Attorney Docket: EXC-964IPR

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inter partes Review Case No. IPR2016-00567

Inter partes Review of: U.S. Patent No. 8,185,964

Issued: May 22, 2012

To: Joseph Robert Marchese

For: Digital Video System Using Networked Cameras

PETITION FOR *INTER PARTES* REVIEW OF USPN 8,185,964

Mail Stop Patent Board
Patent Trial and Appeal Board
P.O. Box 1450
Alexandria, VA 22313-1450

Steven M. Bauer, Reg. No. 31,481
Joseph A. Capraro Jr., Reg. No. 36,471
Proskauer Rose LLP
One International Place
Boston, MA 02110
Tel: (617) 526-9600

Dated: February 5, 2016

Table of Contents

Table of Exhibits

Exhibit	Description	Publication Date or Filing Date	Type of Prior Art (35 U.S.C.)
1001	USPN 8,185,964 (patent under *Inter Partes* Review)	Feb. 18, 2010	N/A
1002	The file history for the '964 patent	N/A	N/A
1003	Declaration of Mr. Greg Thompson in Support of the Request for *Inter Partes* Review of the '964 Patent	N/A	N/A
1004	USPN 6,166,729 to Acosta et al. ("Acosta")	May 7, 1997	102(e)
1005	USPN 5,905,859 to Holloway et al. ("Holloway")	May 18, 1999 (Publication) January 9, 1997 (Filing)	102(a)/102(e)
1006	USPN 6,292,838 to Nelson ("Nelson")	August 23, 1999	102(e)
1007	AXIS 200 User's Manual ("Axis 200")	October, 1998	102(b)
1008	AXIS 2100 Network Camera User's Guide ("Axis 2100")	November, 1999	102(a)
1009	AXIS 2400 and AXIS 2401 Video Servers Administration Manual ("Axis 2400")	July, 1999	102(a)
1010	Declaration of James Marcella	NA	NA
1011	USPN 6,438,530 to Heiden et al. ("Heiden")	December 29, 1999	102(e)
1012	USPN 6,477,648 to Schell et al. ("Schell")	March 23, 1997	102(e)
1013	ANSI/IEEE Std 802.3-1985 ("Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications") ("802.3 Standard")	1985	102(b)

Through counsel, Petitioner Exacq Technologies, Inc. ("Petitioner" or "Exacq") hereby petitions for *inter partes* review ("IPR") under 35 U.S.C. §§ 311-319 and 37 C.F.R. § 42 of claims 1-4 of U.S. Patent 8,185,964 (Ex. 1001) (the "'964 patent"). This Petition shows that there is a reasonable likelihood that Petitioner will prevail in establishing that at least one of these claims is unpatentable. Petitioner requests that each of these claims be declared unpatentable and canceled.

I. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(A)

A. Real Party-In-Interest under 37 C.F.R. § 42.8(b)(1)

Petitioner, Exacq Technologies, Inc., and Tyco Fire & Security (US) Management, Inc., Sensormatic Electronics, LLC, Tyco International Management Company, LLC, and SimplexGrinnell LP are the real parties-in-interest.

B. Related Matters under 37 C.F.R. § 42.8(b)(2)

The following matters would affect, or be affected by, a decision in this proceeding: *JDS Technologies, Inc. v. Exacq Technologies, Inc.*, Civil Action No. 2:15-cv-10387-AC, filed on January 28, 2015 in the U.S. District Court for the Eastern District of Michigan; *JDS Technologies, Inc. v. Avigilon USA Corporation, Inc. and Avigilon Corporation*, Civil Action No. 2:15-cv-10385-AC, filed on January 28, 2015 in the U.S. District Court for the Eastern District of Michigan;

IPR2016-00511; U.S. Patent No. 6,891,566; and U.S. Patent Application No. 13/453,595.

C. Lead and Back-Up Counsel under 37 C.F.R. § 42.8(b)(3)

Petitioner provides the following designation of counsel.

LEAD COUNSEL	BACK-UP COUNSEL
Steven M. Bauer Reg. No. 31,481 Proskauer Rose LLP One International Place Boston, MA 02110 Tel: (617) 526-9600 Fax: (617) 526-9899 PTABMattersBoston@proskauer.com	Joseph A. Capraro Jr. Reg. No. 36,471 Proskauer Rose LLP One International Place Boston, MA 02110 Tel: (617) 526-9600 Fax: (617) 526-9899 jcapraro@proskauer.com

D. Service Information under 37 C.F.R. § 42.8(b)(4)

For purposes of this proceeding, Exacq may be served at the lead counsel address provided in Section I.C.

E. Proof of Service on the Patent Owner

A copy of this Petition, including all exhibits and a power of attorney, is being served by PRIORITY MAIL® on Brooks Kushman P.C., 1000 Town Center, Twenty-Second Floor, Southfield, MI 48075.

F. Power of Attorney

A power of attorney is being filed with the designation of lead counsel in accordance with 37 C.F.R. § 42.10(b).

II. PAYMENT OF FEES – 37 C.F.R. § 42.103

The undersigned authorizes the Director to charge the fee set forth in 37C.F.R. § 42.15(a), as required by 37 C.F.R. § 42.103, to Deposit Account No. 50-3081. The undersigned further authorizes payment for any additional fees that might be due in connection with this Petition to be charged to the above referenced Deposit Account.

III. REQUIREMENTS FOR *INTER PARTES* REVIEW UNDER 37 C.F.R. § 42.104

A. Grounds for Standing under 37 C.F.R. § 42.104(a)

Petitioner certifies that the '964 patent is eligible for *inter partes* review and further certifies that Petitioner is not barred or otherwise estopped from requesting review challenging the identified claims on the grounds identified within the present petition.[1]

[1] Petitioner was served on February 6, 2015, with the complaint in *JDS Technologies, Inc. v. Exacq Technologies, Inc.*, Civil Action No. 2:15-cv-10387-AC, alleging infringement of the '964 patent.

B. Identification of Challenge under 37 C.F.R. § 42.104(b) and Statement of Precise Relief Requested

Petitioner requests *inter partes* review of claims 1-4 of the '964 patent on the grounds set forth in the table below and requests that each of the claims be found unpatentable and canceled. An explanation of how claims 1-4 are unpatentable under the grounds identified, including the identification of where each element is found in the prior art and the relevance of the prior art, is provided below. Additional explanation and support for each ground of rejection is set forth in the Declaration of Mr. Greg Thompson. (*See* Ex. 1003.)

Ground	'964 Patent Claims	Basis for Rejection
1	1 and 3	Acosta (35 U.S.C. § 102)
2	2-3	Acosta and Axis 200[2] (35 U.S.C. § 103)
3	4	Acosta, Axis 200, and Nelson (35 U.S.C. § 103)

[2] The October, 1998 publication date of Axis 200 is confirmed by the declaration of James Marcella stating Axis 200 was publicly available for download at axis.com and was publicly distributed with the purchase of an Axis 200 camera. (*See* Marcella Decl. ¶¶ 5-10 (Ex. 1010).)

C. Threshold Requirement for *Inter Partes* Review Under 37 C.F.R. § 42.108(c)

An IPR should be instituted when there is a "reasonable likelihood that the requester will prevail with respect to at least one of the claims challenged." 35 U.S.C. § 314(a). This petition demonstrates that there is a reasonable likelihood that Petitioner will prevail with respect to at least one of the challenged claims and that each of the challenged claims is unpatentable.

IV. LEVEL OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the relevant field at the alleged time of invention of the '964 patent would have an undergraduate degree in computer science or electrical engineering and 2-3 years of experience designing and programming video management system software, or an equivalent combination of education and experience. (*See* Thompson Decl. ¶¶ 27-32 (Ex. 1003).)

V. CLAIM CONSTRUCTION

Claims in *inter partes* review are given the "broadest reasonable construction in light of the specification of the patent in which [they] appear[]." 37 C.F.R. § 42.100(b); see Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48, 764, 48,766. All claim terms in the '964 patent should be given their broadest

reasonable meaning in light of the specification as commonly understood by those of ordinary skill.[3]

VI. OVERVIEW OF THE '964 PATENT

The '964 patent is directed to a "digital video system including a computer connected via a network to a number of video servers and cameras." ('964 patent, Abstract (Ex. 1001).) As shown in FIG. 1 below, "video system 20 includes a client computer 22, a plurality of cameras 24, and one or more standalone video servers 26." ('964 patent, 5:7-10 (Ex. 1001).) "The client computer is connected to the cameras 24 and video servers 26 via a network 28 which can include a private network segment 30 and a public network such as the Internet 32." ('964 patent, 5:10-14 (Ex. 1001).)

[3] The proposed claim construction is for this petition only. Petitioner reserves the right to advance different claim constructions in the related case *JDS Technologies, Inc. v. Exacq Technologies, Inc.*, Civil Action No. 2:15-cv-10387-AC.

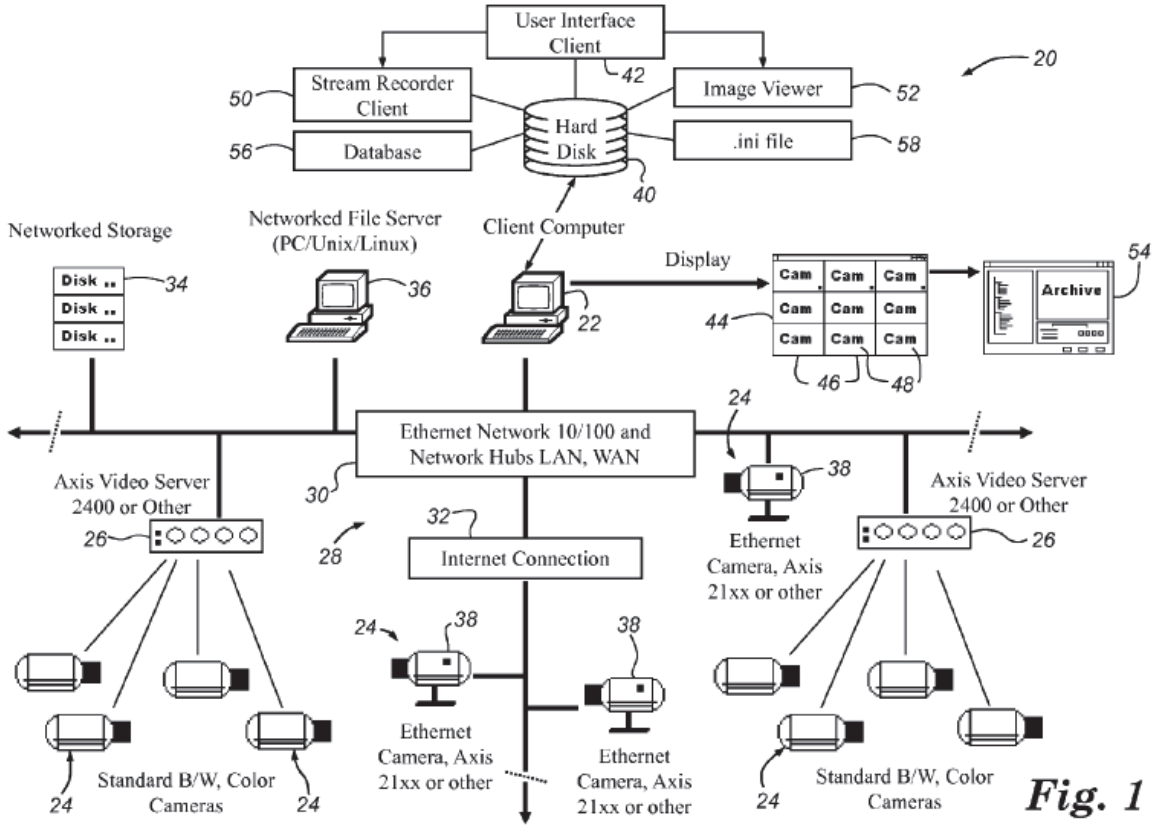


Fig. 1

The ’964 patent discusses the “client computer 22 includes a computer readable memory [] for digital storage of a user interface client application 42 that includes a user interface program along with a number of additional software components.” (’964 patent, 5:31-36 (Ex. 1001).) The ’964 patent describes the operation of the client program 42 as follows:

> In general, the user interface client program 42 is operable to access locally stored camera data that uniquely identifies the cameras 24 and then attempts access to those cameras over the network 28. The program 24 is operable to verify access to at least those cameras 24

> that are currently accessible, and to generate a user interface display 44 (on the computer's monitor) that includes a display window 46 for each of the cameras 24 accessed over the network 28, and to display in each of the display windows 46 an image 48 received from the camera associated with that display window.

('964 patent, 5:54-64 (Ex. 1001).)

The alleged invention relates to methods of controlling access to a video server, a camera, and a hardware device. (Ex. 1003).) For example, the '964 patent describes "retrieving embedded MAC addresses for purposes of validating access to the cameras 24 identified in the database 56." ('964 patent, 6:36-38; see also 6:43-48 ("If the user has selected "start" to begin accessing images or video, then the next step is to initialize and test the cameras and/or servers by verifying the IP addresses, testing for a valid MAC addresses, and, if the IP addresses and MAC addresses are valid, assigning the user settings and enabling or disabling individual cameras or servers.") (Ex. 1001).)

A. Summary of the Prosecution History

The '964 patent issued from U.S. Patent Application No. 12/708,394 ('394 application), filed on February 18, 2010. The '394 application is a continuation of U.S. Patent Application No. 11/125,795, filed on May 10, 2005 (now abandoned), which is a continuation of U.S. Patent Application No. 09/808,543, filed on March

14, 2001 (now U.S. Patent No. 6,891,566). U.S. Patent Application No. 09/808,543 claims the benefit of U.S. Provisional Application No. 60/189,162, filed on March 14, 2000. This Petition assumes, without conceding, the '964 patent's earliest priority date is March 14, 2000.[4]

VII. THE STATE OF THE ART BEFORE THE ALLEGED INVENTION SHOWS THE '964 PATENT CLAIMS NOTHING NEW OR NON-OBVIOUS

A. Systems of Networked Cameras Were Known

At the time of the '964 patent's earliest priority date, network cameras and video servers were well-known. The '964 patent acknowledges this in its background section:

> There now exists commercially available networkable cameras that can be accessed over networks running TCP/IP, including both LANs and global networks such as the Internet. Ethernet-based digital video servers are now common that are small, autonomous, and usually contain a web-based configuration utility, as well as administration software.

[4] Petitioner reserves the right to challenge whether the '964 is entitled to a priority date of March 14, 2000 in the related case *JDS Technologies, Inc. v. Exacq Technologies, Inc.*, Civil Action No. 2:15-cv-10387-AC.

('964 patent, 2:1-6 (Ex. 1001).) For example, there were several commercially-available network cameras and network video servers produced by Axis Communication AB. (*See* Axis 200 (describing prior art network camera) (Ex. (1007).) (*See* Axis 2100 (describing prior art network camera) (Ex. 1008).), (*See* Axis 2400 (describing prior art network video server) (Ex. 1009).). (*See* Thompson Decl. ¶ 34 (Ex. 1003).)

Systems also existed that connected together multiple networked cameras and video servers. (*See* Thompson Decl. ¶ 35 (Ex. 1003).) These systems tracked the cameras to which they connected, managed network communications with the network cameras, and obtained image data from the network cameras. (*See* Thompson Decl. ¶ 35 (Ex. 1003).) For example, U.S. Patent No. 6,166,729 to Acosta, filed May 7, 1997, discloses a remote viewing system 10 that includes "camera devices 12, a wireless network 14, a central office video management system (COVMS) 16." (Acosta, 4:26-28 (Ex. 1004).) (*See* Thompson Decl. ¶ 35 (Ex. 1003).)

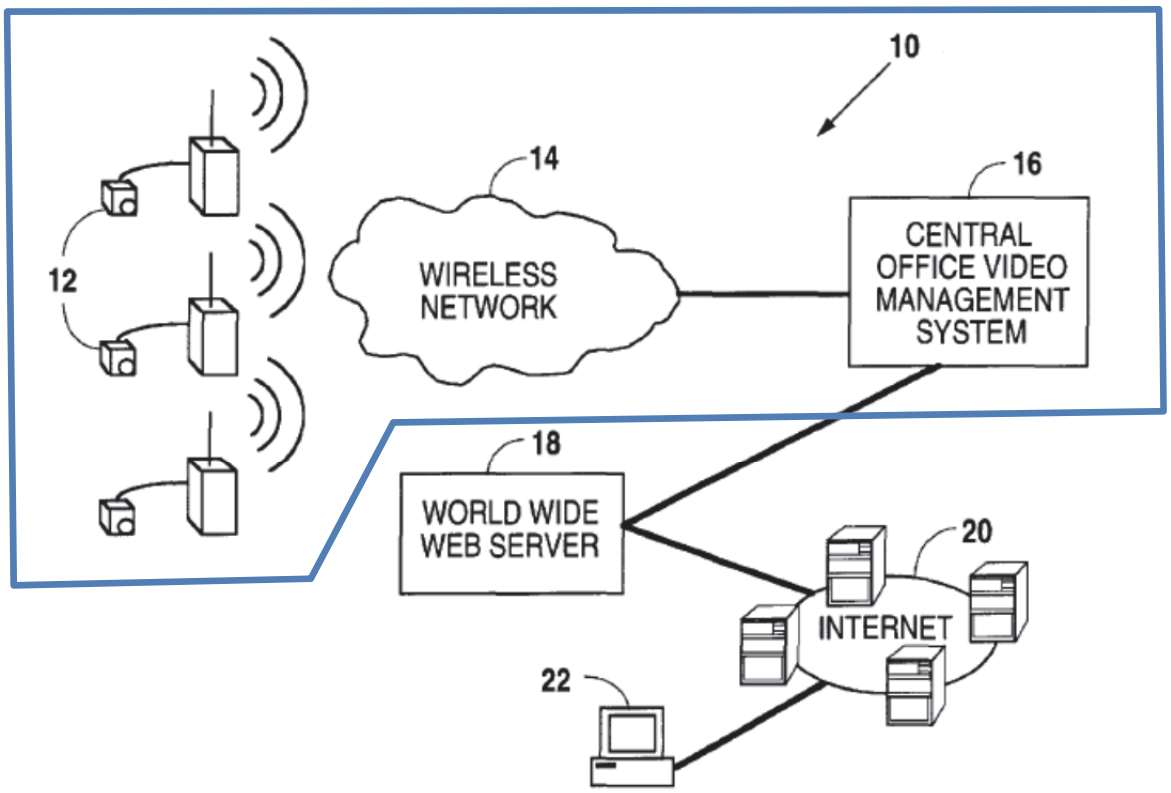


Fig. 1

FIG. 1 of Acosta (Ex. 1004)

Acosta describes that "at the camera 12, the digital data is processed, compressed, and then transmitted over the wireless network 14 to the COVMS 16." (Acosta, 7:29-31 (Ex. 1004).) "The COVMS 16 processes the images and then transfers them to the storage facility for archive, to the World Wide Web 18, and to dedicated connections with the COVMS 16 of certain users, if any." (Acosta, 8:9-12 (Ex. 1004).) Acosta also discloses using serial IDs identifying the camera elements 12 to determine whether the COVMS 16 is authorized to receive image

data from the camera elements 12. (See Acosta, 17:41-18:4 (the COVMS makes a "determination [] in a step 514 whether the camera element 12 is authenticated. If not, the process continues to the step 510 with an unauthorized access alarm and then returns to step 502.") (Ex. 1004).) (*See* Thompson Decl. ¶ 35 (Ex. 1003).)

B. MAC Addresses Were Used to Identify and Authorize Network Devices Long Before the Alleged Invention

MAC addresses, and using them to identify devices in a network, were well-known in computer networking long before the'964 patent's earliest priority date. Indeed, the Ethernet standard expressly states that a MAC address can be used for that purpose. (*See* Thompson Decl. ¶ 36 (Ex. 1003).) For example, the 1985 edition of the IEEE 802.3 standard describes the Media Access Control ("MAC") Frame Structure. (802.3 Standard at 23-27 (Ex. 1013).) The standard provides that "[e]ach MAC frame shall contain two address fields: the Destination Address field and the Source Address field, in that order." (802.3 Standard at 24 (Ex. 1013).) "The Source Address field *shall identify the station* from which the frame was initiated." (802.3 Standard at 24; see also 26 ("The Source Address field specifies the station sending the frame. The Source Address field is not interpreted by the CSMA/CD MAC sublayer.") (Ex. 1013).) (*See* Thompson Decl. ¶ 36 (Ex. 1003).)

Further, the prior art expressly recognizes advantages of using a MAC address as an identifier for a network device, including widespread use and near-

uniqueness. (*See* Thompson Decl. ¶ 37 (Ex. 1003).) For example, U.S. Patent No. 6,438,530 to Heiden et al., filed December 29, 1999, uses MAC addresses as a personal computer ("PC") "signature:" "[a]nother example of a PC signature for a computer that has Ethernet interface standard equipment is a unique ID called a 'MAC address' and every piece of Ethernet hardware ever manufactured has been assigned one under the supervision of a standards organization." (Heiden, 7:13-17 (Ex. 1011).) (See, also, Nelson, 1:54-58 ("[a] MAC layer address is usually statically associated with an individual network interface of a device, for example as stored within a non-volatile memory of a network interface card.") (Ex. 1006).) (*See* Thompson Decl. ¶ 37 (Ex. 1003).)

Using a MAC address to determine whether communications between systems on a network are authorized was also a known technique. (*See* Thompson Decl. ¶ 38 (Ex. 1003).) Networking technologies predating the alleged invention used a device's MAC address to determine whether to allow devices to communicate with other devices on the network. (*See* Thompson Decl. ¶ 38 (Ex. 1003).) For example, Holloway, which was filed January 9, 1997, describes prior art systems where "[t]here are token ring and Ethernet managed hubs that allow a network administrator to define, by MAC address, one or more authorized users per hub port. If an unauthorized MAC address is detected at the hub port, then the port is automatically disabled." (Holloway, 2:6-10 (Ex. 1005).) (*See* Thompson

Decl. ¶ 38 (Ex. 1003).) As another example, U.S. Patent No. 6,477,648 to Schell et al., filed March 23, 1997, describes using MAC addresses to determine which network devices are authorized to communicate: "the [network interface card] also includes a receive address confirmation circuit that functions to ensure that the trusted workstation does not receive packets from entities other than known/authorized servers. That is, the [network interface card] compares the source address of a packet received over the network to verify that it is from a authorized server." (Schell, 2:25-30 (Ex. 1012).) (*See* Thompson Decl. ¶ 38 (Ex. 1003).)

C. It Was Obvious to Apply Networking Techniques to Systems of Networked Cameras

The claims of the '964 patent merely recite applying commonplace networking techniques in the context of networked camera systems then known in the art. (*See* Thompson Decl. ¶ 39 (Ex. 1003).)

A person of ordinary skill in the art at the time would have been well-acquainted with these networking techniques and appreciated their applicability to systems of networked cameras because the techniques are as applicable to connecting networked cameras as they are to connecting other networked devices. (*See* Thompson Decl. ¶ 40 (Ex. 1003).) Many of the same problems are addressed, such as how devices on the network identify each other and how to control which

devices on the network are able to communicate. (*See* Thompson Decl. ¶ 40 (Ex. 1003).) For example, a person of ordinary skill at the time of the alleged invention, and long before, would have understood and appreciated that a MAC address can be used to identify devices on a network, including networked cameras. (*See* Thompson Decl. ¶ 40 (Ex. 1003).) Further, a person of ordinary skill would also appreciate that the MAC address could be used for authorization purposes, such as by comparing the MAC address of a network device to a list of authorized MAC addresses. (*See* Thompson Decl. ¶ 40 (Ex. 1003).)

To one of ordinary skill, the use of these networking techniques amounts to routine design choices. As discussed above, identifying networked devices by their MAC addresses was a common approach taken in networked systems, as was using the MAC address as a device identifier for authorization. (*See* Thompson Decl. ¶ 41 (Ex. 1003).) Accordingly, applying these well-known networking techniques to prior art networked camera systems would have been obvious to one of skill in the art at the time of the alleged invention. (*See* Thompson Decl. ¶ 41 (Ex. 1003).)

VIII. CLAIMS 1-4 OF THE '964 PATENT ARE UNPATENTABLE

A detailed explanation of the relevance and manner of applying the prior art references to claims 1-4 of the '964 patent is provided below.

A. Claims 1 and 3 are Anticipated by Acosta

As described in detail below, Acosta discloses each element of claims 1 and 3. (*See* Thompson Decl. ¶¶ 42-59 (Ex. 1003).)

1. *Claim 1*

a. [1p.] A method of controlling access by a computer to a video server

Acosta discloses "a method of controlling access by a computer to a video server." (*See* Thompson Decl. ¶ 43 (Ex. 1003).) For example, Acosta discloses a method of controlling access by the computer running a central office video management system ("COVMS") 16 to a camera element 12 over a network 14. (See Acosta, 17:41-18:30 (Ex. 1004).) (*See* Thompson Decl. ¶ 43 (Ex. 1003).)

In particular, Acosta discloses that the CommLink Manager of the COVMS 16 controls access to the camera elements 12 and makes "[a] determination . . . whether the camera element 12 is authenticated." (Acosta, 17:62-64 (Ex. 1004).) If the camera element is not authenticated, the CommLink Manager of the COVMS 16 sends "an unauthorized access alarm" and does not configure the COVMS 16 to receive image data from the camera element 12. (See Acosta 17:53-66 (Ex. 1004).) (*See* Thompson Decl. ¶ 44 (Ex. 1003).)

Acosta discloses the COVMS 16 runs on one or more host computers 78 that each are "a dual Pentium Pro 180 MHZ system with 128-256 MB of memory

running the FreeBSD operating system." (Acosta, 6:18-20; See also 13:36-41 ("the COVMS 16 determines whether there are one or more of the host computers 78 of the COVMS 16. If there are more than one of the host computers 78 in the COVMS 16, then each is assigned an ordinal ID from one of the host computers 78 arbitrarily designated as the master of the host computers 78.") (Ex. 1004).) Thus, the COVMS restricts the host computer's 78 access to camera elements 12. (*See* Thompson Decl. ¶ 45 (Ex. 1003).)

Further, the camera elements 12 are video servers because they transmit image data over network 14 to the COVMS 16 running on host computer 78. Acosta discloses "the camera device 12 includes a camera 24, a video digitizer 26, a processor card 28, a remote communications link module 30, an antenna 32, and a power supply 34." (Acosta, 4:42-45 (Ex. 1004).) In operation, "the cameras 12 acquires images at the site at which located and converts those images to digital data information," and "[a]t the camera 12, the digital data is processed, compressed, and then transmitted over the wireless network 14 to the COVMS 16." (Acosta, 7:27-31 (Ex. 1004).) (*See* Thompson Decl. ¶ 46 (Ex. 1003).)

b. [1a.] sending a request from the computer to a video server over a network;

Acosta discloses "sending a request from the computer to a video server over a network." For example, Acosta discloses the "COVMS 16, in a step 522,

then sends a transmit request to the camera element 12 for the particular configuration record applicable to the camera element 12." (Acosta, 18:7-10 (Ex. 1004).) (*See* Thompson Decl. ¶ 47 (Ex. 1003).)

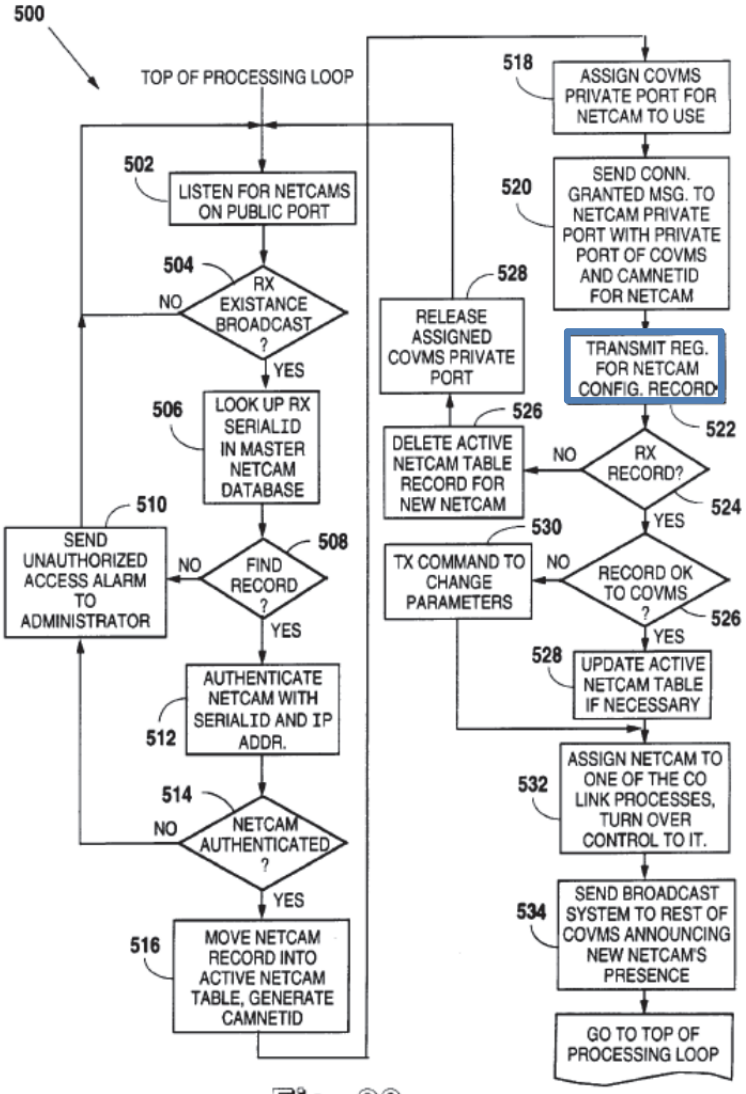


Fig. 20

c. [1b.] receiving at the computer from the video server a unique identifier stored in and identifying the video

server, wherein the unique identifier is received by the computer over the network

Acosta discloses "receiving at the computer from the video server a unique identifier stored in and identifying the video server, wherein the unique identifier is received by the computer over the network." For example, Acosta discloses receiving at the COVMS 16, from camera element 12, a serial ID uniquely identifying the camera element. Acosta further discloses the serial ID is stored on the camera element 12, and sent by the camera element 12 to the COVMS 16 over network 14. (*See* Thompson Decl. ¶ 48 (Ex. 1003).)

Acosta illustrates in "FIG. 20, a process 500 of the CommLink Manager begins with the COVMS 16 listening for the camera elements 12 sending existent broadcasts in a step 502." (Acosta, 17:41-44 (Ex. 1004).) Then, "[i]n a step 504, the COVMS 16 tests whether an incoming broadcast is detected. . . .[and] [i]f an incoming broadcast is detected, that broadcast includes the serial ID for the camera 12." (Acosta, 17:44-48 (Ex. 1004).) FIG. 20 is reproduced below:

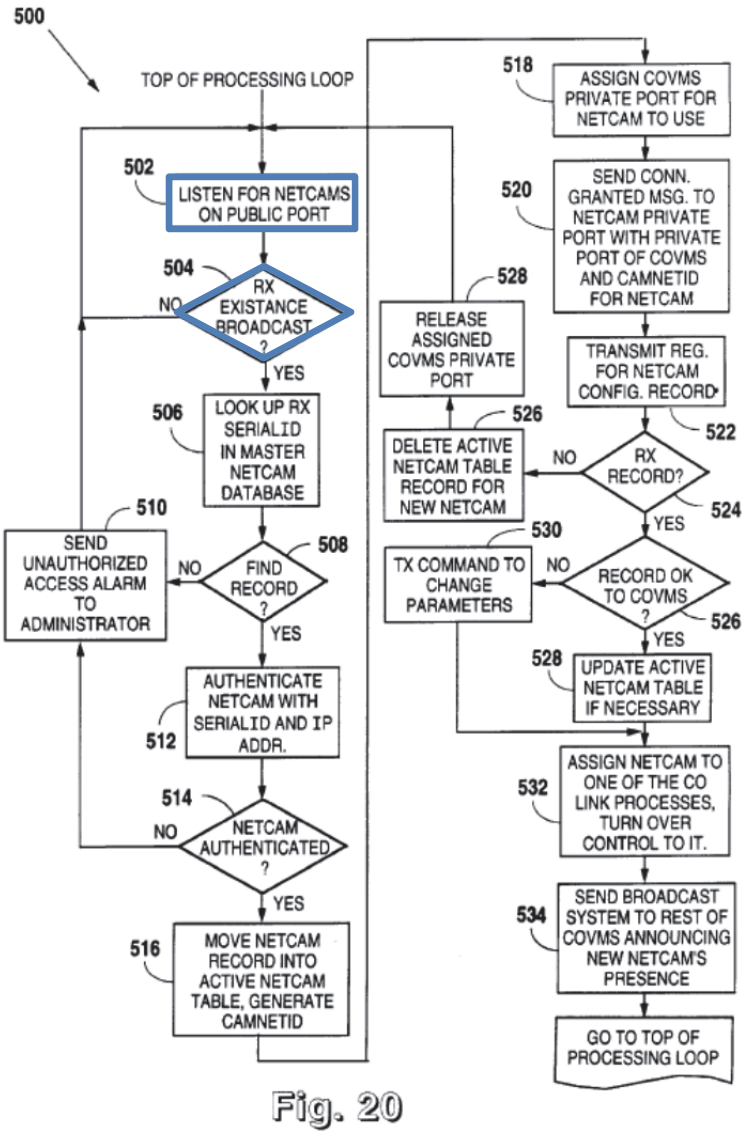


Fig. 20

Acosta FIG. 20 (highlighting added).

Accordingly, Acosta discloses the COVMS 16 receiving the serial ID from camera element 12. (*See* Thompson Decl. ¶ 49 (Ex. 1003).)

One of skill in the art would understand that the serial ID identifies camera element 12 to the COVMS 16. For example, the COVMS 16 uses the serial ID to

identify the camera for authentication purposes. (See, e.g., Acosta, 17:60-63 ("the camera element 12 is authenticated according to the ID and is assigned an IP address in a step 512") (Ex. 1004).) (*See* Thompson Decl. ¶ 50 (Ex. 1003).)

One of skill in the art would further understand that because the serial ID is used to identify and authenticate the camera element 12, it must be unique within the system described by Acosta for the authentication function to be effective. Acosta discloses the COVMS 16 receives the serial ID over network 16 because "[t]he cameras 12 communicate with the COVMS 16 over the wireless network 14." (Acosta, 7:43-44 (Ex. 1004).). Finally, one of ordinary skill in the art would appreciate that the serial ID is necessarily stored by the camera element 12. For example, it would be necessary for the camera element to store the serial ID in order to then transmit it as described in Acosta. (*See* Thompson Decl. ¶ 51 (Ex. 1003).)

d. [1c.] determining that access to the video server is authorized by comparing the unique identifier received by the computer to one or more authorized unique identifiers and

Acosta discloses "determining that access to the video server is authorized by comparing the unique identifier received by the computer to one or more authorized unique identifiers." For example, Acosta discloses the COVMS 16 determining that access to the camera element 12 is authorized by comparing the

serial ID received from camera element 12 to serial IDs in a database on the COVMS 16. (*See* Thompson Decl. ¶ 52 (Ex. 1003).)

Again with reference to FIG. 5 of Acosta, after the COVMS 16 detects an incoming broadcast, "[t]he COVMS 16, in a step 506, looks up the serial ID assigned to the camera element 12 making the broadcast in a database of the COVMS 16 containing the serial ID's for all of the camera elements 12 then operating and obtains an IP address for the particular camera element 12." (Acosta, 17:48-53 (Ex. 1004).) (*See* Thompson Decl. ¶ 53 (Ex. 1003).)

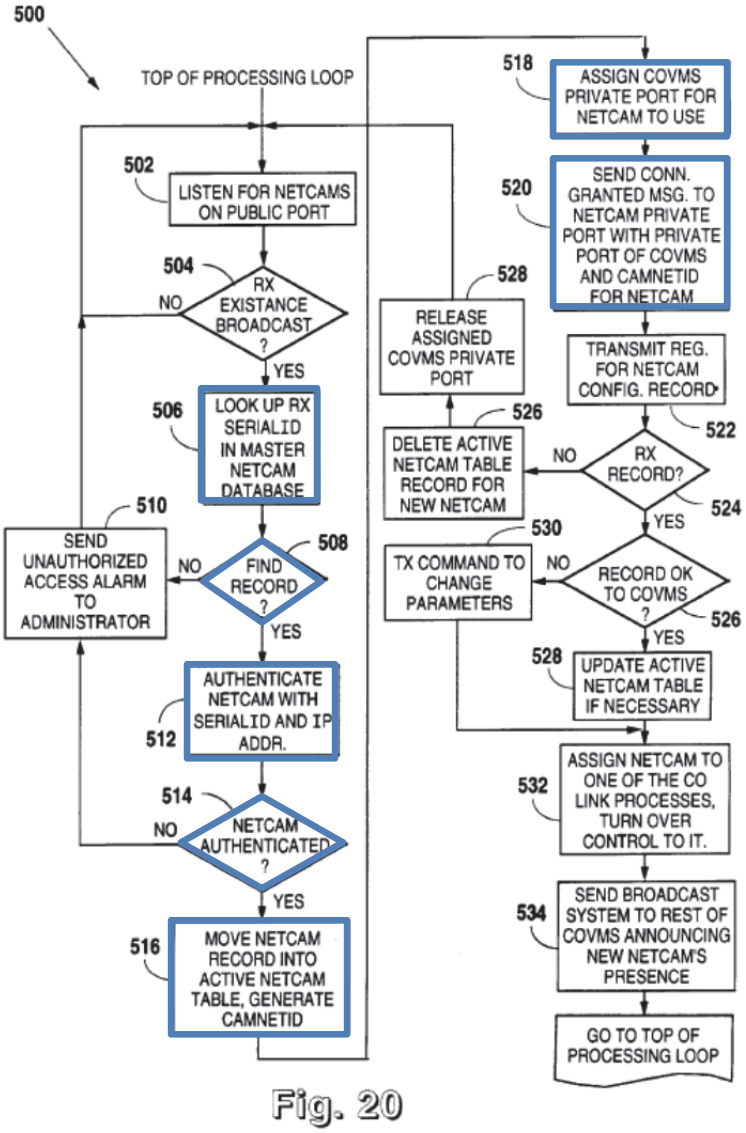


Fig. 20

Acosta FIG. 20 (highlighting added).

Then, "[i]n a step 508, it is determined whether the particular ID and IP address match, and whether the related database record is found." (Acosta, 17:53-55 (Ex. 1004).) Acosta describes that if the related database record is not found, the COVMS 16 determines the camera is not authorized, and the method

"continues to a step 510 of the COVMS 16 sending an unauthorized access alarm to a system administrator, for example, via the administrative computer of the system 16." (Acosta, 17:55-59 (Ex. 1004).) Thus Acosta discloses the COVMS 16 determining that it is not authorized to access the camera element 12 based on a comparison between the serial ID received from the camera element 12 and the serial IDs in the COVMS 16 database (i.e., the authorized serial IDs). (*See* Thompson Decl. ¶ 54 (Ex. 1003).)

The COVMS 16 performs additional authentication based on comparing the received serial ID to serial IDs in the COVMS 16 database: "If the ID and database record are found in the step 508, the camera element 12 is authenticated according to the ID and is assigned an IP address in a step 512." (Acosta, 17:60-62 (Ex. 1004).) If the COVMS determines the camera element 12 is not authenticated, the COVMS raises an unauthorized access alarm. (Acosta, 17:62-66 (Ex. 1004).) Thus Acosta further discloses the COVMS 16 determining that it is not authorized to access the camera element 12 based on a comparison the received serial ID. (*See* Thompson Decl. ¶ 55 (Ex. 1003).)

In contrast, if the camera element 12 "is authenticated, however, the database record for the camera element 12 is moved, in a step 516, into an active table from which is generated a specific identifier for the camera element 12." (Acosta, 17:66-18:2 (Ex. 1004).) The COVMS 16 then assigns "[i]n a step 518, a

particular port of the COVMS 16 . . . for use by the camera element 12 in communications with the COVMS 16." (Acosta, 18:2-4 (Ex. 1004).) Having authenticated the camera element 12, "[i]n a step 520, the COVMS 16 then sends a connection granted message to the camera element 12 via the particular port and the specific identifier." (Acosta, 18:5-7 (Ex. 1004).) (*See* Thompson Decl. ¶ 56 (Ex. 1003).)

e. [1d.] in response to the determination, obtaining at the computer one or more images from the video server for displaying

Acosta discloses "in response to the determination, obtaining at the computer one or more images from the video server for displaying." For example, Acosta discloses the COVMS 16 obtaining images for displaying from camera element 12 in response to determining that the camera element 12 is authorized. (*See* Thompson Decl. ¶ 57 (Ex. 1003).)

Referring to FIG. 5, Acosta discloses that in response to determining the COVMS 16 is authorized to access the camera element 12:

> [i]n a step 534, the COVMS 16 notifies each of its components that the camera element 12 is linked with the system 10. A link message is sent to all components of the system. When the Image Processing Manager receives the link message, it looks for the link and sets up a queue for input."

(Acosta, 18:24-28 (Ex. 1004).) The input queue is used for receiving images from camera element 12: "During set-up of the camera element 12, the CommLink Manager directs the communication link to dump received encoded image data to the designated input queue." (Acosta, 18:36-39 (Ex. 1004).) The images received by the COVMS 16 are for displaying. (See, e.g., Acosta, at Abstract ("A remote viewing system is for viewing digital images of remote locations.") (Ex. 1004).) (*See* Thompson Decl. ¶ 58 (Ex. 1003).)

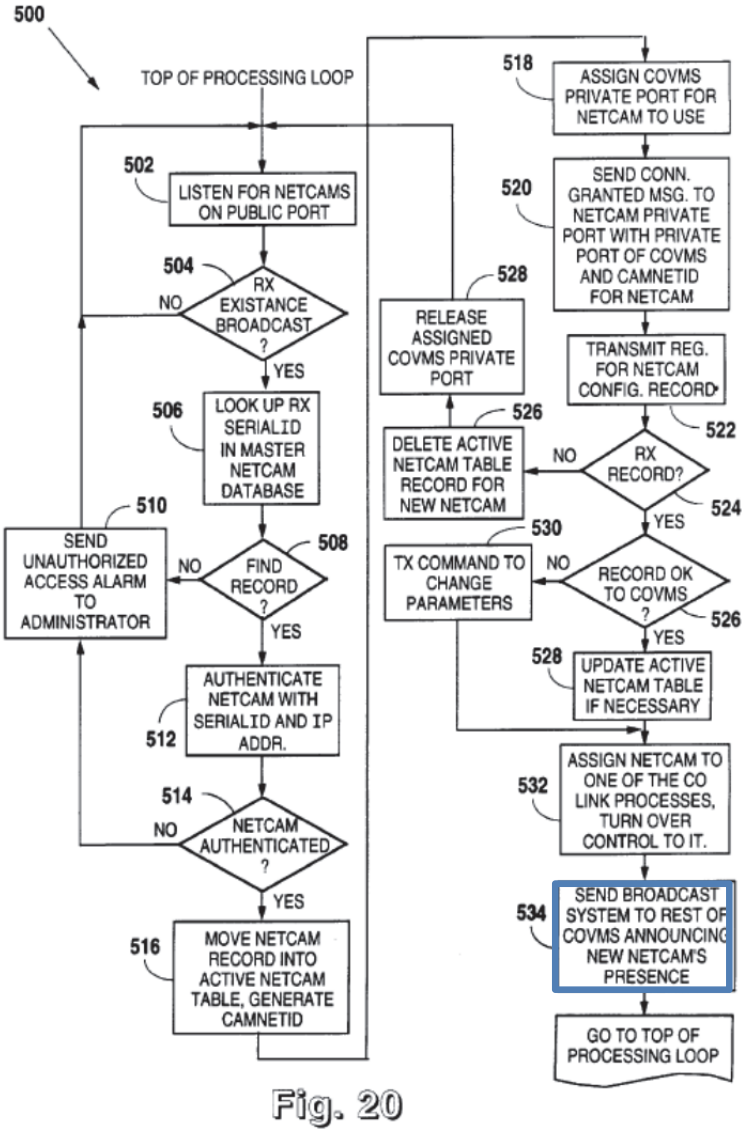


Fig. 20

Acosta FIG. 20 (highlighting added).

2. ***Claim 3: The method of claim 1, wherein the video server is a camera server that includes a camera and a web server with an Ethernet port or a component based video server including inputs for one or more analog video feeds.***

Acosta discloses "the video server is a camera server that includes a camera and a web server with an Ethernet port or a component based video server

including inputs for one or more analog video feeds." For example, Acosta discloses camera element 12 is a component based video server including inputs for one or more analog feeds. (*See* Thompson Decl. ¶ 60 (Ex. 1003).)

Acosta discloses the camera element is a component based video server: "Referring to FIG. 2, the camera device 12 includes a camera 24, a video digitizer 26, a processor card 28, a remote communications link module 30, an antenna 32, and a power supply." (Acosta, 4:43-45 (Ex. 1004).) As illustrated in FIG. 2, the camera element includes an input for one or more analog fees. (*See* Thompson Decl. ¶ 61 (Ex. 1003).)

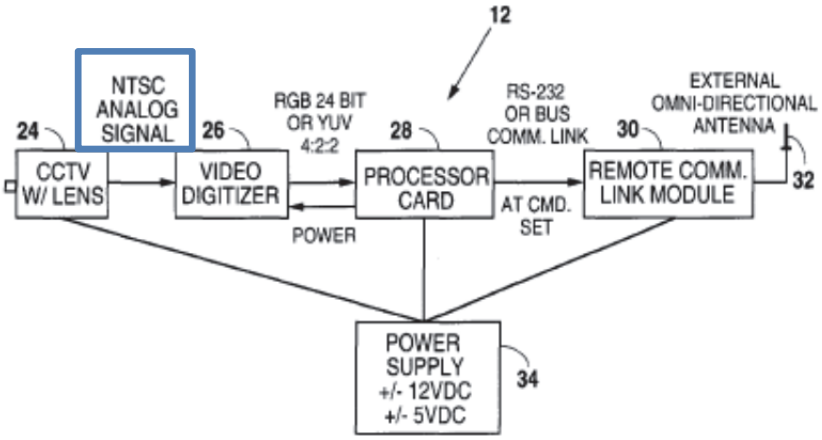


Fig. 2

Acosta FIG. 2 (highlighting added).

B. Claims 2 and 3 are Rendered Obvious by Acosta and Axis 200

As described in detail below, Acosta and Axis 200 render claims 2-3 obvious. (*See* Thompson Decl. ¶¶ 63-73 (Ex. 1003).)

1. *Claim 2: The method of claim 1, wherein the unique identifier is a MAC address.*

Acosta in combination with Axis 200 disclose "the unique identifier is a MAC address." As discussed with respect to claim 1, Acosta discloses a system for determining whether the COVMS 16 is authorized to access the camera element 12. In Acosta, the COVMS 16 receives a serial ID from the camera element 12, the serial ID identifying the camera element 12. The COVMS 16 then determines whether it is authorized to access the camera element 12 by comparing the received serial ID to its master database of camera serial IDs. (*See* Thompson Decl. ¶ 64 (Ex. 1003).)

To the extent that Acosta does not disclose that the serial ID can be a MAC address, Axis 200 discloses this element. (*See* Thompson Decl. ¶ 65 (Ex. 1003).) In particular, Axis 200 discloses a network camera ("Axis 200 camera") with a serial number that is the same as its MAC address. (See Axis 200 at 12 ("Serial Number Please note that the serial number of your AXIS 200 is identical to the Ethernet address of the unit.") (Ex. 1007).) (*See* Thompson Decl. ¶ 65 (Ex. 1003).) One of skill in the art would understand that the Ethernet address referenced in

Axis 200 is the network camera's MAC address. (*See* Thompson Decl. ¶ 65 (Ex. 1003).)

It would have been obvious to modify Acosta's COVMS 16 to be interoperable with the Axis 200 camera instead of or in addition to camera elements 12. (*See* Thompson Decl. ¶ 66 (Ex. 1003).) Acosta and Axis are within the same field of endeavor—networked camera systems. (*See* Thompson Decl. ¶ 66 (Ex. 1003).) Further, they provide complimentary teachings—Acosta describes a COVMS 16 that communicates with several networked camera elements 12, and Axis 200 describes a network camera. (*See* Thompson Decl. ¶ 66 (Ex. 1003).)

Acosta's COVMS 16 is also readily combinable with the Axis 200 camera. (*See* Thompson Decl. ¶ 67 (Ex. 1003).) Acosta describes that "[t]he cameras 12 use the TCP/IP protocol suite for communications over the wireless communications links of the wireless network 14." (Acosta, 7:31-33 (Ex. 1004).) The Axis 200 camera similarly uses TCP/IP: "The AXIS 200 supports TCP/IP and Internet related protocols." (Axis 200 at 6 (Ex. 1007).) (*See* Thompson Decl. ¶ 67 (Ex. 1003).) It would have been within the skill of one in the art to modify Acosta's COVMS 16 to be interoperable with the Axis 200 camera without substantially modifying the architecture of the COVMS 16. (*See* Thompson Decl. ¶ 67 (Ex. 1003).) One of skill in the art would be motivated to do so to increase the network camera devices supported by COVMS 16. (*See* Thompson Decl. ¶ 67

(Ex. 1003).) Thus, modifying Acosta's COVMS 16 to communicate with the Axis 200 camera instead of, or in addition to, camera elements 12 would be the simple substitution of one known, equivalent element for another to obtain the predictable result of interoperability between the COVMS 16 and the Axis 200 camera. (*See* Thompson Decl. ¶ 67 (Ex. 1003).)

In making the COVMS 16 interoperable with the Axis 200 camera, it would have been obvious to modify the COVMS 16 of Acosta to use the MAC address of the Axis 200 camera for authorization. (*See* Thompson Decl. ¶ 68 (Ex. 1003).) As discussed above in Section VII, using a network device's MAC address to identify it when determining whether devices are authorized to communicate was well known. This modification of the COVMS of Acosta would have been a matter of routine design choice yielding predictable results—a way to identify the Axis 200 camera for authorization purposes.

Thus, the combination of Acosta and Axis 200 discloses the unique identifier is a MAC address. (*See* Thompson Decl. ¶ 69 (Ex. 1003).)

2. ***Claim 3: The method of claim 1, wherein the video server is a camera server that includes a camera and a web server with an Ethernet port or a component based video server including inputs for one or more analog video feeds.***

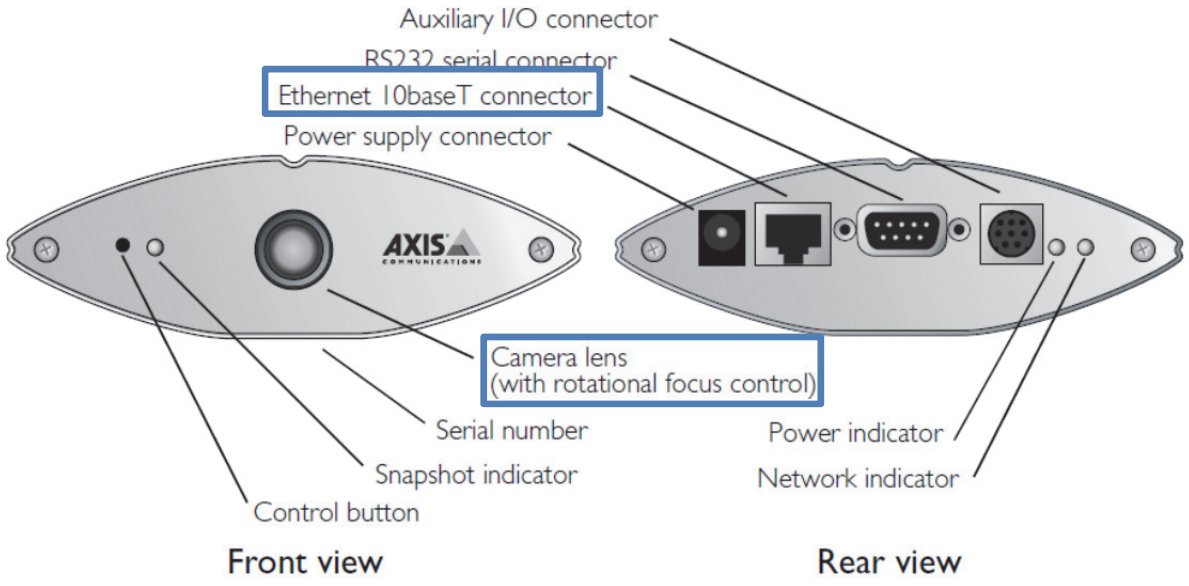
Acosta in combination with Axis 200 discloses "the video server is a camera server that includes a camera and a web server with an Ethernet port or a

component based video server including inputs for one or more analog video feeds." As discussed above, Acosta discloses camera element 12 is a component based video server including inputs for one or more analog feeds. (*See* Thompson Decl. ¶ 70 (Ex. 1003).)

To the extent Acosta does not disclose the video server is a camera server that includes a camera and a web server with an Ethernet port, Axis 200 discloses this element. For example, Axis 200 discloses "[t]he AXIS 200 Network Camera is a digital snapshot camera with a built-in Web server." (Axis 200 at 5 (Ex. 1007).) (*See* Thompson Decl. ¶ 71 (Ex. 1003).) In particular:

> the AXIS 200 is a microprocessor-based device that includes:
>
> - A digital color camera
> - RISC-based hardware for image compression
> - Standalone Web server functionality
> - Physical Ethernet connection

(Axis 200 at 5; see also Axis 200 at 11 (illustrating camera and Ethernet port):



(*See* Thompson Decl. ¶ 71 (Ex. 1003).)

As discussed above with respect to claim 3, a person of ordinary skill in the art would have been motivated to combine Acosta's COVMS 16 with the Axis 200 camera. (*See* Thompson Decl. ¶ 72 (Ex. 1003).)

C. Claim 4 is Rendered Obvious by Acosta, Axis 200, and Nelson

As described in detail below, Acosta, Axis 200, and Nelson render claim 4 obvious. (*See* Thompson Decl. ¶¶ 74-86 (Ex. 1003).)

1. *Claim 4*

a. [4p.] A method of controlling access by a computer to a hardware device, comprising the following steps performed at the computer:

Acosta discloses "[a] method of controlling access by a computer to a hardware device . . . performed at the computer." (*See* Thompson Decl. ¶ 43 (Ex. 1003).) For example, Acosta discloses a method of controlling access by the computer running a central office video management system ("COVMS") 16 to a camera element 12 over a network 14. (*See* Acosta, 17:41-18:30 (Ex. 1004).) (*See* Thompson Decl. ¶ 43 (Ex. 1003).) As discussed above with respect to claim element [1p.], Acosta discloses this claim element. (*See* Thompson Decl. ¶¶ 43-46 (Ex. 1003).)

b. [4a.] executing a computer program stored in computer readable form at the computer, the computer being connected to a hardware device via a network;

Acosta discloses "executing a computer program stored in computer readable form at the computer, the computer being connected to a hardware device via a network." (*See* Thompson Decl. ¶ 76 (Ex. 1003).) For example, Acosta discloses executing the software of the COVMS 16 on a host computer 78. Acosta further discloses that the host computer executing the COVMS 16 is connected to camera element 12 via network 14.

Acosta discloses the COVMS 16 comprises software. (*See* Acosta, 13:23-30 ("upon booting the COVMS 16, the COVMS 16 initially proceeds through a method 300 of initialization of the system 10 . . . The method 300 proceeds with a step 302 in which the Business Manager checks and matches hardware and software release versions of the system 10 in order to ensure that all are properly compatible and supported.") (Ex. 1004).) Acosta discloses the COVMS 16 runs on one or more host computers 78 that each are "a dual Pentium Pro 180 MHZ system with 128-256 MB of memory running the FreeBSD operating system." (Acosta, 6:18-20; see also 13:36-41 ("the COVMS 16 determines whether there are one or more of the host computers 78 of the COVMS 16. If there are more than one of the host computers 78 in the COVMS 16, then each is assigned an ordinal ID from one of the host computers 78 arbitrarily designated as the master of the host computers 78." (Ex. 1004).) (*See* Thompson Decl. ¶ 77 (Ex. 1003).) One of skill in the art would understand the software of the COVMS is stored in computer readable form at the host computer 78 in order for host computer 78 to execute the software. (*See* Thompson Decl. ¶ 77 (Ex. 1003).) Finally, Acosta discloses "[t]he cameras 12 communicate with the COVMS 16 over the wireless network 14." Acosta 7:43-44. (*See* Thompson Decl. ¶ 77 (Ex. 1003).)

c. [4b.] accessing the hardware device from the computer over the network using an IP address associated with the hardware device

Acosta discloses "accessing the hardware device from the computer over the network using an IP address associated with the hardware device." Acosta disclosed the COVMS 16 accessing the camera element 12 using an IP address associate with the camera element 12. (*See* Thompson Decl. ¶ 78 (Ex. 1003).)

Acosta discloses "[t]he cameras 12 communicate with the COVMS 16 over the wireless network 14," and "[t]he cameras 12 use the TCP/IP protocol suite for communications over the wireless communications links of the wireless network 14." (Acosta, 7:31-33; see also 17:33-35 ("The CommLink Manager maps each ID into an IP address before processing communication requests related to the particular communication.") (Ex. 1004).) (*See* Thompson Decl. ¶ 79 (Ex. 1003).) Thus, Acosta discloses communications between the COVMS 16 and camera element use an IP address associated with camera element 12 because the TCP/IP suite is used. (*See* Thompson Decl. ¶ 79 (Ex. 1003).)

Acosta further discloses that the COVMS 16 accesses the camera element 12 by sending requests for data to the camera element 12 and receiving data from the camera element 12 in response. For example, after authenticating the camera element 12, "[t]he COVMS 16, in a step 522, then sends a transmit request to the camera element 12 for the particular configuration record applicable to the camera

element 12." (Acosta, 18:7-10 (Ex. 1004).) (*See* Thompson Decl. ¶ 80 (Ex. 1003).) The COVMS 16 then receives the configuration record from the camera element 12 and performs further processing. (Acosta, 18:10-19 ("A determination is made in a step 524 whether the record is received by the COVMS 16 from the camera element 12 . . . If in the step 524 it is determined that the record is received, the COVMS 16 in a step 526 assesses whether the record is suitable.") (Ex. 1004).) (*See* Thompson Decl. ¶ 80 (Ex. 1003).)

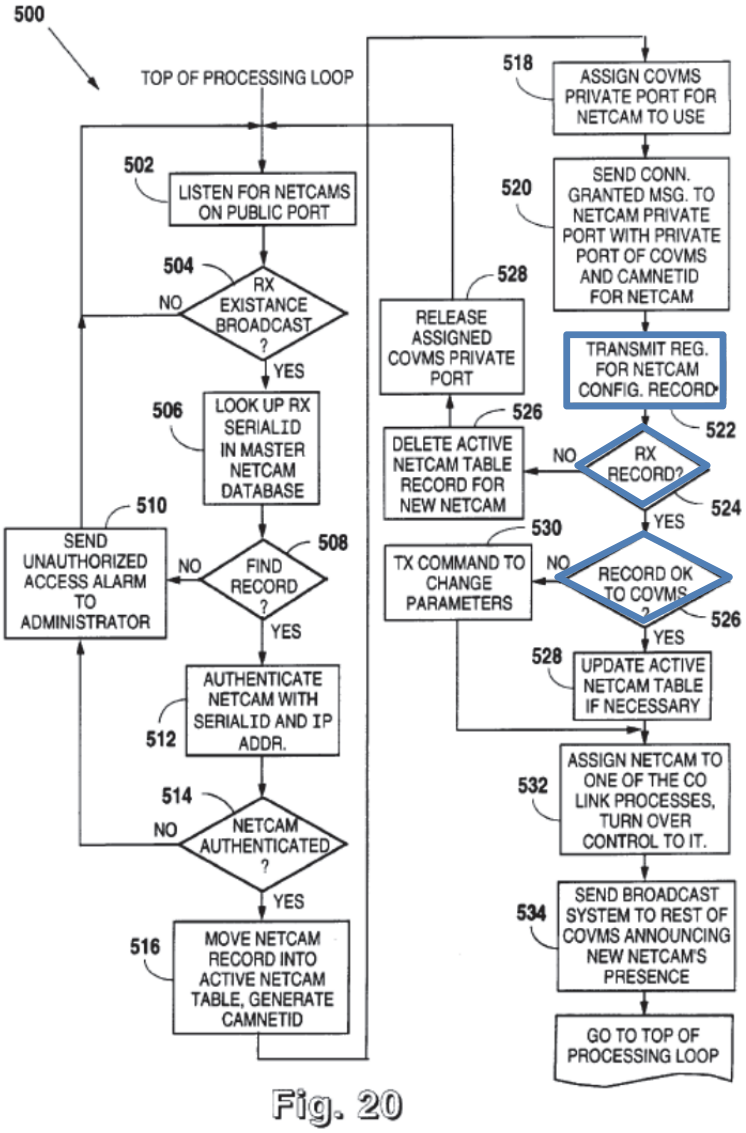


Fig. 20

Acosta FIG. 20 (highlighting added).

d. [4c.] transmitting a request from the computer over the network for a MAC address of the hardware device

Acosta in combination with Axis 200 and Nelson disclose "transmitting a request from the computer over the network for a MAC address of the hardware device." As discussed above with respect to claim 3, Acosta and Axis 200 disclose the COVMS 16 using a MAC address received from the Axis 200 camera to determine whether it is authorized to access the Axis camera 200 by comparing the received MAC address to as stored list of authorized MAC addresses. (*See* Thompson Decl. ¶ 81 (Ex. 1003).)

To the extent Acosta and Axis 200 do not disclose transmitting a request from the computer over the network for a MAC address of the hardware device, Nelson discloses this element. For example, Nelson discloses a "method for determining a MAC layer address of a network interface on a remote device, based on an IP address associated with the same network interface on the remote device." (Nelson, Abstract (Ex. 1006).) (*See* Thompson Decl. ¶ 82 (Ex. 1003).) To determine a MAC address for the remote device, a system "identifies the network interface of the last internetworking device along the route to the remote device that is coupled to the remote subnet to which the interface of the remote device is also coupled." (Nelson, 3:49-52 (Ex. 1006).) (*See* Thompson Decl. ¶ 82 (Ex.

1003).). The system then sends a request for the MAC address for the remote device:

> The system then accesses a cache of MAC layer addresses within the last internetworking device to determine a MAC address of the network interface of the remote device that is associated with the same IP address as provided in the original request.

(Nelson, 3:52-57 (Ex. 1006).) (*See* Thompson Decl. ¶ 82 (Ex. 1003).)

It would have been obvious to modify Acosta's COVMS 16 to send a request for the MAC address of the Axis 200 camera. (*See* Thompson Decl. ¶ 83 (Ex. 1003).) One of skill in the art would have appreciated that in order to obtain the MAC address of the Axis 200 camera, the COVMS 16 could wait to passively receive it, as in Acosta, or actively request it, as in Nelson. (*See* Thompson Decl. ¶ 83 (Ex. 1003).) Whether Acosta's COVMS 16 waited to receive the MAC address or requested it would have would have been a matter of routine design choice yielding predictable results. (*See* Thompson Decl. ¶ 83 (Ex. 1003).)

e. [4d.]receiving at the computer the MAC address of the hardware device over the network; and

Acosta in combination with Axis 200 discloses "receiving at the computer the MAC address of the hardware device over the network." As discussed above with respect to claim element [1b.], Acosta discloses the COVMS 16 receiving the

serial ID of camera element 12 over network 14. (*See* Thompson Decl. ¶ 84 (Ex. 1003).) Further, as discussed above with respect to claim 2, it would have been obvious to modify the system of Acosta to use the MAC address of the camera element 12 as the identifiers. (*See* Thompson Decl. ¶ 84 (Ex. 1003).)

f. [4e.] determining if the computer program is authorized to access the hardware device by validating the MAC address using data accessible to the computer.

Acosta in combination with Axis 200 discloses "determining if the computer program is authorized to access the hardware device by validating the MAC address using data accessible to the computer." As discussed above with respect to claim element [1c.], Acosta discloses the COVMS 16 determining if it is authorized to access the camera element 12 by receiving the serial ID of camera element 12 over network 14. (*See* Thompson Decl. ¶ 85 (Ex. 1003).) Further, as discussed above with respect to claim 2, it would have been obvious to modify the system of Acosta to use the MAC address of the camera element 12 as the identifiers. (*See* Thompson Decl. ¶ 85 (Ex. 1003).)

IX. CONCLUSION

For the foregoing reasons, claims 1-4 of the '964 patent are anticipated and/or obvious. Petitioner respectfully requests institution of IPR for Claims 1-4 of the '964 Patent because there is a reasonable likelihood that Petitioner will

prevail with respect to at least one of these claims challenged in this Petition. Petitioner respectfully requests that these claims be declared unpatentable and canceled.

Respectfully submitted,

By: /Steven M. Bauer/

Steven M. Bauer, Reg. No. 31,481
Joseph A. Capraro Jr., Reg. No. 36,471
Proskauer Rose LLP
One International Place
Boston, MA 02110
Tel: (617) 526-9600

Attorney Docket: EXC-964IPR

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inter Partes Review Case No. IPR2016-00567

Inter partes Review of: U.S. Patent No. 8,185,964
Issued: May 10, 2005
To: Joseph Robert Marchese
For: Digital Video System Using Networked Cameras

CERTIFICATE OF SERVICE UNDER 37 C.F.R. § 42.6(e) AND 42.105(a)

Dear Sir:

Pursuant to 37 C.F.R. § 42.6(e) and 42.105(a), I hereby certify that on February 5, 2016, I caused a complete copy of the Petition for *Inter Partes* Review of U.S. Patent No. 8,185,964 and all supporting exhibits to be served on the Patent Owner of the subject patent at the correspondence address of record as follows:

By PRIORITY MAIL® to:

Brooks Kushman P.C.
1000 Town Center
Twenty-Second Floor
Southfield, MI 48075

By: /Steven M. Bauer/

Steven M. Bauer, Reg. No. 31,481
Joseph A. Capraro Jr., Reg. No. 36,471
Proskauer Rose LLP
One International Place
Boston, MA 02110
Tel: (617) 526-9600