microsoft contends "entering on a first node first user identification information" means "the user inputting the first user identification information on the first node." The parties dispute whether the user is required to input the first user identification information.

At the *Markman* hearing, Alcatel conceded that a user has to enter "first user identification information" at some point.FN2 *Alcatel USA Sourcing, Inc. v. Microsoft Corp.*, Cause No. 6:06cv499, Transcript of *Markman* hearing held on 7/8/2008, 28. This is consistent with the intrinsic record.

FN2. At the *Markman* hearing, the Court inquired what Alcatel's position on how much user input the "entering on a first node first user identification information" limitation requires. In response, Alcatel's counsel stated:

Alcatel's position is that the claim language is clear enough to understand; and that the entering does happen when the claim happens, but it doesn't necessarily have to happen every time a user sits down. For example, you might have connection to the network and then let's say your screensaver comes on. You sit down and you type in a password for the screensaver but you are already connected to the network. You are just typing in a password for a particular screensaver.

So while there does have to be an entering at some point, it certainly doesn't have to be every time the user sits down. The entering happens as part of the method. And a software maker or a company can decide how often they want to use this method because the more often you use it, obviously, the better your security. If you force someone to go through this kind of secure access every time they sit down; and if they are away for ten seconds, you blank out access, then it going to be very secure. You could also choose to use this method only once a day and have that be your level of security, but the claims don't require one way or the other. The claims let you use this method the extent you want to in order to maintain security.

Who or what performs claimed method steps is generally irrelevant to claim scope. *See Amstar Corp. v. Envirotech Corp.*, 730 F.2d 1476, 1482 (Fed.Cir.1984) ("[T]he law recognizes the irrelevance of apparatus distinctions in determining infringement of process claims."); *Int'l Glass Co. v. U.S.*, 187 Ct.Cl. 376, 408 F.2d 395, 400 (Ct.Cl.1969) ("A patented process is infringed only by unauthorized performance of substantially the same process steps in substantially the same way to accomplish substantially the same result. It is not necessary that the accused process be practiced with the same or substantially the same apparatus as disclosed by the patentee."); *Joy Techs., Inc. v. Flakt, Inc.*, 6 F.3d 770, 775 (Fed.Cir.1993) ("A method claim is directly infringed only by one practicing the patented method."). While the specification discloses that a user enters the first user identification information, the disclosed embodiments do not require a user to perform that method step. *E.g.*, '090 Patent, col. 8:14-16; *see also* Phillips, 415 F.3d at 1323-24; *Int'l Glass*, 408 F.2d at 400.

During prosecution of the parent application of the application that became the '830 Patent, the applicants distinguished their invention over U.S. Patent No. 5,721,780 (the "Ensor Patent"). Statements in the

prosecution history distinguish the applicant's invention from the prior art. The doctrine of prosecution disclaimer may narrow a claim term's ordinary meaning to one congruent with the scope surrendered in the prosecution history. *Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1323-24 (Fed.Cir.2003). Prosecution disclaimer may arise from an applicant's statements in an ancestor patent application if the ancestor application relates to the same subject matter as the claim language at issue. *Ormco Corp. v. Align Tech., Inc.*, 498 F.3d 1307, 1314 (Fed.Cir.2007). Generally, statements in a parent application will not disclaim subject matter claimed in the continuation application if the applications contain different claim language. *Invitrogen Corp. v. Clontech Labs., Inc.*, 429 F.3d 1052, 1078 (Fed.Cir.2005).

The applicant must unequivocally disavow a certain claim term meaning for the doctrine to apply. *Omega Eng'g*, 334 F.3d at 1324. If the applicant unequivocally disavows claim scope, the doctrine of prosecution disclaimer applies even if the disclaimer results in a negative claim limitation. *See N. Am. Container, Inc. v. Plastipak Packaging, Inc.*, 415 F.3d 1335 (Fed.Cir.2005) (affirming district court's construction of claim term "generally convex" to require "a majority of convex points along the inner wall and no concave points," as the applicant's statements in prosecution history disclaimed coverage of an inner wall with any concavity). Courts will not apply the doctrine of prosecution disclaimer where the alleged claim scope disavowal is ambiguous. *See Omega Eng'g*, 334 F.3d at 1324.

During prosecution of the parent of the application that became the '830 Patent, the Examiner rejected the claims under 35 U.S.C. s. 103, based in part on the Ensor Patent. Microsoft's Brief in Opposition to Alcatel's Opening Claim Constructions, Ex. 1, at 15-16. In response the applicants distinguished their invention over the Ensor Patent and stated:

While [the] Ensor [Patent] addresses security at the network level, albeit crudely, there is no teaching or suggestion to authenticate users. [The] Ensor [] [Patent's] security service relies instead on recognizing the identity of terminals. There is [no] consideration for who is using the terminals to gain network access. [The] Ensor [Patent] even criticizes a prior art user-based network login in the Background of the Invention and touts the supposed advantages of their alternate user-transparent approach.

Id. at Ex. 1, at 18-19.

The applicants subsequently quoted the Ensor Patent:

This [user identification] form of password security, however, suffers from the problem that it is dependent upon user-interaction. The user is first required to select or agree upon the password, and then memorize and provide the password to the server each time he desires to access the network. In doing so, many users write down the password in fear that they will forget it, and additionally, do not always ensure that their entry of the password is performed undetected. Accordingly, this type of security system provides the opportunity for someone to take advantage of the unwary user and steal his password in order to gain fraudulent access to the network.

Id. at Ex. 1, at 19 (quoting the Ensor Patent, col. 1:34-44).

Finally, the applicants stated "[the] Ensor [Patent] does not contemplate providing access to a selectable or personalized set of network nodes." Microsoft's Brief in Opposition to Alcatel's Opening Claim Constructions, Ex. 1, at 19.

In total, the applicants distinguished a system that did not obtain any information from the user. The applicants' statements, however, do not require the claimed invention to obtain all information from the user. All that is required is that the claimed invention consider who uses the computer that attempts to access the network.

In light of the foregoing, a lay jury will understand the term "entering on a first node first user identification information." The Court has resolved the parties' claim-scope dispute recognizing that both parties agree the user must enter first user identification information at some time and will not further construe the term. *See* O2 Micro, 521 F.3d at 1362.

Associating ... Each [User] With a Group of Nodes Represented by a Virtual Local Area Network Selected for the User

Claim 12 of the '830 Patent contains the term "associating ... each [user] with a group of nodes represented by a virtual local area network selected for the user." Alcatel contends the term does not require construction. Microsoft argues "associating ... each [user] with a group of nodes represented by the virtual local area network selected for the user" means "selecting a VLAN for each user and, based on the user's unique key, assigning to the user a group of nodes represented by the VLAN." The parties dispute FN3 whether "associating" requires the method to perform the steps of "selecting a VLAN for each user" and "assigning to the user a group of nodes represented by the VLAN."

FN3. Alcatel also contends "selected for the user" means "for which the user has access." The claim language does not require the user to have access to the group of nodes at the time of the association, but only requires that the group of nodes are selected for the user. '830 Patent, col. 13:17-27. A lay jury will understand "selected for the user," and the Court will not construe the term.

Microsoft's construction improperly narrows the claims. The claim language uses the term "associating," a broader term than "assigning." '830 Patent, col. 13:17-27. Additionally, the specification does not require assignment of a group of nodes to a user during the authentication process. *See id.* at Fig. 9, col. 11:22-45 (describing authentication process where authentication server transmits list of authorized network resources and time restrictions to authentication agent).

In addition, the claim does not require the active step of "selecting a VLAN," as the claim states the VLAN has already been selected for the user. *Id.* at col. 13:17-27. The specification also indicates the user authentication method does not require active selection of the nodes represented by a VLAN, as those nodes may have been selected before the association of the user with those nodes. *See id.* at col. 7:50-64 (stating network administrator can input user-specific entries which preferably include user identification information, which may include a password, and a list of authorized network resources).

A lay jury will understand the term "associating ... each [user] with a group of nodes represented by a virtual local area network selected for the user." The Court has resolved the parties' claim-scope dispute and declines to construe the term. *See* O2 Micro, 521 F.3d at 1362.

Prior to Establishing Communicability

Claim 12 of the '830 Patent contains the term "prior to establishing communicability." Alcatel contends the term means "before permitting access." Microsoft contends "prior to establishing communicability" should

be construed in the context of "prior to establishing communicability between the user and the group of nodes selected for the user" and argues this phrase means "prior to enabling communication between the user and the group of nodes selected for the user."

Claim 12 claims a user authentication method that comprises the step of "verifying in a login sequence for each of the plurality of users the user's unique user key prior to establishing communicability between the user and the group of nodes selected for the user." '830 Patent, col. 13:18-27. The specification indicates the invention authenticates a user, which requires verifying a user's unique user key, before it grants the user access to their personalized sets of network resources. *Id.* at Abstract; *see also id.* at col. 2:34-36; *id.* at col. 2:54-65 (stating "a service which requires that local users be authenticated before gaining access to personalized sets of network resources" accomplishes object of invention "to provide a service which grants user access to personalized sets of network resources upon verifying signature information"). Thus, in the context of the patent, "prior to establishing communicability" means "before permitting access."

Verifying in a Log-In Sequence for Each of the Plurality of Users the User's Unique User Key

Claim 12 of the '830 Patent contains the term "verifying a log-in sequence for each of the plurality of users the user's unique user key." Alcatel contends the term does not require construction. Microsoft argues the term means "for each user, presenting the user with a log-in challenge and comparing the response input by the user to the unique user key."

Microsoft's construction improperly limits the "verifying a log-in sequence for each of the plurality of users the user's unique user key" term. The specification discloses a verification process that compares a user's response to a log-in challenge with user identification information stored in the network. *Id.* at col. 2:42-46, col. 3:6-10. However, nothing in the intrinsic record limits the "verifying" step to this specific series of steps, and it would be improper to so limit the claims. *See Phillips*, 415 F.3d at 1323-24. The Court has resolved the parties' dispute and will not further define the term. *See O2 Micro*, 521 F.3d at 1362.

First User Identification Information

Claims 17 and 37 of the '830 Patent and claims 1, 3, 5, and 25 of the '090 Patent contain the term "first user identification information." Alcatel argues the term does not require construction. Microsoft contends "first user identification information" means "information known to the user that identifies the user to the communications network." The parties dispute whether the user must know the first user identification information and whether the "first user identification information" must identify the user to the communications network.

Nothing in the patents require the user to know the "first user identification information." The claims do not include a knowledge requirement. While the specifications indicates user identification information preferably includes a password, which is assumably known to the user, the specifications do not limit the invention. '830 Patent, col. 7:52-64; '090 Patent, col. 7:56-58.

Further, it is improper to limit the "first user information" to information that identifies a user to the communications network. The claims themselves explain how communications networks that employ the methods use the "first user identification information" to authenticate a user. *E.g.* '830 Patent, col. 13:66-col. 14:20 (claiming method that comprises steps of: "entering ... first user identification information"; "transmitting to an authentication agent ... 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 [notification information] ... if the first user identification information matches user identification information in the database of user identification information"). Thus, in light of the claims, there is no reason to specify the purpose of the "first identification information."

A lay jury will understand the term "first user identification information." The Court has resolved the parties' claim-scope dispute and declines to construe the term. *See* O2 Micro, 521 F.3d at 1362.

'799 Patent

Translation Rules that Resolve the Incompatibility of the Internal and External Address Realms

The asserted claims contains the term "translation rules that resolve the incompatibility of the internal and external address realms." Alcatel contends the term does not require construction. Microsoft contends the term means "a rule for translating an address valid in the internal address realm into an address valid in the external address realm, and for translating the address valid in the external realm into the address valid in the internal address realm." The parties dispute whether the claimed "translation rules" must include a rule that translates, in both directions, addresses valid in one realm into an address valid the other realm.

Microsoft's construction improperly limits the claims. Claim 1 claims a network address translation device that comprises, in part, "an address translator for translating addresses included in the headers or message packets incoming to and outgoing from the internal address realm in accordance with translation rules that resolve the incompatibility of the internal and external address realms." '799 Patent, col. 16:29-50. Thus, the claim indicates the network address translation device can use different rules for packets arriving to the internal address realm and packets departing from the internal address realm, so long as the applied rule resolves the incompatibility between the internal and external address realms. The dependant claims further limit the "translation rules" and what they accomplish. *Id.* at col. 16:57-col. 17:34.

The specification discloses types of translation rules. *Id.* at col. 9:12-47. These rules include address pairings for the internal and external realms and conditional translation rules based on the characteristics of a message, including its source and its destination. *Id.* at col. 9:14-46. For example, a translation rule could be formulated so the address translator checks the source address or the port of an incoming message and performs different steps depending on the address or port. *Id.* at col. 9:19-27. These conditional steps may include translating the address or discarding the packet. *Id.* Whatever the translation rules the address translator obeys, all the claims require is that the translation rules resolve the incompatibility of the internal and external address realms. *Id.* at col. 16:29-50.

Thus, the term "translation rules that resolve the incompatibility of the internal and external address realms" does not require a specific translation rule. Having resolved the parties' dispute, the Court will not construe the term. *See* O2 Micro, 521 F.3d at 1362.

'767 Patent

An Act of the Gateway

Claim 28 contains three disputed "an act of the gateway" limitations. Alcatel contends these limitations are step-plus-function limitations governed by 35 U.S.C. s. 112 para. 6. Microsoft argues these limitations are

not step-plus-function limitations and that the limitations do not require construction.

35 U.S.C. s. 112 para. 6 allows a patentee to claim a step for performing a recited function without recital of supporting acts, and such a claim is limited to acts described in the specification and equivalents thereof. In method claims, the use of the term "step for" raises a rebuttable presumption that 35 U.S.C. s. 112 para. 6 applies. *Masco Corp. v. U.S.*, 303 F.3d 1316, 1326 (Fed.Cir.2002) (citing *Greenberg v. Ethicon Endo-Surgery, Inc.*, 91 F.3d 1580, 1583 (Fed.Cir.1991)). However, even where a drafter employs "step-for" language, 35 U.S.C. s. 112 para. 6 governs construction of the limitation "only when steps plus function *without acts* are present." *Masco*, 303 F.3d at 1326 (quoting *O.I. Corp. v. Tekmar Co.*, 115 F.3d 1576, 1582 (Fed.Cir.1997)) (emphasis in original).

Similarly, when a claim does not employ "step for" language, courts presume 35 U.S.C. s. 112 para. 6 does not apply. *See Masco*, 303 F.3d at 1326; *Greenberg*, 91 F.3d at 1583; *CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1369 (Fed.Cir.2002). The presumption "is a strong one that is not readily overcome." *See Lighting World, Inc. v. Birchwood Lighting, Inc.*, 382 F.3d 1354, 1362 (Fed.Cir.2004). The presumption is overcome if the claim provides steps and functions without acts. *See Masco*, 303 F.3d at 1326.

Claim 28 contains three disputed "an act of the gateway" limitations: "an act of the gateway identifying a device module that corresponds to the device type, network type, or both associated with the address of the intended remote destination device"; "an act of the gateway using the identified device module to manipulate the received data or message"; and "an act of the gateway transmitting the data or message from the gateway through the one or more remote networks to the intended remote destination device." '767 Patent, col. 22:3-42. Each limitation does not use "step for" language, and each limitation recites an act.

Thus, Alcatel has not rebutted the presumption that the "an act of the gateway" limitations are not step-plus-function limitations. *See Masco*, 303 F.3d at 1326. Having resolved the parties' dispute, the Court will not further construe the disputed "an act of the gateway" limitations. *See O2 Micro*, 521 F.3d at 1362.

A Step For Using the Identified Device Module / A Step for Transmitting the Data or Message

Claims 1 and 3 contain the disputed "step for" limitations. Alcatel contends the terms are step-plus-function limitations. Microsoft contends the terms are not step-plus-function terms and that the limitations do not require construction.

In method claims, the use of the term "step for" raises a rebuttable presumption that 35 U.S.C. s. 112 para. 6 applies. *Masco*, 303 F.3d 1316, 1326 (Fed.Cir.2002) (citing *Greenberg*, 91 F.3d at 1583). However, even where a drafter employs step-plus-function language, 35 U.S.C. s. 112 para. 6 governs construction of the limitation "only when steps plus function *without acts* are present." *Masco*, 303 F.3d at 1326 (quoting *O.I. Corp.*, 115 F.3d at 1582) (emphasis in original).

Claims 1 and 3 contain the following disputed "step for" limitations: "a step for using the identified device module to manipulate the data or message so that the data or message is then transmitted from the gateway through the one or more remote networks to the intended remote destination device using a protocol and a format recognized by the intended remote destination device, irrespective of differences in the originating and receiving protocols"; and "a step for transmitting the data or message over the one or more remote networks to the intended remote destination device using the protocol and the format recognized by the intended remote destination device." '767 Patent, col. 15:64-col. 16:33, col. 16:39-46.

The claims recite the acts of "using the identified device module to manipulate the data or message" and "transmitting the data or message over the one or more remote networks to the intended remote destination device." Thus, the limitations are not step-plus-function limitations governed by 35 U.S.C. s. 112 para. 6. *Masco*, 303 F.3d at 1326. Having resolved the parties' dispute, the Court will not further construe the "step for using" and "step for transmitting" limitations. *See O2 Micro*, 521 F.3d at 1362.

Device Module(s)

Claims 1, 11, and 28 contain the term "device module." Microsoft contends "device module" means "hardware and/or executable code." Alcatel claims the term does not require construction. Alcatel argues Microsoft's construction eliminates the "device" from "device module."

One of ordinary skill in the art would understand, after a review of the intrinsic record, that a "device module" has the capabilities of a device driver and a network driver. The claims indicates a "device module" has the ability to manipulate the format of data or a message for a particular device and can convert from one network protocol to another. '767 Patent, col. 15:64-col. 16:33, col. 17:57-col. 18:27 (describing "a plurality of device modules at the gateway for manipulating data and messages into any of a plurality of formats or protocols for diverse device and network types"); *id.* at col. 22:3-42 (describing "a device module that corresponds to a device type, network type, or both associated with the address of the intended remote destination device"). In addition, the specification uses the term "device module" synonymously with device driver module. '767 Patent, Fig. 4, col. 10:42-52, col. 12:38-60, col. 13:19-67. Thus, "device module" means "a device driver and/or network driver."

Intended

Claim 28 contains the term "intended remote destination device." Alcatel argues the term "intended" is indefinite and claim 28 is invalid. Microsoft contends the term "intended" is definite and does not require construction.

A claim is invalid as indefinite under 35 U.S.C. s. 112 para. 2 if the claim fails to particularly point out and distinctly claim the subject matter that the applicant regards as the invention. The primary purpose of the definiteness requirement is to ensure public notice of the scope of the patentee's legal protection, such that interested members of the public can determine whether or not they infringe. *Halliburton Energy Servs., Inc. v. M-I, LLC*, 514 F.3d 1244, 1249 (Fed.Cir.2008); *Oakley, Inc. v. Sunglass Hut Int'l*, 316 F.3d 1331, 1340 (Fed.Cir.2003) (quoting *All Dental Prodx, LLC v. Advantage Dental Prods., Inc.*, 309 F.3d 774, 779-80 (Fed.Cir.2002)). Thus, the definiteness inquiry focuses on how a skilled artisan would understand the claims, and courts apply general claim construction principles in their efforts to construe allegedly indefinite claim terms. *Datamize, LLC v. Plumtree Software, Inc.*, 417 F.3d 1342, 1348 (Fed.Cir.2005); *Young v. Lumenis, Inc.*, 492 F.3d 1336, 1346 (Fed.Cir.2006).

A claim is indefinite only if the claim is "not amenable to construction" or "insolubly ambiguous." *Datamize*, 417 F.3d at 1347; *Halliburton*, 514 F.3d at 1249 ("The common thread in all of [the cases where the court concluded a claim was indefinite] is that claims were only held indefinite only where a person of ordinary skill in the art could not determine the bounds of the claim, i.e., the claims were insolubly ambiguous."). An accused infringer will prevail on an indefiniteness challenge if it "shows by clear and convincing evidence that a skilled artisan could not discern the boundaries of the claim based on the claim language, the specification, and the prosecution history, as well as her knowledge of the relevant art area."

Halliburton, 514 F.3d at 1249-50. Courts presume issued claims are valid, and a court may only find a claim indefinite only if reasonable efforts at claim construction prove futile. *Datamize*, 417 F.3d at 1347-48. Thus, a claim term is definite if it can be given any reasonable meaning. *See id.* at 1347.

A claim term is not indefinite solely because the term presents a difficult claim construction issue. *Exxon Research & Eng'g Co. v. U.S.*, 265 F.3d 1371, 1375 (Fed.Cir.2001). Similarly, a claim is not indefinite merely because the claim employs words of degree to define the invention or does not define the invention with mathematical precision. *BJ Servs. Co. v. Halliburton Energy Servs. , Inc.*, 338 F.3d 1368, 1372 (Fed.Cir.2003); *Oakley*, 316 F.3d at 1341-42, *Exxon*, 265 F.3d at 1377-80; *see also Andrews Corp. v. Gabriel Elecs., Inc.*, 847 F.2d 819, 821-22 (Fed.Cir.1988). The amount of precision necessary to define a claim is a function of the claimed subject matter. *See Miles Labs., Inc. v. Shandon Inc.*, 997 F.2d 870, 875 (Fed.Cir.1993); *Exxon*, 265 F.3d at 1378-79. Whether a claim is precise enough depends on how a skilled artisan would read the claim in light of specification, the prosecution history, relevant extrinsic evidence, and her knowledge of the relevant art. *See Halliburton*, 514 F.3d at 1249-50; *Exxon*, 265 F.3d at 1378-79; *Phillips*, 415 F.3d at 1314-1318.

Alcatel has not shown by clear and convincing evidence that the "intended remote destination device" term is indefinite. In the context of the claims, the intended remote destination device refers to the association between the message and device to which it is destined. '767 Patent, col. 2:54-56, col. 22:3-42. Alcatel argues there is no objective way to determine which remote destination device is the intended remote destination device. However, which remote destination device is the "intended" remote destination device is immaterial to the scope of the claims. All that is required is that a message is intended for at least one remote destination device. *Id.* at col. 22:3-42. While the choice of the intended remote destination device is a subjective one, which remote destination device is the "intended" remote destination device is immaterial, and infringement does not completely depend upon a person's remote destination device choice. *See Datamize*, 417 F.3d at 1350.

Thus, the claim term "intended" is not indefinite. Having resolved the parties' dispute, the Court will not construe the term. *See O2 Micro*, 521 F.3d at 1362.

Means-Plus-Function Limitations

Claim 11 contains three disputed means-plus-function limitations: "means for determining a specific address for each received data or message so that a destination device or network type may be identified for the received data or message"; "means for identifying from a plurality of device modules at the gateway for manipulating received data and messages into any of a plurality of formats or protocols for diverse device and network types, a device module associated with each received data or message's destination device type, network type, or both"; and "means for manipulating each received data or message so that each received data or message is then transmitted from the gateway through one or more remote networks to an intended remote destination device using a protocol and a format recognized by the intended remote destination device, irrespective of differences in the originating and receiving protocols." The parties agree each limitation is a means-plus-function limitation but disagree on the recited functions and the corresponding structures.

"The first step in construing [a means-plus-function] limitation is a determination of the function of the means-plus-function limitation." *Medtronic*, 248 F.3d at 1311. "The phrase 'means for' generally invokes 35 U.S.C. s. 112 para. 6, and is typically followed by the recited *function and claim limitations*." *Lockheed*

Martin Corp. v. Space Systems/Loral, Inc., 324 F.3d 1308, 1319 (Fed.Cir.2003) (citing Greenberg, 91 F.3d at 1584) (emphasis in original). Courts may not improperly narrow or limit the recited function beyond the scope of the claim language. Lockheed Martin, 324 F.3d at 1319 (citing Micro Chem. Inc. v. Great Plains Chem. Co., 194 F.3d 1250, 1258 (Fed.Cir.1999)). Conversely, courts may not ignore the clear limitations in the claim language to improperly broaden the scope of the function and must construe the recited function to include limitations contained in the claim language. *See* Lockheed Martin, 324 F.3d at 1319.

After the Court determines and construes the recited function, the Court must identify the corresponding structure in the specification. Medtronic, 248 F.3d at 1311. To qualify as sufficient structure, the disclosed structure must correspond to the recited function. Default Proof Credit Card Sys., Inc. v. Home Depot U.S.A., Inc., 412 F.3d 1291, 1298 (Fed.Cir.2005). A structure disclosed in the specification qualifies as "corresponding" structure only if the specification or prosecution history clearly link or associate that structure to the recited function. *Id.* The corresponding structure does not need to include all necessary elements to enable the claimed invention to operate, but the structure must include all structure that is clearly linked to performing, and actually performs the recited function. Braun Med., 124 F.3d at 1424-25. Courts consider the entire specification to determine the structure that is capable to perform the recited function. Default Proof, 412 F.3d at 1298.

The corresponding structure for a means-plus-function claim limitation with a computer-implemented function is limited to the algorithm disclosed in the specification. Harris Corp. v. Ericsson Inc., 417 F.3d 1241, 1253 (Fed.Cir.2005); WMS Gaming, Inc. v. Int'l Game Tech., 184 F.3d 1339, 1349 (Fed.Cir.1999) ("In a means-plus-function claim in which the disclosed structure is a computer, or microprocessor, programmed to carry out an algorithm, the disclosed structure is not the general purpose computer, but rather the special purpose computer programmed to perform the disclosed algorithm."). Courts allow a patentee to express an algorithm in any understandable terms, which includes mathematical formulas, prose, flow charts, or any other manner that provides sufficient structure. *See* Finisar Corp. v. DirectTV Group, Inc., 523 F.3d 1323, 1340 (Fed.Cir.2008).

Means for Determining a Specific Address for Each Received Data or Message so that a Destination Device or Network Type May Be Identified for the Received Data or Message

The parties agree the recited function is "determining a specific address for each received data or message so that a destination device or network type may be identified for the received data or message." Microsoft argues the corresponding structure is "one or more processors which process information such as a telephone number, a uniform resource locator (URL), an address in a lookup table or any other information source, and equivalents thereof." Alcatel argues the corresponding structure is "message processor 406 and the corresponding hardware and/or software that performs the act of reading the address 281; locator module 408; mass memory 410, magnetic hard disk drive 27, the system memory 22, the removable magnetic disk 29, or the removable optical disk 31; address table 500.

The parties agree a processor is part of the corresponding structure. The disclosed processor in the specification is message processor 406. '767 Patent, Fig. 4, col. 10:36-col. 11:14. The message processor 406 determines the specific address of the message in two instances: (1) if the addressed passed to message processor 406 is a specific address associated with the data or message; and (2) if the address passed to message processor 406 is a generic address associated with the data or message. *Id.* at col. 10:65-col. 11:14. In each instance, the corresponding structure the performs the recited function contains different elements.

A specific address is an address which, by itself, comprises enough information to properly route the associated data or message over a remote network to a remote device. Id. at col. 8:55-58. Examples of specific addresses are telephone numbers and URLs. Id. at col. 8:58-60. If the address associated with the data or message is a specific address, message processor 406 determines the specific address by reading the data or message. Id. Thus, the structure that "determin[es] a specific address for each received data or message so that a destination device or network type may be identified for the received data or message" is message processor 406 programmed to read the address from the message. Harris, 417 F.3d at 1253; WMS Gaming, 184 F.3d at 1349.

A generic address is an address which requires the aid of a reference source to properly route the associated data or message to a remote device. '767 Patent, col. 8:65-67. An example of a generic address is "John Doe's home phone number in Tyler," which may be sufficient to properly route data or a message to John Doe's home phone only after looking up John Doe's home phone number in an address book or the Tyler phonebook. Id. at col. 8:67-col. 9:3.

In this instance, message processor 406 reads the generic address and looks up the specific address associated with the generic address in a table or other information source. Id. at col. 9:3-8. To perform the function, message processor 406 transmits the data or message to locator module 408 associated with the mass memory 410. Id. at col. 11:5-8. The locator module 408 reads the specific address from a lookup table stored in the mass memory 410 and provides that address to message processor 406. Id. at col. 11:12-14, col. 11:20-27. Thus, the structure that "determin[es] a specific address for each received data or message so that a destination device or network type may be identified for the received data or message" is message processor 406 using locator module 408 that uses a lookup table stored in mass memory 410. Mass memory 410 may be any suitable device, such as a magnetic hard disk drive 27, system memory 22, a removable magnetic disk 29, or a removable optical disk 31. Id. at col. 11:8-12.

In total, the corresponding structure that performs the recited function is "(1) message processor 406 and the corresponding software that reads the address from the message; or (2) message processor 406 accessing the address using a locator module 408 that uses a lookup table stored in a mass memory 410, which may be any suitable storage device, such as the system memory 22, a hard disk 27, removable magnetic disk 29, or removable optical disk 31."

Means for Identifying From a Plurality of Device Modules at the Gateway for Manipulating Received Data and Messages Into Any of a Plurality of Formats or Protocols for Diverse Device and Network Types, a Device Module Associated with Each Received Data or Message's Destination Device Type, Network Type, or Both

The parties dispute both the recited function and corresponding structure. Microsoft argues the recited function is "identifying from a plurality of device modules ... a device module associated with each received data or message's destination device type, network type, or both." Alcatel argues the recited function is "identifying from a plurality of device modules at the gateway for manipulating received data and messages into any of a plurality of formats or protocols for diverse device and network types, a device module associated with each received data or message's destination device type, network type, or both." The parties dispute whether the "at the gateway for manipulating received data and messages into any of a plurality of formats or protocols for diverse device and network types" language is part of the recited function.

The "means for identifying" structure forms part of the claimed gateway means. Id. at col. 17:57-col. 18:27.

As the claim indicates the "means for identifying" identifies device modules at the gateway, as opposed to device modules located elsewhere, the recited function must include that language. *See* Lockheed Martin, 324 F.3d at 1319. Thus, the recited function is "identifying from a plurality of device modules at the gateway for manipulating received data and messages into any of a plurality of formats or protocols for diverse device and network types, a device module associated with each received data or message's destination device type, network type, or both."

Microsoft contends the corresponding structure is "one or more processors which process executable code and/or accesses, for example, an identifier table and/or an address table, and equivalents thereof." Alcatel contends the corresponding structure is "executable code and hardware for performing the act of identifying the device driver associated with the specific identification of the remote device 270 by simply reading the specific identification of the remote device 270 from the message 280; identification table; locator module 408; message processor 406 ."

Similar to the "means for determining" limitation, the specification describes two operations of the "means for identifying." If the message or data include a specific identification of a remote device, the "means for identifying" extracts the device type from the message and uses executable code or hardware to identify the appropriate device module. '767 Patent, col. 11:67-col. 12:7. In this instance, the corresponding structure is a processor, which the specification discloses as message processor 406, programmed with software that reads the device type from the message and identifies the driver that corresponds to the device-type. Harris, 417 F.3d at 1253; WMS Gaming, 184 F.3d at 1349.

If the message or data does not include a specific identification of a remote device, the "means for identifying" obtains the device type of the remote device using the address associated with the data or message. If the address associated with the data or message is a specific address, message processor 406 provides the specific address of the device to locator module 408 to look up the device type of the remote device in mass memory 410. '767 Patent, col. 12:8-13. Locator module 408 uses a data structure that represents an identification table to look up the device type of the remote device. *Id.* If the address associated with the data or message is a generic address, the system obtains the corresponding specific address and, using the specific address in the manner described above, obtains the device type of the remote device. *Id.* at col. 12:13-17.

In both instances, locator module 408 provides the device type of the remote device to message processor 406. *Id.* at col. 12:28-31. Identification of the device type implicitly identifies the device module. *Id.* at col. 12:31-37; *id.* at col. 11:58-62 ("[T]he identity of the device module has a well known association with the identity of the device."). Thus, where the message or data does not include a specific identification of a remote device, the corresponding structure is message processor 406 accessing the device type using locator module 408 that uses a lookup table in mass memory 410.

In total the corresponding structure that performs the recited function is "1) message processor 406 and the corresponding software that reads the device type from the message and identifies the driver corresponding to the device type; or 2) message processor 406 accessing the device type using a locator module 408 that uses a lookup table stored in mass memory 410, which may be any suitable storage device, such as the system memory 22, a hard disk 27, removable magnetic disk 29, or removable optical disk 31."

Means for Manipulating Each Received Data or Message so that Each Received Data or Message is then Transmitted from the Gateway Through One or More Remote Networks to an Intended Remote

Destination Device Using a Protocol and a Format Recognized by the Intended Remote Destination Device, Irrespective of Differences in the Originating and Receiving Protocols

The parties agree the recited function is "manipulating each received data or message so that each received data or message is then transmitted from the gateway through one or more remote networks to an intended remote destination device using a protocol and a format recognized by the intended remote destination device, irrespective of differences in the originating and receiving protocols." Microsoft contends the corresponding structure is "one or more processors which process executable code and/or uses the hardware associated with the identified device module, and equivalents thereof." Alcatel argues the corresponding structure is "executable code and hardware for transporting the message 280 from memory location to memory location between each manipulation; message object 248; message processor 406; device module library 414; device driver interface 412."

The specification indicates modules manipulate the message. *Id.* at col. 11:50-56; *id.* at col. 12:38-41 ("[I]t may be necessary to identify the network driver module that can manipulate the message 280 to be in a format recognizable by the remote device 270."); *id.* at col. 13:27-30 ("The message 280 is then provided as the message object 428 to the appropriate device module through the device driver interface 412. The device module then manipulates the message 280 to be in a format recognized by the remote device 270...."); *id.* at col. 14:28-32 ("Ultimately, after manipulation by the appropriate device module, and possible manipulation by appropriate encryption modules, and other modules as desired, the message 280 is in a format that a remote device 270 or 271 can handle."); *see also id.* at col. 15:64-col. 16:33, col. 17:57-col. 18:27 (describing "a plurality of device modules at the gateway for manipulating data and messages into any of a plurality of formats or protocols for diverse device and network types"). Of these modules, the specification only clearly links the identified device module as necessary to manipulate the data or message into a format recognized by the intended remote destination device.FN4 *Id.* at col. 11:50-56, col. 13:27-30. These modules are software called by or executed on message processor 406. *Id.* at col. 10:36-57; *id.* at col. 13:19-47.

FN4. The specification also states "it may be necessary to identify the network driver module that can manipulate the message to be in a format recognizable by the remote device." *Id.* at col. 12:38-41 (internal references to Figs. 2 and 3 omitted). To the extent a network driver module is corresponding structure, it is unnecessary to include a network driver module as corresponding structure, as the construction of device module covers a network driver.

The specification indicates the "means for manipulating" may include executable code or hardware to transfer the message from memory location to memory location between manipulations. *Id.* at col. 11:41-44. A message object may be used instead of the code or hardware that transfers the message from memory location to memory location such that the message resides at the same memory location for each manipulation. *Id.* at col. 11:44-49. However, regardless of the approach, the executable code, hardware, and message object, while necessary to perform the recited function, do not manipulate the message and are not corresponding structure. Default Proof, 412 F.3d at 1298 ("While corresponding structure need not include all things necessary to enable the claimed invention to work, it must include all structure that actually performs the recited function."); *Asyst Tech., Inc. v. Empak, Inc.*, 268 F.3d 1364, 1370 (Fed.Cir.2001) ("Structural features that do not actually perform the recited function do not constitute corresponding structure and thus do not serve as claim limitations.").

In light of the foregoing, the corresponding structure is "message processor 406, the software that executes the identified device module, and the identified device module." Harris, 417 F.3d at 1253; WMS Gaming, 184 F.3d at 1349.

Identifying ... a Device Module Associated With [that Corresponds to] the Device Type, Network Type, or Both

Claims 1 and 28 contain the term "identifying ... a device module associated with [that corresponds to] the device type, network type, or both." The term appears in limitations Alcatel alleges are step-plus-function limitations, and, outside that context, Alcatel argues the term does not require construction. Microsoft argues "identifying ... a device module associated with [that corresponds to] the device type, network type, or both" means "one or more processors identifies the device module associated with the device type, network type, or both by for example, processing executable code and/or accessing, for example, an identifier table and/or an address table."

As noted above, the specification describes two ways the system identifies the device module depending on whether the device type of the remote device resides in the data or message. *See id.* at col. 11:67-col. 12:37. Both of these approaches require a processor to determine the corresponding device module. *Id.* Thus, "identifying ... a device module associated with [that corresponds to] the device type, network type, or both" means "one or more processors determine the device module that corresponds to the device type, network type, or both."

Originating Protocols / Receiving Protocols

Claims 1, 11, and 28 contain the terms "originating protocols" and "receiving protocols." Microsoft contends "originating protocols" means "a set of rules that governs the way the devices communicate or exchange data within the originating network." Alcatel argues "originating protocols" means "a protocol distinct from the receiving protocol that the receiving device cannot interpret." Microsoft argues "receiving protocols" means "a set of rules that governs the way the devices communicate or exchange data within the remote network." Alcatel argues "receiving protocols" means "a protocol distinct from the originating protocol that the originating device cannot interpret." The parties dispute whether the "originating protocols" and "receiving protocols" must be distinct from one another, whether the originating device can interpret receiving protocols, and whether the receiving device can interpret originating protocols.

The specification describes protocols as sets of rules that govern the way computers communicate or exchange data over a network. *Id.* at col. 1:14-23. This description comports with extrinsic evidence that defines "protocol" as "a specific set of rules, procedures or conventions relating to format and timing of data transmissions between two devices." NEWTON'S TELECOM DICTIONARY 484 (11th ed.1996). The claims and specification indicate network devices within the originating network utilize the "originating protocol" to communicate with each other and computers within the receiving network utilize the "receiving protocol" to communicate with each other. '767 Patent, col. 1:14-23, col. 7:55-59, col. 9:16-24.

The claims specify that at least some of the "receiving protocols" are different from the "originating protocols." *Id.* at col. 15:64-col. 16:33, col. 17:57-col. 18:27, col. 22:3-42. However, the claims do not require all the originating and receiving protocols be different. Further, the specification does not foreclose on the possibility that some originating and receiving protocols are utilized by both the originating and receiving networks. *See id.* at col. 1:46-49.

Thus, "originating protocols" means "a set of rules that governs the way the devices communicate or exchange data within the originating network." "Receiving protocols" means "a set of rules that governs the way the devices communicate or exchange data within the remote network."

'273 Patent

Message Server / Data-Centric Network Server / Telephony-Centric Network Server

The asserted claims contain the terms "message server," "data-centric network server," and "telephony-centric network server." The parties' constructions raise two disputes: whether the "message server" includes "translation logic and software" and whether a "server" is limited to a single computer.

Translation Logic and Software

The patent indicates translation logic and software reside in the "message server." The specification explains the "message server," which does not appear to have an ordinary meaning outside the context of the '273 Patent, "includes translation logic and special-purpose software to translate voice-to-text and text-to-voice so that a message can be seamlessly entered, transmitted, and received." *Id.* at col. 15:31-34. As the "message server" performs the translation, the originating and receiving devices do not require special-purpose translation logic or software to send and receive messages. *Id.* at col. 15:41-44. This benefit of the "message server," according to the specification, overcomes obstacles in the prior art. *Id.* at col. 14:8-17. Thus, one of ordinary skill in the art would understand translation logic and software reside in the "message server."

Server

The asserted claims are open-ended and contain the terms "a message server," "a data-centric network server," and "a telephony-centric network server." *Id.* at col. 21:53-67, col. 22:64-col. 23:13. In patent parlance, the terms "a" and "the" carry the presumptive meaning of "one or more" when used in open-ended claims that contain the transitional phrase "comprising." *ReedHycalog UK, Ltd. v. Baker Hughes Oilfield Operations Inc.*, No. 6:06 CV 222, 2007 WL 3001423, at * 18 (Davis, J.) (citing *Free Motion Fitness, Inc. v. Cybex Int'l, Inc.*, 423 F.3d 1343, 1350-51 (Fed.Cir.2005)). This presumption is especially strong. *Baldwin Graphic Sys., Inc. v. Siebert, Inc.*, 512 F.3d 1338, 1342 (Fed.Cir.2008) ("That 'a' or 'an' can mean 'one or more' is best described as a rule, rather than merely as a presumption or even a convention."). To overcome the presumption, the patent must reveal the patentee's clear intent to limit "a" or "an" to "one." *Id.* at 1342 (citing *KCJ Corp. v. Kinetic Concepts, Inc.*, 223 F.3d 1351, 1356 (Fed.Cir.2003)).

Nothing in the specification indicates a "server" is limited to a single computer or device. Further, the specification indicates the "message server" and "data-centric network server" are located at a networks operations center, which commonly involve multiple computers that operate as servers. *See* '273 Patent, Fig. 4, col. 14:23-28. Thus, a "server" is not limited to a single computer.

For the abovementioned reasons, "message server" means "one or more computers that both provide services for processing messages and that contain translation logic and software," "data-centric network server," means "one or more computers connected to a data-centric network that provide services over the data-centric network," and "telephony-centric network server" means "one or more computers connected to a telephony-centric network that provide services to the telephony-centric network."

Translating the Message Into

Claims 17 and 35 contain the term "translating [translate] the message into." Microsoft contends "translating [translate] the message into" does not require construction. Alcatel argues the term means "translating [translate] the message from a format incompatible with the receiving device to." The parties dispute whether the format of the pre-translated message must be incompatible with the receiving device.

Alcatel's construction overly limits the claim. The claims only contain the "translating" function and do speak to the format of the original message. *Id.* at col. 21:53-67, col. 22:64-13. Nothing in the claims or the specification requires the format of the original message to be incompatible with the receiving device. The intrinsic record does not disclaim a receiving device that is compatible with multiple message formats and nothing in the intrinsic record requires translation only when the receiving device is not compatible with the format of the original message.

A lay jury will understand the term "translating [translate] the message into." Having resolved the parties' dispute, the Court will not construe "translating [translate] the message into." *See O2 Micro*, 521 F.3d at 1362.

CONCLUSION

For the foregoing reasons, the Court interprets the claim language in this case in the manner set forth above. For ease of reference, the Court's claim interpretations are set forth in a table as Appendix B. The claims with the disputed terms in bold are set forth in Appendix A.

So **ORDERED**.

APPENDIX A

U.S. Pat. No. 6,339,830

12. A user authentication method for a communication network having a plurality of nodes, the method comprising: **associating based on a unique user key each of a plurality of users of the network with a group of nodes represented by a virtual local area network selected for the user;** and **verifying in a log-in sequence for each of the plurality of users the user's unique user key prior to establishing communicability** between the user and the group of nodes selected for the user.

17. 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.

24. A user authentication system for a communication network comprising: a first node for entering user identification information; a second node for receiving the user identification information from the first node and comparing for a match the user identification information with user identification information in a database of user identification information; and a port on the second node that is authenticated upon a match for allowing communication between the first node and a group of nodes associated with the user identification information, and is not authenticated upon a mismatch, thereby failing to establish communication between the first node and other nodes, wherein the group of nodes is associated with a **virtual local area network**.

37. 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**; transmitting from the authentication server to the authentication agent, the result of the comparison; transmitting from the authentication server to the authentication agent a list of network resources for which the user is authorized if the result is a match; and associating a list of network resources with the first node if the result is a match.

U.S. Pat. No. 6,661,799

1. A network address translation device for facilitating message packet communication between a first application having an internal address valid in an internal address realm and one or more applications in an external address realm, said internal address realm having available to it a set of available addresses valid for use in the external address realm, comprising: an address translator for translating addresses included in the headers of message packets incoming to and outgoing from the internal address realm in accordance with **translation rules that resolve the incompatibility of the internal and external address realms**; an address manager for establishing and storing the translation rules, said address manager having access to the set of available addresses valid for use in the external address realm; and a control channel communicating with the address manager for receiving from the first application a service request message for establishing in response to the first application's service request a translation rule specified by the first application.

2. The network address translation device of claim 1, wherein the first application specifies that the translation rule to be established associates the first application's internal address with an available external address and the first application has access to the associated available external address as data for an outgoing message packet.

3. The network address translation device of claim 1 wherein the first application specifies that the translation rule to be established associates the first application's internal address with an available external address that is a particular WP address or within a specified range of IP addresses.

4. The network address translation device of claim 1 wherein the first application specifies that the translation rule is one of two or more translation rules applicable to an incoming message packet, where the selection of which translation rule is applied is contingent on address information in the incoming message packet.

8. The network address translation device of claim 1 wherein the internal address realm is a private network and the external address realm is the Internet and the address manager establishes a translation rule by associating an address valid in the private network realm with an address valid in the Internet.
9. The network address translation device of claim 4, wherein the selection of which translation rule is applied is made in response to the presence or absence of specified originating address information in the incoming message.
12. The network address translation device of claim 3, wherein the translation rule to be established forces the outgoing message packet to have a destination address in a transit network.
13. The network address translation device of claim 3, wherein the translation rule to be established forces at least a portion of the packet communication between the first application and the second application to pass through a specified network.
14. A method for facilitating message packet communication between a first application having an internal address valid in an internal address realm and one or more applications in an external address realm, said internal address realm having available to it a set of addresses valid for use in the external address realm, comprising: providing the internal address realm with a network address translation device having an address translator for translating addresses included in the headers of message packets incoming to and outgoing from the internal address realm in accordance with **translation rules that resolve the incompatibility of the internal and external address realms**; providing an address manager for establishing and storing the translation rules, said address manager having access to the set of available addresses valid for use in the external address realm; and providing a control channel communicating with the address manager for receiving from the first application a service request message for establishing in response to the first application's service request a translation rule specified by the first application.
15. The method of claim 14, wherein the step of providing a control channel comprises receiving from the first application a request that specifies that the translation rule to be established associates the first application's internal address with an available external address and providing the first application access to the associated available external address as data for an outgoing message packet.
16. The method of claim 14 wherein the step of providing a control channel for receiving a request comprises receiving from the first application a request that specifies that the translation rule to be established associates the first application's internal address with an available external address that is a particular IP address or within a specified range of IP addresses.
17. The method of claim 14 wherein the step of providing a control channel for receiving a request comprises receiving from the first application a request that the translation rule is one of two or more translation rules applicable to an incoming message packet, where the selection of which translation rule is applied is contingent on address information in the incoming message packet.
18. The method of claim 14 wherein the step of providing a control channel for receiving a request comprises receiving from the first application a request for a translation rule for a terminating address.
19. The method of claim 14 wherein the step of providing a control channel for receiving a request comprises receiving from the first application a request for a translation rule for an originating address.

21. The method of claim 14 wherein the internal address realm is a private network and the external address realm is the Internet and the step of providing an address manager comprises providing an address manager that establishes a translation rule by associating an address valid in the private network realm with an address valid in the Internet.

22. The method of claim 17, wherein step of providing a control channel for receiving a request comprises receiving from the first application a request that the translation rule is one of two or more translation rules applicable to an incoming message, where the selection of which translation rule is applied is made in response to the presence or absence of specified originating address information in the incoming message.

25. The method of claim 16, wherein the step of providing a control channel for receiving a request comprises receiving from the first application a request that the translation rule to be established forces the outgoing message packet to have a destination address in a transit network.

26. The method of claim 16, wherein step of providing a control channel for receiving a request comprises receiving from the first application a request that the translation rule to be established forces at least a portion of the packet communication between the first application and the second application to pass through a specified network.

U.S. Pat. No. 6,674,767

1. In a networked computer system that includes one or more originating devices for originating data or messages, and wherein the originating devices are logically connected to and communicate using one or more **originating protocols** with one or more originating networks logically connected to a gateway, the gateway in turn being logically connected to one or more remote networks that are logically connected to and that communicate to one or more remote destination devices using one or more **receiving protocols**, at least some of which are different from the **originating protocols**, a method of forwarding the originating data or messages from the one or more originating devices through the gateway to the one or more remote destination devices notwithstanding the differences used in the originating and **receiving protocols**, the method comprising the following: a step for generating, at one or more of the originating devices, data or a message intended for at least one remote destination device; a step for communicating the generated data or message through one or more originating networks to a gateway using the one or more of the **originating protocols**; a step for identifying at the gateway a device type, a network type, or both, for the at least one remote destination device; a step for identifying, from a plurality of **device modules** at the gateway for manipulating data and messages into any of a plurality of formats or protocols for diverse device and network types, a **device module** associated with the device type, network type, or both, identified for the intended remote destination device; and a **step for using the identified device module to manipulate the data or message so that the data or message is then transmitted from the gateway through the one or more remote networks to the intended remote destination device using a protocol and a format recognized by the intended remote destination device, irrespective of differences in the originating and receiving protocols.**

3. The method of claim 1, further comprising the following: **a step for transmitting the data or message over the one or more remote networks to the intended remote destination device using the protocol and the format recognized by the intended remote destination device.**

11. A networked computer system for permitting data or messages that are originated using one or more **originating protocols** to be communicated across one or more networks to a remote destination that uses a receiving protocol different from the **originating protocols**, comprising: one or more originating devices for originating data or messages using one or more **originating protocols**; one or more originating networks logically connected to the one or more originating devices and which communicate therewith using the one or more **originating protocols**; gateway means logically connected to the one or more originating devices through the one or more originating networks, for receiving the originated data or messages using the one or more **originating protocols**, said gateway means comprising: **means for determining a specific address for each received data or message so that a destination device or network type may be identified for the received data or message**; **means for identifying from a plurality of device modules at the gateway for manipulating received data and messages into any of a plurality of formats or protocols for diverse device and network types, a device module associated with each received data or message's destination device type, network type, or both**; and **means for manipulating each received data or message so that each received data or message is then transmitted from the gateway through one or more remote networks to an intended remote destination device using a protocol and a format recognized by the intended remote destination device, irrespective of differences in the originating and receiving protocols**; one or more remote networks logically connected to the gateway; and at least one or more remote destination devices logically connected through the one or more remote networks.

28. In a networked computer system that includes one or more originating devices for originating data or messages, and wherein the originating devices are logically connected to and communicate using one or more **originating protocols** with one or more originating networks logically connected to a gateway, the gateway in turn being logically connected to one or more remote networks that are logically connected to and that communicate to one or more remote destination devices using one or more **receiving protocols**, at least some of which are different from the **originating protocols**, a method of forwarding the originating data or messages from the one or more originating devices through the gateway to the one or more remote destination devices notwithstanding the differences used in the originating and **receiving protocols**, the method comprising the following: an act of the gateway receiving data or a message generated at one or more of the originating devices, the received data or a message **intended** for at least one remote destination device; an act of the gateway reading, from the data or message, an address that either directly or indirectly identifies a location of the **intended** remote destination device; an act of the gateway determining a device type, a network type, or both, associated with the address of the **intended** remote destination device; an act of the gateway identifying a device module that corresponds to the device type, network type, or both associated with the address of the intended remote destination device; **an act of the gateway using the identified device module to manipulate the received data or message**; and **an act of the gateway transmitting the data or message from the gateway through the one or more remote networks to the intended remote destination device using a protocol and a format recognized by the intended remote destination device, irrespective of differences in the originating and receiving protocols**.

U.S. Pat. No. 6,874,090

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.

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 transmission 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.

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**.

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**.

U.S. Pat. No. 6,944,273

17. A mechanism for sending to a receiving device a message having a field prescribing the receiving device being coupled to either a data-centric network or a telephony-centric network, the mechanism comprising: a **message server**, for **translating the message into** a format compatible with the receiving device, and for initiating delivery of the message, said **message server** comprising: a **message scheduler**, for causing said **message server** to initiate delivery of the message; and a **data-centric network server**, coupled to sad

message server, for transmitting the message over a data-centric network for delivery to the receiving device wherein the receiving device is addressed by accessing an internet protocol address over the **data-centric network**.

21. The mechanism as recited in claim 17, wherein the message is supplied to the **message server** by an originator.

23. The mechanism as recited in claim 21, wherein said originator supplies the message in text or voice form from an originating device that is addressable over the data-centric network.

24. The mechanism as recited in claim 23, wherein said **data-centric network server** transmits a message entry web page to said originator for configuration of the message.

30. The mechanism as recited in claim 17, wherein said **message server** selects said format for delivery according to receiving capabilities of the receiving device.

35. A system for sending a message to a receiving device, the system comprising: a **message scheduler**, configured to initiate delivery of the message; a **message server**, coupled to said **message scheduler**, configured to **translate the message into** a format that is compatible with the receiving device; a **data-centric network server**, coupled to said **message server**, configured to transmit the message; a data-centric network, coupled to said data-centric network server, configured to route the message from said **data-centric network server** to either the receiving device or a **telephony-centric network server**, wherein, if the receiving device is addressed by a telephone number over a telephony-centric network, then said data-centric network routes the message to said **telephony-centric network server**.

42. The system as recited in claim 41, wherein said **data-centric network server** transmits a message entry web page to said originating device for configuration of the message.

APPENDIX B

Ref. Nos.	Term or Phrase to be Construed (Claims)	Court's Construction
1	virtual local area network / VLAN	subnetworks 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
	('830 Patent, claims 12, 25, 26, 27; '090 Patent, claim 27)	
2	LAN Link	a connection, other than a dial-up phone connection, to a local area network (LAN)
	('830, claims 17, 37; '090 Patent, claims 1, 25)	
3	MAC-based authentication flow	information exchange in which the authentication client uses the MAC address of the authentication agent for the purposes of authentication
	('090 Patent, claims 1, 3, 4, 5)	
4	comparing on the authentication server the first user identification information with	<i>No construction required</i>

user identification information in a database
of user identification information

	('830 Patent, claims 17, 37; '090 Patent, claims 1, 25)	
5	database of user identification information	<i>No construction required (AGREED)</i>
	('830 Patent, claims 17, 37; '090 Patent, claims 1, 5, 25)	
6	entering on a first node first user identification information	<i>No construction required</i>
	('830 Patent, claims 17, 37; '090 Patent, claims 1, 25)	
7	associating ... each [user] with a group of nodes represented by a virtual local area network selected for the user	<i>No construction required</i>
	('830 Patent, claim 12)	
8	prior to establishing communicability	before permitting access
	('830 Patent, claim 12)	
9	verifying a log-in sequence for each of the plurality of users the user's unique key	<i>No construction required</i>
	('830 Patent, claim 12)	
10	first user identification information	<i>No construction required</i>
	('830 Patent, claims 17, 37; '090 Patent, claims 1, 3, 5, 25)	
11	translation rules that resolve the incompatibility of the internal and external address realms	<i>No construction required</i>
	('799 Patent, claims 1, 2, 3, 4, 8, 9, 12, 13, 14, 15, 16, 17, 18, 19, 21, 22, 25, 26)	
12	an act of the gateway identifying a device module that corresponds to the device type, network type, or both associated with the address of the intended remote destination device	<i>No construction required</i>

('767 Patent, claim 28)

an act of the gateway using the identified device module to manipulate the received data or message

No construction required

('767 Patent, claim 28)

an act of the gateway transmitting the data or message from the gateway through the one or more remote networks to the intended remote destination device

No construction required

	('767 Patent, claim 28)	
--	-------------------------	--

13 a step for using the identified device module to manipulate the data or message so that the data or message is then transmitted from the gateway through the one or more remote networks to the intended remote destination device using a protocol and a format recognized by the intended remote destination device, irrespective of differences in the originating and receiving protocols

No construction required

a step for transmitting the data or message over the one or more remote networks to the intended remote destination device using the protocol and the format recognized by the intended remote destination device

No construction required

	('767 Patent, claims 1, 3)	
--	----------------------------	--

14 device module(s)

a device driver and/or network driver

	('767 Patent, claims 1, 11, 28)	
--	---------------------------------	--

15 intended

No construction required

	('767 Patent, claim 28)	
--	-------------------------	--

16 means for determining a specific address for each received data or message so that a destination device or network type may be identified for the received data or message

Function: determining a specific address for each received data or message so that a destination device or network type may be identified for the received data or message (AGREED)

	('767 Patent, claim 11)	
--	-------------------------	--

Structure: (1) message processor 406 and the corresponding software that reads the address from the message; or (2) message processor 406 accessing the

		address using locator module 408 that uses a lookup table stored in mass memory 410, which may be any suitable storage device, such as the system memory 22, a hard disk 27, removable magnetic disk 29, or removable optical disk 31
17	means for identifying from a plurality of device modules at the gateway for manipulating received data and messages into any of a plurality of formats or protocols for diverse device and network types, a device module associated with each received data or message's destination device type, network type, or both	Function: identifying from a plurality of device modules at the gateway for manipulating received data and messages into any of a plurality of formats or protocols for diverse device and network types, a device module associated with each received data or message's destination device type, network type, or both
	('767 Patent, claim 11)	Structure: 1) message processor 406 and the corresponding software that reads the device type from the message and identifies the driver corresponding to the device type; or 2) message processor 406 accessing the device type using a locator module 408 that uses a lookup table stored in mass memory 410, which may be any suitable storage device, such as the system memory 22, a hard disk 27, removable magnetic disk 29, or removable optical disk 31
18	means for manipulating each received data or message so that each received data or message is then transmitted from the gateway through one or more remote networks to an intended remote destination device using a protocol and a format recognized by the intended remote destination device, irrespective of differences in the originating and receiving protocols	Function: manipulating each received data or message so that each received data or message is then transmitted from the gateway through one or more remote networks to an intended remote destination device using a protocol and a format recognized by the intended remote destination device, irrespective of differences in the originating and receiving protocols (AGREED)
	('767 Patent, claim 11)	Structure: message processor 406, the software that executes the identified device module, and the identified device module
19	identifying ... a device module associated with [that corresponds to] the device type, network type, or both	one or more processors determine the device module that corresponds to the device type, network type, or both
	('767 Patent, claim 1, 28)	
20	originating protocols	a set of rules that governs the way the devices communicate or exchange data within the originating network
	('767 Patent, claims 1, 11, 28)	

	receiving protocols	a set of rules that governs the way the devices communicate or exchange data within the remote network
	('767 Patent, claims 1, 11, 28)	
21	message scheduler	AGREED-hardware or software that reside on or more computers that schedules messages for delivery
	('273 Patent, claims 17, 21, 30, 35)	
22	message server	one or more computers that both provide services for processing messages and that contain translation logic and software
	('273 Patent, claims 17, 21, 30, 35)	
	data-centric network server	one or more computers connected to a data-centric network that provide services over the data-centric network
	('273 Patent, 17, 24, 35, 42)	
	telephony-centric network server	one or more computers connected to a telephony-centric network that provide services to the telephony-centric network
	('273 Patent, claim 35)	
23	translating [translate] the message into	<i>No construction required</i>
	('273 Patent, claims 17, 35)	
24	addressed/addressable	AGREED-capable of being identified
	('273 Patent, claims 17, 18, 22, 23, 35, 36, 38, 39, and 40)	
25	data-centric network	AGREED-a network that carries digital data, primarily to facilitate information exchange among computers and computer peripherals. Examples included distributed computer networks such as the Internet.
	('273 Patent, claims 17, 23, 24, 35, 36, 38, 40)	
26	delivery	AGREED-transmission
	('273 Patent, claims 17, 30, 35)	
27	telephony-centric network	AGREED-a network that carries telephony information such as voice, fax, page messages, and the like, primarily to facilitate information exchange among telephony devices
	('273 Patent, claims 17, 18, 22, 35, 38, and 39)	

Produced by Sans Paper, LLC.