

1 The opinion in support of the decision being entered today was *not* written for publication
2 and is *not* binding precedent of the Board

3
4 UNITED STATES PATENT AND TRADEMARK OFFICE

5
6
7 BEFORE THE BOARD OF PATENT APPEALS
8 AND INTERFERENCES

9
10
11 *Ex parte* SURFCONTROL, INC.

12
13 Appeal No. 2006-1084
14 Reexamination Control Number 90/006,334
15 Patent No. 6,219,786 B1
16 Technology Center 2100

17
18
19 On Brief
20 Decided: February 27, 2007

21
22
23
24 Before LEE E. BARRETT, JAMESON LEE and JAMES T. MOORE,
25 *Administrative Patent Judges.*

26
27 LEE, *Administrative Patent Judge.*

28
29 DECISION ON APPEAL

30 A. Statement of the Case

31 This is a decision on appeal by the Patent Owner under 35 U.S.C.
32 § 134(b) and § 306 from the Examiner's Final Rejection of the Claims 1-18
33 in Patent No. 6,219,786 B1. We have jurisdiction under 35 U.S.C. § 6(b).

1 The Examiner rejected claims 2, 3 and 13 under 35 U.S.C. § 103 as
2 being unpatentable over Abraham and Stein.

3

4 B. Issues

5 Has the Examiner established unpatentability of claims 15-18 under
6 35 U.S.C. § 112, second paragraph, for indefiniteness?

7 Has the Examiner established unpatentability of claims 1, 4-12, and
8 14-15 under 35 U.S.C. § 102(e), as anticipated by Abraham?

9 Has the Examiner established unpatentability of claims 1, 4, 9 and 15
10 under 35 U.S.C. § 102(e), as anticipated by Cirasole?

11 Has the Examiner established unpatentability of claims 1-9 and 11-18
12 under 35 U.S.C. § 102(b), as anticipated by Engel?

13 Has the Examiner established unpatentability of claim 10 under
14 35 U.S.C. § 103, for obviousness based on Engel and Shwed?

15 Has the Examiner established unpatentability of claims 2, 3, and 13
16 under 35 U.S.C. § 103, for obviousness based on Abraham and Lodin?

17 Has the Examiner established unpatentability of claims 2, 3 and 13
18 under 35 U.S.C. § 103, for obviousness based on Abraham and Stein?

19

20 C. Summary of the Decision

21 No. The Examiner has not established the unpatentability of any
22 claims under any ground.

1 D. Findings of Fact (FF)

2 1. The invention is directed to a method and apparatus for
3 monitoring and controlling access by computer users to network resources.
4 ('786 Patent, col. 1, lines 4-8.)

5 2. In the context of the invention, the management of an
6 organization may set a network access control policy for its employees for
7 two reasons: (1) maximizing employee productivity by ensuring that
8 Internet access is used primarily for business purposes, and (2) maximizing
9 the Internet-connection capability of the organization, particularly during
10 peak usage times. ('786 Patent, col. 2, lines 9-15.) For example, the more
11 users are accessing the network, the more degraded the network accessing
12 capability becomes.

13 3. A traditional approach to providing access control is to apply
14 known firewall technology and focus on well-known data packet filtering
15 techniques, where no data packet is allowed to be forwarded without prior
16 filtering. ('786 Patent, col. 2, lines 31-38.)

17 4. In modern networks, including the Internet, each node-to-node
18 transmission is divided into multiple data packets which are separately
19 transmitted to a destination node. At the destination node, the multiple
20 packets are assembled to form the original message. ('786 Patent, col. 6,
21 lines 51-56.)

22 5. One sample data packet is illustrated in Figure 3 of the '786
23 Patent. ('786 Patent, col. 6, lines 56-57.)

1 6. There are protocols for network communications, usually in the
2 form of a layered set. ('786 Patent, col. 7, lines 30-31.)

3 7. The International Standards Organization (ISO) has developed
4 a model communication protocol referred to as the ISO 7-layer model.
5 Figure 4 of the '786 Patent illustrates the seven layers of the ISO model.
6 ('786 Patent, col. 7, lines 31-38.)

7 8. In the ISO, each layer represents a particular function. ('786
8 Patent, col. 7, lines 34-35.)

9 9. The lower-most layer of the ISO, Layer 1, is the hardware
10 network connection, such as a physical wire. ('786 Patent, col. 7, lines 39-
11 41.)

12 10. ISO Layer 2, Data Link Layer 52, is responsible for providing
13 reliable transmissions of data and it may be a network interface card that
14 links a computer to the network. ('786 Patent, col. 7, lines 41-44.)

15 11. ISO Layer 3, the Network Layer 54, is the network software for
16 routing packets throughout the network. ('786 Patent, col. 7, lines 45-46.)

17 12. ISO Layer 4, the Transport Layer 56, transports data from the
18 network to the upper levels of the ISO model. ('786 Patent, col. 7, lines 46-
19 48.)

20 13. ISO Layer 5, the Session Layer 58, deals with establishing
21 network sessions whereby logical connections are established based on a
22 user request. ('786 Patent, col. 7, lines 49-51.)

1 14. ISO Layer 6, the Presentation Layer 60, deals with the
2 presentation of data to an application which resides at ISP Layer 7. ('786
3 Patent, col. 7, lines 51-53.)

4 15. ISO Layer 7, the Application Layer 62, provides access to the
5 internet for a user. ('786 Patent, col. 7, line 55.)

6 16. Claims 1, 11, and 15 are the only independent claims on
7 appeal.

8 17. Claims 1, 11 and 15 read as follows:

9 1. A method of providing access control to
10 resources of a network comprising steps of:

11 monitoring network traffic of data packets in
12 which each said data packet includes identifications of
13 source and destination nodes and includes contextual
14 information, including receiving said data packets
15 transmitted to and from nodes of said network such that
16 receptions of said data packets are non-intrusive with
17 respect to traffic flow of said network;

18 with respect to individual node-to-node
19 transmissions within said network, assembling pluralities
20 of said received data packets specific to said individual
21 node-to-node transmissions, thereby forming an
22 assembled multi-packet communication for each of said
23 node-to-node transmission, wherein said node-to-node
24 transmissions are each in a form of an original composite
25 signal separated into a plurality of said data packets for
26 full and final reassembly at a destination node identified
27 in said data packets of said node-to-node transmission;

28 based upon said assembled multi-packet
29 communications, identifying source nodes and
30
31
32

1 destination nodes and contextual information for said
2 individual node-to-node transmissions; and

3
4 applying access rules to said assembled multi-
5 packet communications in determinations of whether said
6 individual node-to-node transmissions are restricted
7 transmissions, including basing said determinations on
8 said identifying said source and destination nodes and
9 said contextual information, wherein said steps of
10 monitoring, assembling, identifying and applying are
11 executed non-intrusively with respect to said restricted
12 transmissions and with respect to node-to-node
13 transmissions determined to be unrestricted transmissions
14 upon applying said access rules to said assembled multi-
15 packet communications of said unrestricted
16 transmissions, such that traffic flow of data packets from
17 said source nodes to said destination nodes is unaffected
18 by said steps.

19
20 11. A method of providing access control to
21 resources that are internal to and external of a network of
22 nodes, including computing devices of users of said
23 network, said method comprising steps of:

24
25 generating a rules base related to restricting access
26 to said resources by said nodes of said network, including
27 forming a first set of rules specific to access to external
28 resources and a second set of rules specific to access
29 internal resources;

30
31 monitoring transmissions that include one of said
32 computing devices;

33
34 acquiring information regarding each said
35 transmission, including determining information relating
36 to at least Layers 2, 3 and 7 of the ISO model, wherein

1 said steps of monitoring and acquiring include receiving
2 and assembling data packets to form a multi-packet
3 communication for each said transmission, said acquiring
4 including using said multi-packet communications to
5 determine said information; and

6
7 applying said rules base to said acquired
8 information to detect transmissions in which access to
9 said resources is restricted by said rules base, including
10 initiating a predetermined action in response to detecting
11 that a specific transmission relates to an access that is
12 restricted.

13
14 15. A system for providing access control to resources
15 of a network comprising:

16
17 a plurality of nodes, including computing devices;

18
19 means for non-intrusively intercepting data packets
20 to and from said nodes such that said intercepting is
21 substantially transparent to continuous packet flow
22 within said network, said data packets being intact
23 packets consistent with a packet protocol for
24 transmissions within said network;

25
26 means for identifying said data packets of discrete
27 transmissions and assembling said data packets, said
28 means for identifying and assembling having an output of
29 an assembled multi-packet communication for each said
30 discrete transmission, said means for identifying and
31 assembling being non-intrusive with respect to said
32 continuous packet flow of said data packets within said
33 network;

34
35 means connected to said output for determining
36 sources and destinations of said discrete transmissions

1 and determining user-generated contextual information
2 contained within said multi-packet communications;

3
4 a rule base store having a plurality of rules relating
5 to controlling access to said resources of said network;
6 and

7
8 means for controlling said access based upon
9 matching said rules to said sources, destinations and user-
10 generated contextual information from said means for
11 determining, said means for controlling being enabled to
12 apply rule actions to those said discrete transmissions for
13 which said matching indicates a restriction, said means
14 for controlling further being enabled to allow continuous
15 flow of packets of said discrete transmissions to remain
16 unhindered when said rules indicate an unrestricted
17 transmission on a basis of said multi-packet
18 communications.

19
20 18. The '786 Patent describes "non-intrusive" monitoring of data
21 packets in the network as one performed not at choke points in the network
22 ('786 Patent, col. 6, lines 14-16) and one in which "there will be no impact
23 on performance of the network." ('786 Patent, col. 7, lines 17-20.)

24 19. "Non-intrusive monitoring of network traffic," as referred to in
25 the '786 Patent, occurs by both receiving and assembling data packets of
26 node-to-node transmissions. ('786 Patent, col. 6, lines 49-51.)

27 20. In Stein, on page 405, it is stated:

28 If you have an extra router available, an attractive
29 alternative is to create a small screened subnetwork for
30 the sole use of the Web server (Figure 14.4). The router
31 separates the Web server from the rest of the internal
32 network; its rules allow the Web server to talk to the

1 firewall gateway using port 80 but blocks the server from
2 talking to any other host in your organization or directly
3 to the outside world.
4

5 E. Principles of law

6 Claims under reexamination are properly given their broadest
7 reasonable interpretation consistent with the patent disclosure. In re
8 American Academy of Science Tech Center, 367 F.3d 1359, 1364, 70
9 USPQ2d 1827, 1830 (Fed. Cir. 2004). A claim is sufficiently definite under
10 35 U.S.C. § 112, ¶ 2, if a person skilled in the field of the invention would
11 reasonably understand it when it is read in the context of the specification.
12 Marley Mouldings Ltd. v. Mikron Industries, Inc., 417 F.3d 1356, 1359, 75
13 USPQ2d 1954, 1956 (Fed. Cir. 2005). To establish anticipation under 35
14 U.S.C. § 102, each and every element in a claim, arranged as is recited in the
15 claim, must be found in a single prior art reference. Karsten Mfg. Corp. v.
16 Cleveland Golf Co., 242 F.3d 1376, 1383, 58 USPQ2d 1286, 1291 (Fed. Cir.
17 2001). Anticipation can be found when a claim limitation is inherent or
18 otherwise implicit in the relevant reference. Standard Havens Products, Inc.
19 v. Gencor Industries, Inc., 953 F.2d 1360, 1369, 21 USPQ2d 1321, 1328
20 (Fed. Cir. 1991). But, for establishing inherent disclosure, that which is
21 missing in the express description must necessarily be present and would be
22 so recognized by one with ordinary skill in the art. Continental Can Co.
23 USA, Inc. v. Monsanto Co., 948 F.2d 1264, 1268, 20 USPQ2d 1746, 1749
24 (Fed. Cir. 1991). Inherency may not be established by probabilities or
25 possibilities, and the mere fact that a certain thing may result from a given

1 set of circumstance is not sufficient. In re Oelrich, 666 F.2d 578, 581, 212
2 USPQ 323, 326 (CCPA 1981).

3
4 F. Analysis

5 The Indefiniteness Rejection under 35 U.S.C. § 112.

6 In support of the indefiniteness rejection of claims 15-18, the
7 Examiner explained that in the context of independent claim 15, on which all
8 of claims 16-18 depend, it is internally inconsistent to have continuous data
9 packet flow and absence of impact on network performance on the one hand
10 and interception of the same data packets on the other. The Examiner's
11 position is that if the data packets are "intercepted" as is recited in claim 15,
12 then it simply cannot be true that the flow of data packet is continuous or
13 that there is no impact on network performance. The concern is misplaced.
14 According to Merriam-Webster's Collegiate Dictionary, 609 (10th ed. 1999),
15 "intercept" in the context of signal communication can have the meaning of
16 "to receive (a communication or signal directed elsewhere) usu. secretly."
17 Given that a communication can be intercepted in secret, the meaning of
18 "intercept" is sufficiently broad to cover the case of non-intrusive reception
19 where the flow of data packets are non-interrupted. Therefore, the broadest
20 reasonable interpretation of the term "intercept" does not require interruption
21 of packet flow or a negative impact on network performance. "Intercept" in
22 the context of the invention is like engaging in eavesdropping rather than
23 seizure of a physical object.

24 Further in support of the indefiniteness rejection of claims 15-18, the
25 Examiner explained that in the context of claim 15, on which all claims 16-

1 18 depend, it is internally inconsistent to recite “intact” data packets and also
2 an output of an assembled multi-packet communication for each discrete
3 transmission. Evidently, the Examiner is of the view that if the data packets
4 are intact, meaning whole, nothing has to be assembled. The position is
5 misplaced. Although each data packet as recited is “intact,” meaning whole,
6 and need not be assembled, an entire communication is made up of multiple
7 data packets and need to be assembled. That comes from a plain reading of
8 the claim language. There is no internal inconsistency in that regard.

9 For the foregoing reasons, one with ordinary skill in the art would not
10 see any internal inconsistency as is articulated by the Examiner.

11 The Anticipation Rejection of
12 Claims 1, 4-12 and 14-15 over Abraham
13

14 Independent claim 1 requires a step of monitoring network traffic of
15 data packets including receiving the data packets such that the reception is
16 “non-intrusive” with respect to traffic flow of the network. Claim 1 also
17 requires assembling the received data packets to form an assembled multi-
18 packet communication, identifying the source and destination nodes and
19 contextual information based on the assembled multi-packet communication,
20 and applying access rules to the multi-packet communication, all non-
21 intrusively such that traffic flow of data packets is unaffected by the steps.
22 Claims 4-10 depend directly or indirectly from claim 1 and thus include all
23 the features of claim 1.

24 Independent claim 15 is an apparatus claim including a number of
25 means-plus-function clause recitations under 35 U.S.C. § 112, sixth

1 paragraph. There is a means for “non-intrusively” intercepting data packets
2 to and from a plurality of nodes in a network such that the interception is
3 substantially transparent to continuous packet flow within the network.
4 There is a means for identifying the data packets in a discrete transmission
5 and for assembling the data packets, which is “non-intrusive” with respect to
6 continuous packet flow of data packets within the network. There is also a
7 means for controlling access to the resources of the network based on
8 matching access rules to sources of transmissions, which allows continuous
9 flow of data packets in the discrete transmission to remain unhindered when
10 the rules indicate an unrestricted transmission.

11 As is explained in the ‘786 Patent, non-intrusive monitoring is done at
12 nodes other than choke points in the network and has no impact on the
13 performance of the network (See FF. 18 and 19). In the context of the ‘786
14 Patent, “non-intrusive” action with regard to reception or interception of data
15 packets, and identifying and assembling of data packets means without
16 interruption of the original flow of the data packets in the network, very
17 much as is recited in claims 1 and 15.

18 For a proper anticipation rejection of claims 1, 4-10 and 15, Abraham
19 must disclose non-intrusive reception or interception of data packets, and
20 non-intrusive identifying and assembling of a multiple data packet
21 communication forming a discrete transmission. For claims 1 and 4-10,
22 Abraham must also disclose non-intrusive application of access rules to the
23 assembled multi-packet communication and discrete transmission. For
24 claim 15, Abraham must disclose controlling of access by matching access

1 rule to the assembled discrete multi-packet transmission where the data flow
2 is unhindered if the result of rule application indicates unrestricted access.
3 Thus, for claim 15 the controlling of access is also non-intrusive in case the
4 access is determined to be unrestricted.

5 More importantly, the step of applying access rules of claim 1 is
6 applied to an assembled multi-packet communication, rather than any data
7 packet individually, and the function of access control of claim 15 is based
8 on matching access rules to information gleaned from the assembled multi-
9 packet communication and discrete transmission.

10 Similarly, independent claim 11 requires a monitoring and an
11 acquiring step which together include receiving and assembling data packets
12 to form an “assembled multi-packet communication” for each transmission,
13 and applying access rules to information determined from the “assembled
14 multi-packet communication,” specifically information relating to at least
15 Layers 2, 3 and 7 of the ISO model. Claim 11, unlike claims 1 and 15
16 however, does not require its monitoring, acquiring, receiving, assembling,
17 and applying steps to be non-intrusive. Claim 12, which depends from claim
18 11, recites that the monitoring and the acquiring steps, which together
19 include the receiving and assembling steps, are executed non-intrusively.
20 Claim 13 depends from claim 12 and claim 14 depends from claim 11.

21 With respect to Abraham as anticipatory prior art, the Examiner has
22 not established that it discloses the assembling feature required by claims 1,
23 11 and 15, and the subsequent application of access rules to the assembled
24 multi-packet communication (claims 1 and 11) or the subsequent controlling

1 of access based on matching access rules to information determined from the
2 assembled multi-packet communication (claim 15), much less the non-
3 intrusive manner of assembling a multi-packet communication and
4 subsequent non-intrusive applying of rules to the assembled multi-packet
5 communication as are recited in claims 1 and 15.

6 For a number of claim features including the assembling of multi-
7 packet communication, the Examiner collectively cites to the following
8 portions of Abraham: Figs. 2, 3A, 9A-9D, col. 5, lines 25-30, col. 6, lines
9 47-54, et seq., and col. 7, lines 15-25, et seq., and col. 11, lines 13, et seq.
10 For the feature of applying access rules of claim 1, the Examiner cites to
11 these portions of Abraham: Abstract, Figs. 2, 3A [elements 50, 62, 72, 76,
12 78], 4 [element 50], 5, 7A-7C, 8E, 9A-12, 15A-118, col. 2, lines 13-35, et
13 seq., col. 5, lines 54-59, et seq., col. 6, lines 25-36, et seq., col. 7, lines 38-
14 65, et seq., col. 8, lines 13-25, et seq., col. 9, lines 55, et seq., and col. 11,
15 line 1, et seq. For the feature of applying access rules of claim 11 and
16 controlling access based on matching rules of claim 15, the Examiner cites
17 to these portions of Abraham: Figs. 14-15B, 16, 21, 24, 25A-B, col. 6, lines
18 25-35, et seq. and lines 63-67, et seq., col. 7-8, col. 9, lines 43-67, et seq.,
19 col. 10, lines 13-25, and col. 11-12. We have reviewed all of the cited
20 portions referenced by the Examiner. However, not in any instance do we
21 find disclosure of the assembling of received or intercepted data packets into
22 a multi-packet communication for purposes of application of any access rule
23 or the application of access rule to an assembled multi-packet
24 communication (claim 1) or information content acquired from the

1 assembled multi-packet communication (claims 11 and 15) to determine
2 access. As is indicated by the Patent Owner, the portions cited by the
3 Examiner reflect an application of access rules to each individual data
4 packet, not an assembled multi-packet communication or information
5 content acquired from an assembled multi-packet communication. In that
6 connection, note Abraham, col. 46, lines 44-49:

7 Once the IP packet has been filtered, and the
8 appropriate action for the IP packet taken by the filter
9 engine 78, the logic returns to decision block 682 and
10 awaits interception of another IP packet. Blocks 682
11 through 706 are then repeated for each IP packet
12 intercepted by the filter engine 78.

13
14 Additionally, with respect to claims 1 and 15, the Examiner has not
15 shown that Abraham discloses the non-intrusive features required by the
16 claimed invention. In that connection, the Examiner cites to Abraham in col.
17 13, lines 20-23, which portion states: “If the system administrator selects
18 the Allow Network Protocols check box in the corporate default window
19 102, IP packets communicated using a predefined list of network protocols
20 are allowed to pass through the filter engine 78 unconditionally.” That
21 description is consistent with either non-intrusive monitoring, identifying
22 and access control, or intrusive monitoring, identifying and access control.
23 The fact that a data packet of a certain type is allowed to pass through the
24 filter engine 78 unconditionally does not necessarily mean that reception of
25 the data packet, identification of the same, and determination of that data
26 packet as within a group authorized to pass through the filter
27 unconditionally, all took place without disruption of data flow.

1 be buffered. If the data packet or packets trigger the
2 filtering scheme, such as by containing specific words or
3 phrases, the transmission to the user may be terminated.
4

5 As for the “non-intrusive” feature, the Examiner appears to take the
6 position that so long as unrestricted communication somehow winds its way
7 to the intended destination node at some time, after all the receiving,
8 assembling, identifying, and applying functions have been carried out, all
9 that which have taken place can be regarded as non-intrusive. That
10 interpretation is far from being consistent with the ‘786 Patent. As is
11 explained in the ‘786 Patent, non-intrusive monitoring is done at nodes other
12 than choke points in the network and has no impact on the performance of
13 the network (See FF. 18 and 19). Claim 1 further buttresses the “non-
14 intrusive” requirement by particularly specifying that the monitoring,
15 assembling, identifying, and applying steps are performed “such that traffic
16 flow of data packets from said source nodes to said destination nodes is
17 unaffected by said steps.” Claim 15 further buttresses the “non-intrusive”
18 requirement by particularly specifying that the identifying and assembling
19 are non-intrusive “with respect to said continuous packet flow of said data
20 packets within said network,” and that the access control is enabled “to
21 allow continuous flow of packets of said discrete transmissions to remain
22 unhindered when said rules indicate an unrestricted transmission on the basis
23 of said multi-packet communications.” The Examiner evidently has not
24 analyzed the impact on data packet flow with respect to the access control
25 disclosed in Cirasole. Moreover, the above-quoted portion of Cirasole cited
26 by the Examiner suggests data packet flow is indeed affected by the filtering

1 process, as a data packet is not forwarded to the destination node unless and
2 until it has first been screened by the filtering scheme.

3 Stevens is relied on by the Examiner to show the details of
4 conventional TCP/IP (Transmission Control Protocol/Internet protocol) and
5 does not make up for the deficiencies of the Abraham as discussed above.

6 The Anticipation Rejection of
7 Claims 1-9 and 11-18 over Engel
8

9 As is in the case of the anticipation rejections over Abraham and
10 Cirasole, in the case of the alleged anticipation by Engel, the Examiner has
11 failed to establish that Engel discloses assembling of data packets to form a
12 multi-packet communication to which is then applied the access rules (claim
13 1) for controlling access or the information content of which is used for
14 applying an access rule (claims 11 and 15). According to the Examiner, the
15 sending of a discrete transmission or communication in multiple data
16 packets and the subsequent collection and assembly of the separate packets
17 to reform the original transmitted message is conventional in the art. It is,
18 and the Patent Owner agrees with that assessment. But it cannot be taken
19 out of context. For receiving the entire transmission at the destination node,
20 it is conventional and common place to reassemble the separately
21 transmitted data packets into the original multi-packet communication.
22 That, however, is not what the claim feature in dispute is about. The
23 invention claimed is about controlling network access by applying an access
24 rule to an assembled multi-packet communication (claim 1) or information
25 content acquired from an assembled multi-packet communication (claims 11

1 and 15). The Examiner has not shown where in Engel is there a disclosure
2 of assembling data packets to form a multi-packet communication to which
3 is applied an access rule or to the acquired information which is applied an
4 access rule. Moreover, it appears from col. 6, lines 46-55 of Engel,
5 reproduced below, that the monitoring and application of an access rule is on
6 a packet by packet basis:

7 The method of determining whether to terminate the
8 transmission can be based on any of the data bits inside the
9 packet 20. For example, the access controller 16a can make its
10 decision based upon the contents of the source field 20a,
11 destination field 20b, or protocol type field 20c, as well as
12 network addresses or transport and higher layer service requests
13 contained in the data field 20d. Stated another way, any logical
14 test can be used to evaluate any of the bits in the packet 20 to
15 determine its eligibility for transmission.
16

17 Figures 1-3 of Engel, cited by the Examiner, also do not illustrate any
18 application of an access rule to an assembled multi-packet communication.
19 Rather, Figure 1 illustrates the internal fields of a data packet and Figures 2
20 and 3 illustrate the detection and decision making with respect to each
21 individual data packet.

22 On page 31 of the Answer, the Examiner states: “Since modern
23 networks routinely perform packet segmentation and assembly, and the very
24 packets and protocol disclosed by appellant are used in the invention of
25 ‘Engel ‘984, it is therefore inherent that Engel ‘984 makes use of this well
26 known packetization and assembly of data transmission units.” The
27 conclusion of inherency is both misapplied and without merit. First, the
28 context is misplaced. The Examiner has misapplied what is commonly done

1 at a destination node to reconstruct a multi-packet communication to the
2 different environment of intercepting data packets intended for elsewhere to
3 determine network access. Secondly, the Examiner has articulated no basis
4 why, for purposes of monitoring network access, an access rule must
5 necessarily be applied to an entire multi-packet communication and not
6 individual data packets on a packet by packet basis.

7 The Obviousness Rejection of
8 Claim 10 over Engel and Shwed
9

10 Claim 10 depends from claim 1 and adds the step of “executing first-
11 line network intrusion detection at an entry point of said network, such that
12 transmissions from nodes that are external to said network are subject to
13 first-line network intrusion restriction rules, said first-line network intrusion
14 detection being independent of said step of applying said access rules.”
15 Shwed is relied on by the Examiner to show a first-line network intrusion
16 detection that is independent of the step of applying the access rules, and
17 does not make up for the deficiencies of Engel as already discussed above
18 with regard to the anticipation rejection of claim 1 over Engel.

19 The Obviousness Rejections of Claims 2, 3 and 13
20 over Abraham and Lodin and
21 over Abraham and Stein
22

23 Claim 2 depends from independent claim 1, and claim 3 depends from
24 claim 2. Claim 13 depends from claim 12 which depends from independent
25 claim 11. Independent claims 1 and 11 had already been rejected by the
26 Examiner as anticipated by Abraham. References Lodin and Stein are each
27 relied on to meet the additional features of the dependent claims, and do not

1 make up for the deficiencies discussed above regarding the application of
2 Abraham to independent claims 1 and 11. On that basis alone, the
3 obviousness rejection of claims 2, 3 and 13 cannot be sustained. In any
4 event, however, as will be explained below, neither Lodin nor Stein
5 discloses what the Examiner has relied on those references to show.

6 Claim 2 requires that the receiving and assembling steps be executed
7 at a network element outside of the direct path from source nodes to
8 destination nodes, and claim 13 requires the monitoring and information
9 acquiring steps to include receiving and assembling data packets at a node
10 outside of the direct path of the intended transmissions. On page 36 of the
11 Answer, the Examiner states: “Lodin was provided to teach typical LAN
12 and network configuration that provides a means of monitoring and
13 controlling network transmission that is not within a direct line with a
14 workstation/computer.” Also on page 36 of the Answer, the Examiner
15 states:

16 Figure 4 of Lodin, shows a more detailed view of
17 how firewall, host, servers, administrators etc. may be
18 located such that they are not in the direct line of
19 transmission. The screened subnet places the
20 transmission outside of the direct path of the
21 firewall/bastion and only allowed selected data to pass
22 (Lodin fig. 4). Thereby, allowing for the transmission of
23 the network to be monitored and routed without passing
24 directly through a firewall.

25
26 All above-quoted statements are incorrect insofar as they suggest that in
27 Lodin access control of a transmission is not implemented within the direct
28 line of communication between the source node and the destination node of

1 an intended transmission. The “screened subnet” referred to by the
2 Examiner in Figure 4 is a packet-filtering firewall that prevents direct
3 communication between a protected network from an external network.
4 Lodin, page 29, col. 2, lines 19-21 and Figure 4 (bottom). As is shown in
5 Figure 4 (bottom), one router channels communication between devices
6 inside the protected network to two bastion hosts, and another router
7 channels communication between the external untrusted network and the
8 two bastion hosts. A firewall represented by the two routers and the two
9 bastion hosts exists in the direct line of communication between devices in
10 the internal network and devices in the external network.

11 Regarding Stein, the Examiner states (Answer on pages 36-37):

12 As per Stein, it shows a basic and fundamental
13 configuration for a screened subnet (fig. 14.4) and
14 implementation of one where the proxy provides
15 transmission routing that is not in the direct path of the
16 source to destination. This well known method provides
17 for routing to occur that provides a limited and controlled
18 access to the server, see page 406.

19
20 The above-quoted statement is incorrect insofar as it is attempting to read
21 the additional features of claims 2 and 13 onto Stein. As is described on
22 page 405 of Stein and illustrated in Stein’s Figure 14.4, the screened subnet
23 is for the exclusive use of the web server and is in the direct path of access
24 by anyone to the web server. (FF. 20). If the Examiner is referring to
25 transmissions between devices on the external network and devices in the
26 internal network, the screened subnet is not in the direct path of
27 communication but it also plays no role in regulating such communications.

1 According to claims 2 and 13, the monitoring, receiving, assembling, and
2 information acquiring steps must take place outside of the direct path of
3 communication for the data packets in those communications. The
4 Examiner has failed to demonstrate that that is the case in Stein.

5

6

CONCLUSION

7

8 The indefiniteness rejection of claims 15-18 under 35 U.S.C. § 112,
9 second paragraph, is **reversed**.

10 The rejection of claims 1, 4-12, and 14-15 as anticipated by Abraham
11 under 35 U.S.C. § 102(e) is **reversed**.

12 The rejection of claims 1, 4, 9 and 15 as anticipated by Cirasole under
13 35 U.S.C. § 102(e) is **reversed**.

14 The rejection of claims 1-9 and 11-18 as anticipated by Engel under
15 35 U.S.C. § 102(b) is **reversed**.

16 The rejection of claim 10 as unpatentable over Engel under 35 U.S.C.
17 § 103 is **reversed**.

18 The rejection of claims 2, 3, and 13 as unpatentable over Abraham
19 and Lodin under 35 U.S.C. § 103 is **reversed**.

20 The rejection of claims 2, 3, and 13 as unpatentable over Abraham
21 and Stein under 35 U.S.C. § 103 is **reversed**.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

REVERSED

_____)
LEE E. BARRETT)
Administrative Patent Judge)
)
)
)
_____) BOARD OF PATENT
JAMESON LEE) APPEALS AND
Administrative Patent Judge) INTERFERENCES
)
)
)
_____)
JAMES T. MOORE)
Administrative Patent Judge)

mtv

Appeal No. 2006-1084
Reexamination Control No. 90/006,334

1 Via First Class Mail

2 Attorney for the appellant:

3

4 Terry McHugh

5 101 First Street

6 PMB 560

7 Los Altos, California 94022

8

9 Attorney for third party requester:

10

11 Charles F. Schill

12 Steptoe & Johnson LLP

13 1330 Connecticut Avenue N.W.

14 Washington, DC 20036

Merriam
Webster

Merriam-
Webster's

Collegiate
Dictionary

TENTH
EDITION

Merriam-
Webster's
Collegiate
Dictionary

TENTH EDITION

Property of U.S. Government



A GENUINE MERRIAM-WEBSTER

The name *Webster* alone is no guarantee of excellence. It is used by a number of publishers and may serve mainly to mislead an unwary buyer.

Merriam-Webster™ is the name you should look for when you consider the purchase of dictionaries or other fine reference books. It carries the reputation of a company that has been publishing since 1831 and is your assurance of quality and authority.

Copyright © 1999 by Merriam-Webster, Incorporated

Philippines Copyright 1999 by Merriam-Webster, Incorporated

Library of Congress Cataloging in Publication Data

Main entry under title:

Merriam-Webster's collegiate dictionary. — 10th ed.

p. cm.

Includes index.

ISBN 0-87779-708-0 (unindexed : alk. paper). — ISBN 0-87779-709-9 (indexed :
alk. paper). — ISBN 0-87779-710-2 (deluxe indexed : alk. paper). — ISBN
0-87779-707-2 (laminated cover, unindexed).

1. English language—Dictionaries. I. Merriam-Webster, Inc.

PE1628.M36 1998

423—dc21

97-41846

CIP

Merriam-Webster's Collegiate® Dictionary, Tenth Edition principal copyright 1993

COLLEGIATE is a registered trademark of Merriam-Webster, Incorporated

All rights reserved. No part of this book covered by the copyrights hereon may be reproduced or copied in any form or by any means—graphic, electronic, or mechanical, including photocopying, taping, or information storage and retrieval systems—without written permission of the publisher.

Made in the United States of America

242526WC99

aptness and sometimes suggests... (clever with words). ALERT... understanding (alert to new...)

gen(t)-sē-ā, -gen(t)-ā n [Russ intell... (1907): intellectuals who form...]

adj [ME, fr. L intelligibilis... nsible by the intellect only; 2...]

prehended — in-tel-li-gi-bil-i-ty... le-ness \-'tē-lə-jə-bəl-nəs\ n —

n-p(ə)-trən(t)s\ n (15c): lack of... drinking of intoxicants

adj [ME intemperat, fr. L intem... perare to temper] (14c): not tem... excessive use of intoxicating liqu...

tem-per-ate-ness n... entenden, intenden, fr. MF enten... retch out, direct, aim at, fr. in-

n (14c) 1: to direct the mind on... 3 a: SIGNIFY, MEAN b: to refo... pose or goal: PLAN b: to design

chaic: SET OUT, START — in-tend... (t)s\ n (1739) 1: MANAGEMENT, SU... tive department

fr. MF, fr. L intendens, intenda... (1652): an administrative offi... French, Spanish, or Portuguese mou...

pected to be such in the future (an... ONAL — in-tend-ed-ly adv... erson to whom another is engaged

ASPECTIVE, ASPIRING (an ~ teacher... nant\ n (14c): the true meaning or...

āt\ v (-at-ed; -at-ing [in- + L...]) (1595): to make tender: SOFTEN... n

ME, fr. MF, fr. L intensus, fr. pp. of... a: existing in an extreme degree... b: having or showing a characteris...

2: marked by or expressive of... concentration (~ effort) 3 a: ex... cess of purpose (an ~ student) b: ex... tense-ness n

sa-ñ(-ə)r\ n (1835): one that inter... -ñ\ v (-fied; -fy-ing v (1817) -... : STRENGTHEN 2 a: to increase (a... graphic image) by chemical treatm...

PERM ~ w: to become intense or mo... tore acute — in-ten-si-fi-ca-tion\ v... n (1604) 1: INTENSITY 2: COM...

ch-nal, -ten(t)-shə-n\ adj — in-te... tē\ n — in-ten-sion-al-ly\ v... -tē\ n, pl -ties (1665) 1: the quali...

applies to a more individually determined wish or need (his... object was the achievement of pleasure). OBJECTIVE implies...

ing tangible and immediately attainable (their objective is to... the oil fields). GOAL suggests something attained only by pro...

effort and hardship (worked years to reach her goals)... of or relating to... intention b: having external reference SYN see VOL...

in-ten-tion-al-ly\ v, -ten(t)-shə-n\ n — in-ten-tion... -ten(t)-shə-n\ n — in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre,...

in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L... in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L...]

in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L... in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L...]

in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L... in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L...]

in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L... in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L...]

in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L... in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L...]

in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L... in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L...]

in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L... in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L...]

in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L... in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L...]

in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L... in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L...]

in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L... in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L...]

in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L... in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L...]

in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L... in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L...]

in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L... in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L...]

in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L... in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L...]

in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L... in-ter-terred; in-ter-ring [ME enteren, fr. MF enterre, fr. L...]

intercalare] (1614) 1 a: inserted in a calendar (an ~ day) b of a... year: containing an intercalary period (as a day or month) 2: in-

inter-ca-late \in-'tər-kə-'lāt\ v (-lat-ed; -lat-ing [L intercalatus pp. of... intercalare, fr. inter- + calare to proclaim, call — more at LOW] (1603)

1: to insert (as a day) in a calendar 2: to insert between or among... existing elements or layers SYN see INTRODUCE — in-ter-ca-la-tion

\-tər-kə-'lā-shən\ n... in-ter-cede \in-'tər-'sēd\ v (-ced-ed; -ced-ing [L intercedere, fr. inter- +...

cedere to go] (1597): to intervene between parties with a view to... reconciling differences: MEDIATE SYN see INTERPOSE — in-ter-cede-r

n... in-ter-cep-sal \in-'tər-'sep(-t)-'səl\ adj (1837): occurring between cen-... suses (~ estimates) (~ period)

in-ter-cept \in-'tər-'sept\ v [ME, fr. L interceptus pp. of interceptare, fr. inter- +...

capere to take, seize — more at HEAVE] (15c) 1 obs: PREVENT, HINDER 2 a:

to stop, seize, or interrupt in progress or course or before arrival b: to receive (a communication or signal directed else-... where) usu. secretly 3 obs: to interrupt communication or connection

with 4: to include (part of a curve, surface, or solid) between two... points, curves, or surfaces (the part of a circumference ~ed between two radii) 5 a:

to gain possession of (an opponent's pass) b: to intercept a pass thrown by (an opponent)

in-ter-cept \in-'tər-'sept\ n (1821) 1: the distance from the origin to a... point where a graph crosses a coordinate axis 2: INTERCEPTION; esp:

the interception of a missile by an interceptor or of a target by a mis-... sile 3: a message, code, or signal that is intercepted (as by monitor-

ing radio communications) in-ter-cep-tion \in-'tər-'sep-'shən\ n (15c) 1 a: the action of in-

tercepting b: the state of being intercepted 2: something that is in-ter-cepted; esp:

an intercepted forward pass in-ter-cept-er \in-'tər-'sept-'er\ n (1598): one that in-

tercepts; specif: a light high-speed fast-climbing fighter plane or missile designed for defense against raiding bombers or missiles

in-ter-ces-sion \in-'tər-'ses-'shən\ n [ME, fr. MF or L; MF, fr. L intercessio, intercessio, fr. intercedere] (15c) 1: the act of interceding 2:

prayer, petition, or entreaty in favor of another — in-ter-ces-sion-al \-'sesh-nəl, -'sesh-n'əl\ adj — in-ter-ces-sor \-'ses-sər\ n — in-ter-ces-so-ry \-'ses-rē, -'ses-rē\ adj

in-ter-change \in-'tər-'čhānj\ v [ME entrechaungen, fr. MF entrechangier, fr. OF, fr. entre- + changier to change] (14c) 1: to put each of (two things) in the place of the other 2: EXCHANGE ~ v: to change places mutually — in-ter-change-er n

in-ter-change \in-'tər-'čhānj\ n (15c) 1: the act, process, or an in-

stance of interchanging: EXCHANGE 2: a junction of two or more highways by a system of separate levels that permit traffic to pass from one to another without the crossing of traffic streams

in-ter-change-able \in-'tər-'čhānj-'ə-bəl\ adj (14c): capable of being interchanged; esp: permitting mutual substitution (~ parts) — in-ter-change-abil-i-ty \-'čhānj-'ə-bi-lə-tē\ n — in-ter-change-able-ness \-'čhānj-'ə-bəl-nəs\ n — in-ter-change-ably \-'blē\ adv

in-ter-col-le-giate \in-'tər-'kɔlə-'jē-jət, -jē-ət\ adj (ca. 1874): existing, carried on, or participating in activities between colleges (~ athletics)

in-ter-col-um-ni-a-tion \in-'tər-'kɔlə-'dʒm-nē-'ā-shən\ n [L intercolumnium space between two columns, fr. inter- + columna column] (1624) 1:

the clear space between the columns of a series 2: the system of spacing of the columns of a colonnade

in-ter-com \in-'tər-'kɔm\ n [short for intercommunication system] (1940): a two-way communication system with a microphone and loudspeaker at each station for localized use

in-ter-com-mu-ni-cate \in-'tər-'kɔ-'myū-nə-'kāt\ v (1586) 1: to exchange communication with one another 2: to afford passage from one to another — in-ter-com-mu-ni-ca-tion \-'myū-nə-'kā-shən\ n

intercommunication system n (1911) INTERCOM in-ter-com-mu-ni-on \in-'tər-'kɔ-'myū-nyən\ n (1921): interdenominational participation in communion

in-ter-con-nect \in-'tər-'kɔ-'nek-t\ v (1865): to connect with one another ~ v: to be or become mutually connected — in-ter-con-ec-tion \-'nek-shən\ n

interconnected adj (1865) 1: mutually joined or related (~ high-ways) (~ political issues) 2: having internal connections between the parts or elements — in-ter-con-ec-ted-ness n

in-ter-con-ti-nen-tal \in-'tər-'kɔn-'tɪ-'nən-tl\ adj (ca. 1855) 1: extending among continents or carried on between continents 2: capable of traveling between continents (~ ballistic missile)

in-ter-con-ver-sion \in-'tər-'kɔn-'vər-zhən, -shən\ n (1865): mutual conversion (~ of chemical compounds) — in-ter-con-vert \-'vɔrt\ v — in-ter-con-vert-i-bil-i-ty \-'vɔrt-'bi-lə-tē\ n — in-ter-con-vert-i-ble \-'vɔrt-'ə-bəl\ adj

in-ter-cool-er \in-'tər-'kū-lər\ n (1899): a device for cooling a fluid (as air) between successive heat-generating processes

in-ter-co-s-tal \in-'tər-'kɔs-tl\ adj [NL intercostalis, fr. L inter- + costa rib — more at COAST] (1597): situated or extending between the ribs (~ spaces) (~ muscles) — intercostal n

in-ter-course \in-'tər-'kɔrs, -kɔrs\ n [ME intercurse, prob. fr. MF intercourse, fr. ML intercourse, fr. L act of running between, fr. intercurre to run between, fr. inter- + currere to run — more at CAR] (15c) 1:

connection or dealings between persons or groups 2: exchange esp. of thoughts or feelings; COMMUNION 3: physical sexual contact between individuals that involves the genitalia of at least one person (heterosexual ~) (anal ~) (oral ~); esp: SEXUAL INTERCOURSE 1

in-ter-crop \in-'tər-'krɔp, in-'tər-\ v (1898): to grow a crop in be-tween (another) ~ v: to grow two or more crops simultaneously (as in alternate rows) on the same plot — in-ter-crop \in-'tər-'krɔp\ n

in-ter-cross \in-'tər-'krɔs\ v (1711): CROSS in-ter-cross \in-'tər-'krɔs\ n (1859): an instance or a product of crossbreeding

in-ter-do-mi-n-ion \in-'tər-'dɔm-'i-ŋ-i-ŋ\ n

in-ter-elec-trode \in-'tər-'el-ek-'trɔd\ n

in-ter-elec-trom \in-'tər-'el-ek-'trɔm\ n

in-ter-elec-tro-de \in-'tər-'el-ek-'trɔd\ n

in-ter-ep-i-dem-ic \in-'tər-'ep-'i-'dem-'ik\ n

in-ter-eth-ic \in-'tər-'eθ-'ik\ n

in-ter-fac-ty \in-'tər-'fæs-'tē-tē\ n

in-ter-fa-mi-li-al \in-'tər-'fæ-'mɪ-'li-əl\ n

in-ter-fam-ly \in-'tər-'fæ-'mē-tē\ n

in-ter-flu-ent \in-'tər-'flū-'ent\ n

in-ter-gar-tish \in-'tər-'gɑr-'tɪʃ\ n

bring war of INTERROBANG

in-ter-act \in-'tər-'rækt\ v (1839): to act upon one another

in-ter-act \in-'tər-'rækt\ v (1839): to act upon one another

in-ter-act \in-'tər-'rækt\ v (1839): to act upon one another

in-ter-act \in-'tər-'rækt\ v (1839): to act upon one another

in-ter-act \in-'tər-'rækt\ v (1839): to act upon one another

in-ter-act \in-'tər-'rækt\ v (1839): to act upon one another