# Exacq Technologies, Inc.
# Exhibit 1003

Attorney Docket: EXC-964IPR

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

*Inter partes* Review Case No. IPR2016-_____

*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

**DECLARATION OF GREG THOMPSON**
**REGARDING U.S. PATENT NO. 8,185,964**

## Table of Contents

I, Greg Thompson, declare:

1. I make this declaration based on personal knowledge, and I am competent to testify about the matters set forth herein.

2. I have been retained by counsel for the Petitioner to review relevant materials and render my expert opinion in connection with technical matters related to U.S. Patent No. 8,185,964 ("'964 patent") (Ex. 1001). I submit this declaration in connection with Petitioner's Petition for *Inter Partes* Review of Claims 1-4 of U.S. Patent No. 8,185,964 ("Petition"). I am being compensated for my time at a rate of $200 per hour, plus actual expenses. My compensation is not dependent in any way upon the outcome of this Petition.

3. For at least the reasons expressed in this declaration, I agree with the contents of the Petition.

## I. PERSONAL BACKGROUND AND QUALIFICATIONS

4. My professional career has spanned close to 38 years. During these years, I have gained extensive experience in the analysis, design, architecture, standards, and development of products and services in the areas of multimedia and networked video delivery (including MPEG, IPTV and Video-on-Demand), computer networks (including TCP/IP and Ethernet), application development (including web-based technologies), and cloud-based services.

5. I am currently a Mentor, Venture Advisor and Consultant to multiple startup companies out of the i-GATE Innovation Hub in Livermore, California, which is supported by Lawrence Livermore National Labs (LLNL), Sandia National Labs, the Tri-Valley cities including Livermore, Pleasanton, Dublin, and Danville, and the County of Alameda.

6. Previously, I was Chief Technology Officer for Multimedia at Huawei Technologies USA. Huawei is the world's largest provider of Information and Communication Technology (ICT) solutions. From November 2010 to the present time, both at Huawei and i-GATE, I have focused on helping drive collaboration and innovation using lean-startup methods and modern networking, multimedia, cloud and maker technologies, while also educating others on its standards and best practices.

7. Prior to Huawei, I was a Sr. Director and Chief Video Architect at Cisco Systems Inc., a leader in network technologies. From September 2003 to October 2008, and later as a consultant to Cisco through November 2010, I was as a video technology expert across multiple business units ("BUs") helping design and architect products, including Cisco's EdgeQAMs for cable Video-on-Demand (VoD) and its Video Quality Enhancement (VQE) offerings. I organized cross-BU video architecture summits and presented at industry conferences including Cisco-Live Networkers, Society of Motion Picture and Television Engineers (SMPTE),

National Telecommunications Cooperative Association (NTCA), Society of Cable Telecommunications Engineers (SCTE), and other conferences.

8. While at Cisco, I also served as a video technology evaluator in three potential acquisitions (UTStarcom, Scientific Atlanta, and Arroyo Video Solutions Inc.). Following the Scientific Atlanta acquisition, I taught IPTV technology to Scientific Atlanta employees. I was also a member of Cisco's Video Cisco Patents Online (CPOL) committee through which I evaluated and advanced video-related patents. I was also a visiting engineer to Comcast during their RNG generation video Set Top Box design.

9. I was also co-chair of Cisco's video-related standards efforts in the ITU-T, ATIS-IIF, DVB, MSF and other SDOs and co-led Cisco's efforts in the International Telecommunications Union's (ITU-T) IPTV Focus Group developing International standards for the delivery of multimedia Television services over Internet Protocol (IPTV) from July 2006 through early 2008.

10. Prior to Cisco, I was Chief Technology Officer for Larry Ellison's nCUBE company, a super-computer company that pivoted into the development of service provider Video-on-Demand. From March 1993 to September 2003 at nCUBE, I led the development of its MediaCUBE video server products in conjunction with the OMS/OVS team at Oracle, applying super-computer and networking technologies in the world's first VoD Telco trials at British Telecom,

US West, and in Bell Atlantic's Stargazer trial in Reston VA. The nCUBE VoD servers delivered MPEG-2 TS video over ATM, channelized T3 and Ethernet. We later deployed what was at that time the world's largest VoD deployment in New York City for Time Warner Cable. During this period, I also worked extensively with leading broadcast Conditional Access System (CAS) companies in updating their CAS systems to support the random access "trick-mode" operations needed for VoD.

11. Between February 1983 and March 1993, I was a co-founder of Interlink Computer Sciences Inc. (INLK), where we developed DECnet and TCP/IP networking for IBM's MVS and VM systems. The company went public on NASDAQ in 1996. I led the design and implementation of the 3711 Network Controller, connecting IBM channels to an Ethernet network, and the VM/DECnet product in support of DuPont, its initial and lead customer.

12. From January 1978 to February 1983 I worked at Digital Equipment Corp (DEC), consulting to multiple customers including LLNL, NASA/Ames Research Center, and the US Navy regarding DEC products and network technologies. At LLNL, I helped design the control system for the ATA particle beam accelerator at Site 300. For NASA/Ames, I supported the development of their DECnet network of VAX/VMS and RSX-11 systems. For the US Navy in

Monterey CA, I debugged and corrected problems with their third-party developed 2780/3780-based communications subsystem.

13. I received a B.S. in Computer Science and Engineering in 1978 at the Massachusetts Institute of Technology (MIT) after winning a Hertz Foundation undergraduate scholarship. Later, in 2007 at Cisco, I also earned a Stanford Certificate in Advanced Project Management (SCPM) from Stanford University.

14. I am a long time member of the Institute of Electrical and Electronics Engineers (IEEE), the Society of Motion Picture and Television Engineers (SMPTE), and the Society of Cable Telecommunications Engineers (SCTE).

15. I have given the Introduction to IPTV Architectures, Technologies, and Standards tutorial at the 2007 SMPTE Fall Technical conference in Brooklyn NY. I was an invited guest editor of the IEEE Internet Computing journal's May/June 2009 special issue on IPTV and the July 2009 online issue of IEEE Computing Now.

16. I am also a current member of MIT's Education Council, interviewing high school applicants who apply to attend MIT.

17. A copy of my CV is attached to this declaration as Appendix A.

## II. UNDERSTANDING OF LEGAL STANDARDS

18. I am not a lawyer and I have no legal training. I have been informed by Petitioner's counsel about certain legal principles and standards, which I have

assumed and applied for purposes of this declaration. Some of these, which form the legal framework for the opinions I am providing, are summarized below.

A. **Validity**

19. I have been informed that a patent claim may be found invalid if it is anticipated or rendered obvious by prior art. I have considered references such as patents and publications to be prior art to the '964 patent if they were patented or published more than one year before the alleged priority date of the '964 patent, or if they were patented or filed as an application for a patent, which was subsequently published, with a date prior to the date the subject matter of the claims of the '964 patent was allegedly invented. For purposes of this declaration, I have assumed that the priority date of the claims of the '964 patent is March 14, 2000, the date on which the provisional application to which the '964 patent claims priority was filed.

20. I have been informed that a patent claim is anticipated under 35 U.S.C. § 102 if each and every limitation of the claim is disclosed in a single prior art reference as arranged in the claim. I understand that each element of a patent claim may be disclosed by a prior art reference either expressly or inherently. My understanding is that even an "express" disclosure does not necessarily need to use the same words as the claim. I also understand that an element of a patent claim is inherent in a prior art reference if the element must necessarily be present, and its

presence would be recognized by a person of ordinary skill in the art. However, I understand that inherency cannot be established by mere probabilities or possibilities.

21. I understand that not all innovations are patentable; even if a claimed product or method is not disclosed in its entirety in a single prior art reference, the claim is nonetheless invalid if the differences between the patented subject matter and the prior art are such that the subject matter as a whole would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. I am informed that this standard is set forth in 35 U.S.C. § 103(a).

22. I understand that when considering the issues of obviousness, I am to do the following: (i) determine the scope and content of the prior art; (ii) ascertain the differences between the prior art and the claims at issue; (iii) resolve the level of ordinary skill in the pertinent art; and (iv) consider objective evidence of non-obviousness (so-called "secondary considerations"). I appreciate that secondary considerations must be assessed as part of the overall obviousness analysis, and should not be considered merely to decide whether they alter any initial obviousness conclusions that could be drawn based on the prior art. I understand examples of evidence of secondary considerations of non-obviousness include evidence of commercial success, long-felt but unsolved needs, failure of others, and unexpected results. I am not aware of any secondary considerations that

would rebut my opinion that claims 1-4 of the ’964 patent would have been obvious (and I reserve the right to address any supposed secondary considerations to the extent the patent owner attempts to raise them in this proceeding).

23. To the contrary, the claimed invention of the ’964 patent did not solve a long-felt but unsolved need, fix the failure of others, or achieve unexpected results considering the prior art had already addressed and solved the same issues in the same way. I am not aware of any evidence showing a nexus between the commercial success of any product and the claimed invention of the ’964 patent.

24. In determining whether the subject matter as a whole would have been obvious at the time that the invention was made to a person having ordinary skill in the art, I have been informed of several principles regarding the combination of elements of the prior art.

25. First, a combination of familiar elements according to known methods is likely to be obvious when it yields predictable results. Second, simple substitution of one known element for another is likely to be obvious when it yields predictable results. Third, the use of known techniques to improve similar devices (methods, or products) in the same way is likely to be obvious when it yields predictable results. Fourth, applying a known technique to a known device ready for improvement is likely to be obvious when it yields predictable results. Fifth, merely choosing from a finite number of identified, predictable solutions, is

likely to be obvious when there is a reasonable expectation of success. Sixth, known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces and such variations are likely to be obvious if the variations are predictable to one of ordinary skill in the art.

26. I understand that the "teaching, suggestion, or motivation" test is a useful guide in establishing a rationale for combining elements of the prior art. This test poses the question as to whether there is an explicit teaching, suggestion, or motivation in the prior art to combine prior art elements in a way that realizes the claimed invention. Though useful to the obviousness inquiry, I understand that this test should not be treated as a rigid rule. It is not necessary to seek out precise teachings; it is permissible to consider the inferences and creative steps that a person of ordinary skill in the art would employ.

B. **The Level of Ordinary Skill in the Art**

27. I understand that "a person of ordinary skill in the relevant field" is presumed to be a person with standard skill, creativity, and knowledge in a particular field or industry. This person thinks along the line of conventional wisdom in the art but is neither an automaton nor one who undertakes to innovate, whether it is by patient, expensive, and systematic research or by extraordinary insight.

28. In assessing the level of ordinary skill, I further understand one may consider several factors, including: (1) the educational level of the inventor; (2) the educational level of active workers in the field; (3) type of problems encountered in the art; (4) prior art solutions to those problems; (5) the rate of innovation in the field; and (6) the sophistication of the technology.

29. Based on my experience, I have an understanding of the capabilities of a person of ordinary skill in the relevant fields. I have supervised, directed, and worked with many such persons over the course of my career. Further, I had at least those capabilities myself on the priority date of the '964 patent.

30. I have been informed that the level of skill in the art is evidenced by prior art references. The prior art discussed herein demonstrates that a person of ordinary skill in the field, on the assumed priority date of the '964 patent, was aware of networked camera systems, commonplace networking techniques, and the applicability of those networking techniques to the networked camera systems.

31. I have been asked to offer an opinion on the characteristics of a person having ordinary skill in the art as of the priority date of the '964 patent. In view of the specification of the '964 patent and the prior art references of record, it is my opinion that a person of ordinary skill at that time in the relevant field 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.

32. Regarding the above factors for determining the level of ordinary skill in the art, I considered the following in developing my opinion: the educational level of active workers in the field, in my experience, is typically a bachelor's degree in computer science or electrical engineering; the problems encountered in the art generally relate to connecting applications to networked devices so they are interoperable; the prior art solutions include networked video camera systems and networking techniques collectively using the same concepts, techniques, and technologies as claimed in the '964 patent; the rapidity with which innovations were made in this field was high because the technologies described and claimed in the '964 patent were largely based on software that could be developed quickly and expanded to include then-known features in expected ways to achieve increasingly useful results; and the sophistication of the technology was moderate because in order to make it accessible to users and professional system builders, there was reduced technical complexity.

## III. MATERIALS REVIEWED AND CONSIDERED

33. In connection with my work on this matter, I have reviewed the following documents:

| Exhibit | Description |
|---|---|
| 1001 | USPN 8,185,964 (patent under *Inter Partes* Review) |

| | |
|---|---|
| 1002 | The file history for the ’964 patent |
| 1004 | USPN 6,166,729 to Acosta et al. (“Acosta”) |
| 1005 | USPN 5,905,859 to Holloway et al. (“Holloway”) |
| 1006 | USPN 6,292,838 to Nelson (“Nelson”) |
| 1007 | AXIS 200 User’s Manual (“Axis 200”) |
| 1008 | AXIS 2100 Network Camera User’s Guide (“Axis 2100”) |
| 1009 | AXIS 2400 and AXIS 2401 Video Servers Administration Manual (“Axis 2400”) |
| 1010 | Declaration of James Marcella |
| 1011 | USPN 6,438,530 to Heiden et al. (“Heiden”) |
| 1012 | USPN 6,477,648 to Schell et al. (“Schell”) |
| 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”) |

## IV. THE STATE OF THE ART BEFORE THE ’964 PATENT’S EARLIEST PRIORITY DATE

### A. Systems of Networked Cameras Were Known

34. 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.

('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).).

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

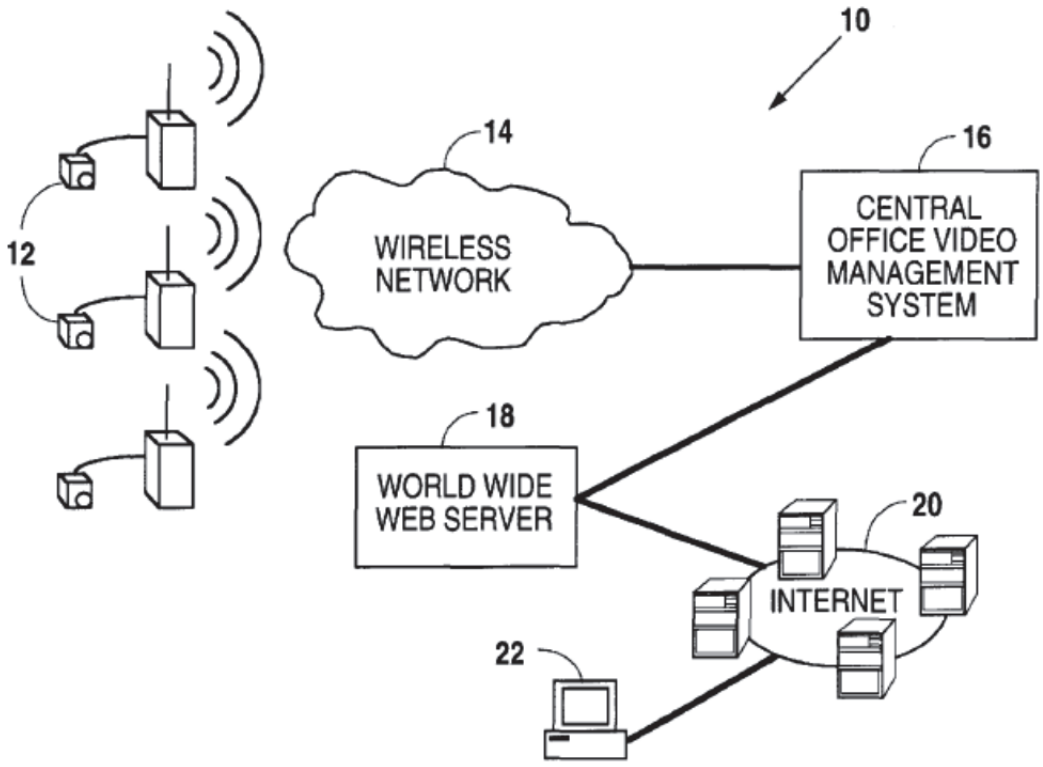



Fig. 1

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).)

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

36. 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. 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).)

37. 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. 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).)

38. Using a MAC address to determine whether communications between systems on a network are authorized was also a known technique. 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. 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).) 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).)

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

39. The claims of the '964 patent merely recite applying commonplace networking techniques in the context of networked camera systems then known in the art.

40. 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 camera as they are to connecting other networked devices. 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. 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. 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 addressed.

41. 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. 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.

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

### A. Claims 1 and 3 are Anticipated by Acosta

42. In my opinion, Acosta anticipates claims 1 and 3.

#### 1. Claim 1

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

43. Acosta discloses "a method of controlling access by a computer to a video server." 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).)

44. 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).)

45. 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.

46. 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).)

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

47. 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).)

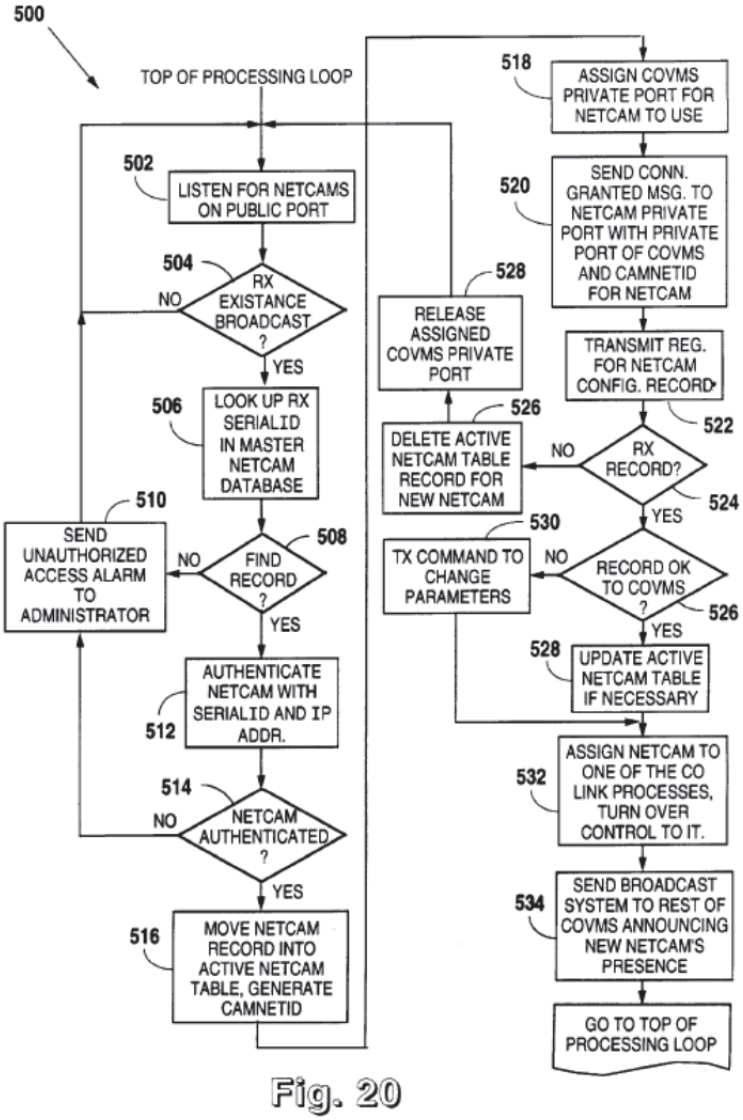



Fig. 20

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**

48. 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.

49. 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:

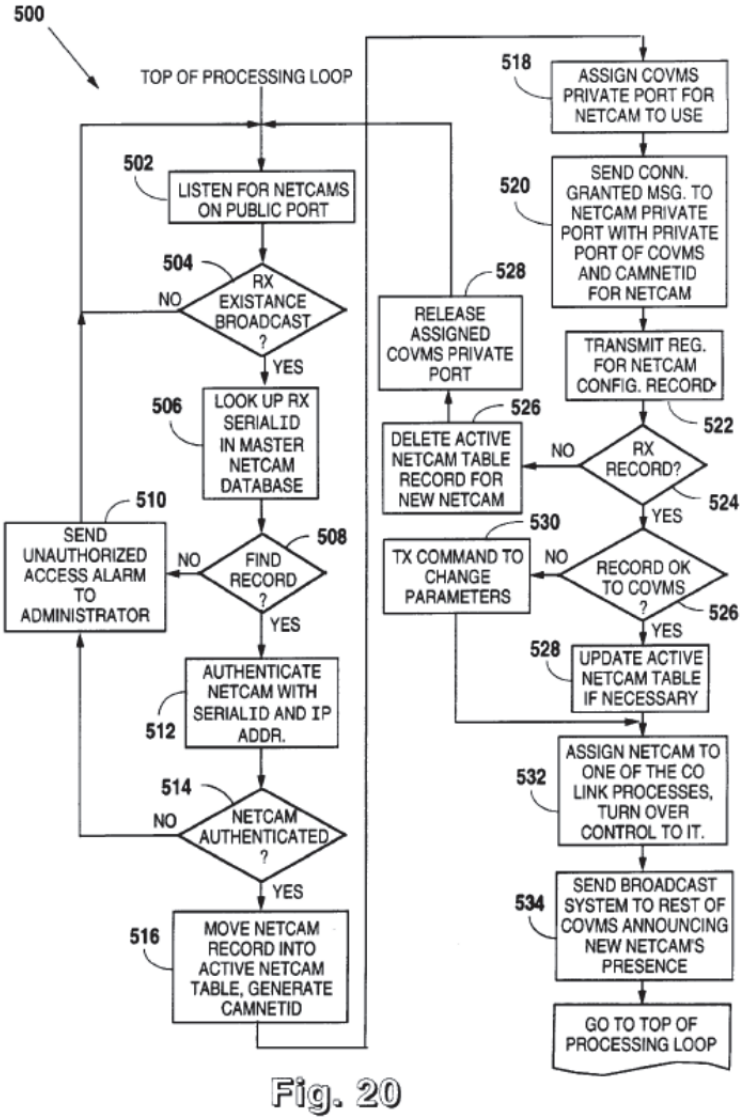



Fig. 20

Accordingly, Acosta discloses the COVMS 16 receiving the serial ID from camera element 12.

50. 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).)

51. 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.

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**

52. 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.

53. 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).)

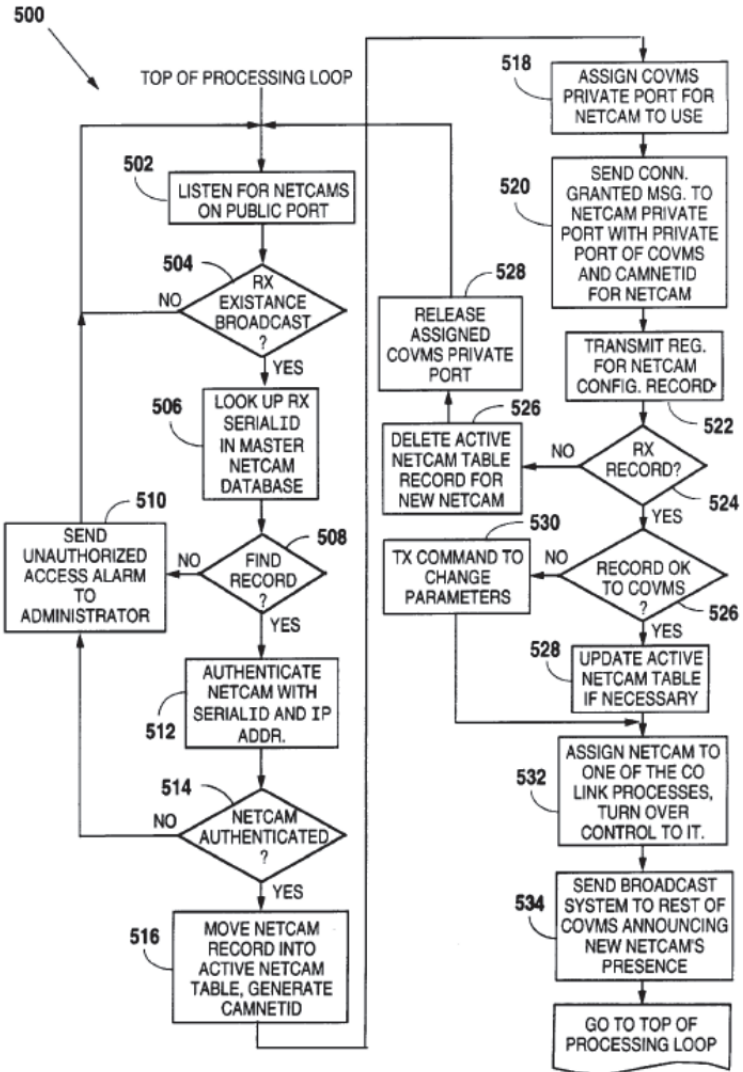


Fig. 20

54. 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).

55. 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.

56. 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).)

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

57. 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.

58. 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).)

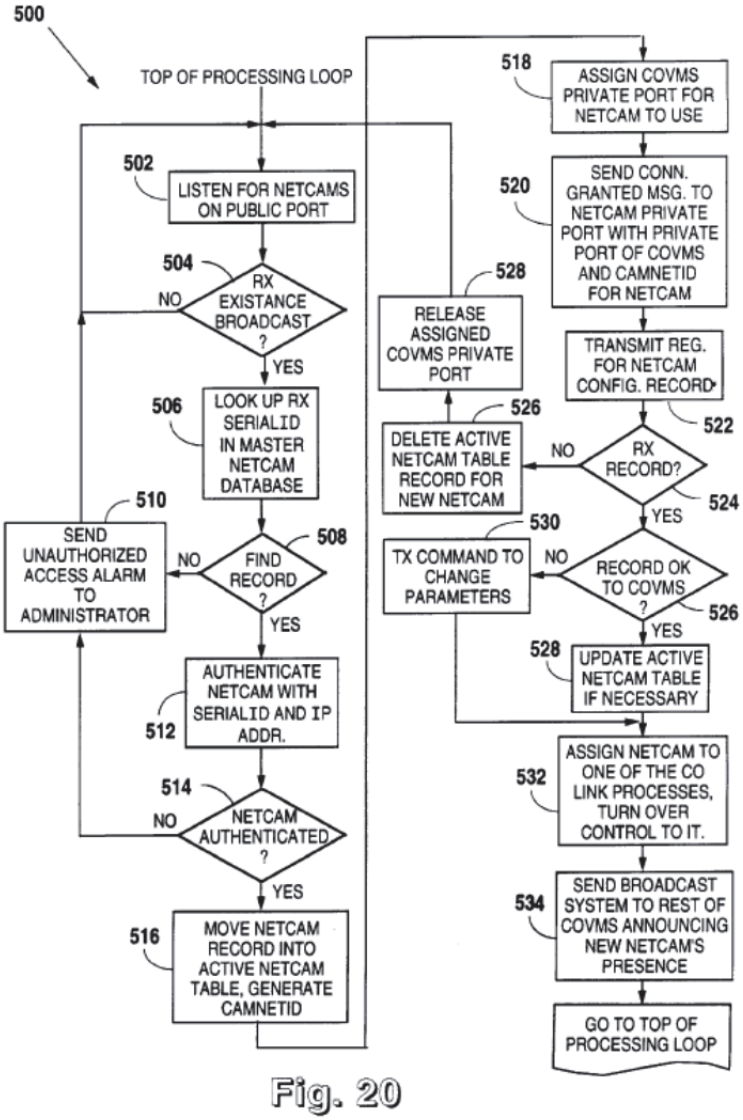



Fig. 20

59. Accordingly, based on my analysis and applying the legal principles discussed above, claim 1 is anticipated by Acosta.

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.**

60. 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.

61. 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.

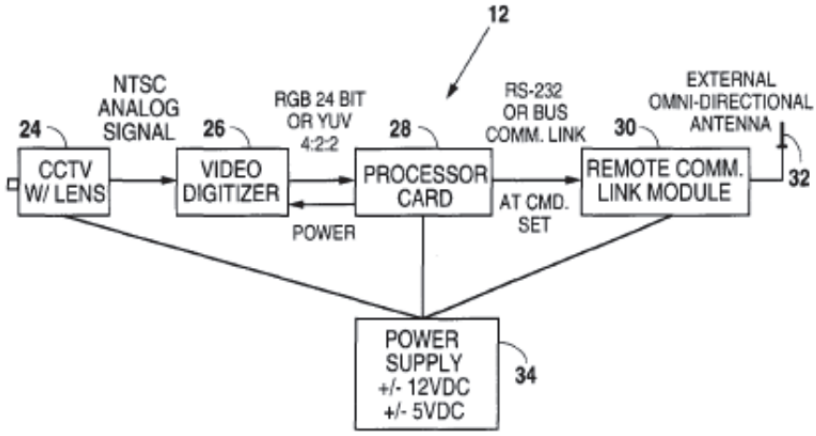



Fig. 2

62. Accordingly, based on my analysis and applying the legal principles discussed above, claim 3 is anticipated by Acosta.

## B. Claims 2 and 3 are Rendered Obvious by Acosta in view of Axis 200

63. In my opinion, Acosta and Axis 200 render claims 2 and 3 obvious.

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

64. 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.

65. To the extent that Acosta does not disclose that the serial ID can be a MAC address, Axis 200 discloses this element. 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).) One of skill in the art would understand that the Ethernet address referenced in Axis 200 is the network camera's MAC address.

66. 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. Acosta and Axis are within the same field of endeavor--networked camera systems. 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.

67. Acosta's COVMS 16 is also readily combinable with the Axis 200 camera. 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).) 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. One of skill in the art would be motivated to do so to increase the network camera devices supported by COVMS 16. 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.

68. 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. As discussed above in Section III, 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.

69. Thus, the combination of Acosta and Axis 200 discloses the unique identifier is a MAC address. Accordingly, based on my analysis and applying the legal principles discussed above, claim 2 would have been in obvious to one of ordinary skill in the art in light of Acosta and Axis 200.

### 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.**

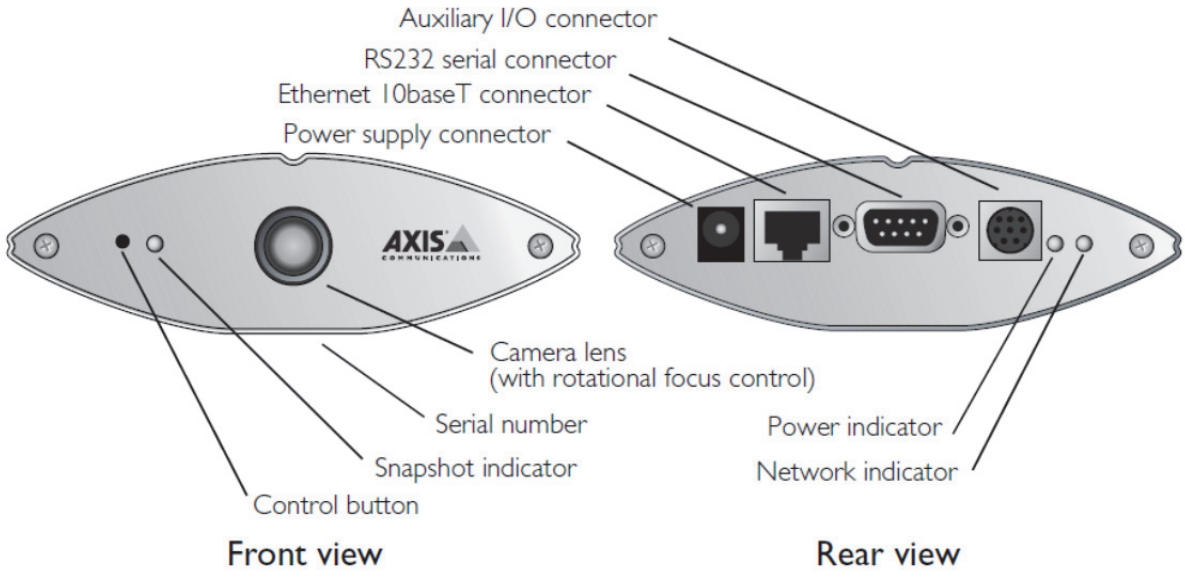
70. Acosta in combination with Axis 200 disclose "the video server is a camera server that includes a camera and a web server with an Ethernet port or a component based video server including inputs for one or more analog video feeds." As discussed above, Acosta discloses camera element 12 is a component based video server including inputs for one or more analog feeds.

71. 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).) 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 11 (illustrating camera and Ethernet port) (Ex. 1007).)




72. 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.

73. Accordingly, based on my analysis and applying the legal principles discussed above, claim 3 would have been in obvious to one of ordinary skill in the art in light of Acosta and Axis 200.

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

74. In my opinion, Acosta, Axis 200, and Nelson render claim 4 obvious.

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:**

75. Acosta discloses "[a] method of controlling access by a computer to a hardware device . . . performed at the computer." 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).) As discussed above with respect to claim element [1p.], Acosta discloses this claim element.

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;**

76. 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." 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.

77. 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).) 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. Finally, Acosta discloses "[t]he cameras 12 communicate with the COVMS 16 over the wireless network 14." Acosta 7:43-44.

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

78. 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.

79. 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).) 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.

80. 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).) 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 CO VMS 16 in a step 526 assesses whether the record is suitable.") (Ex. 1004).)

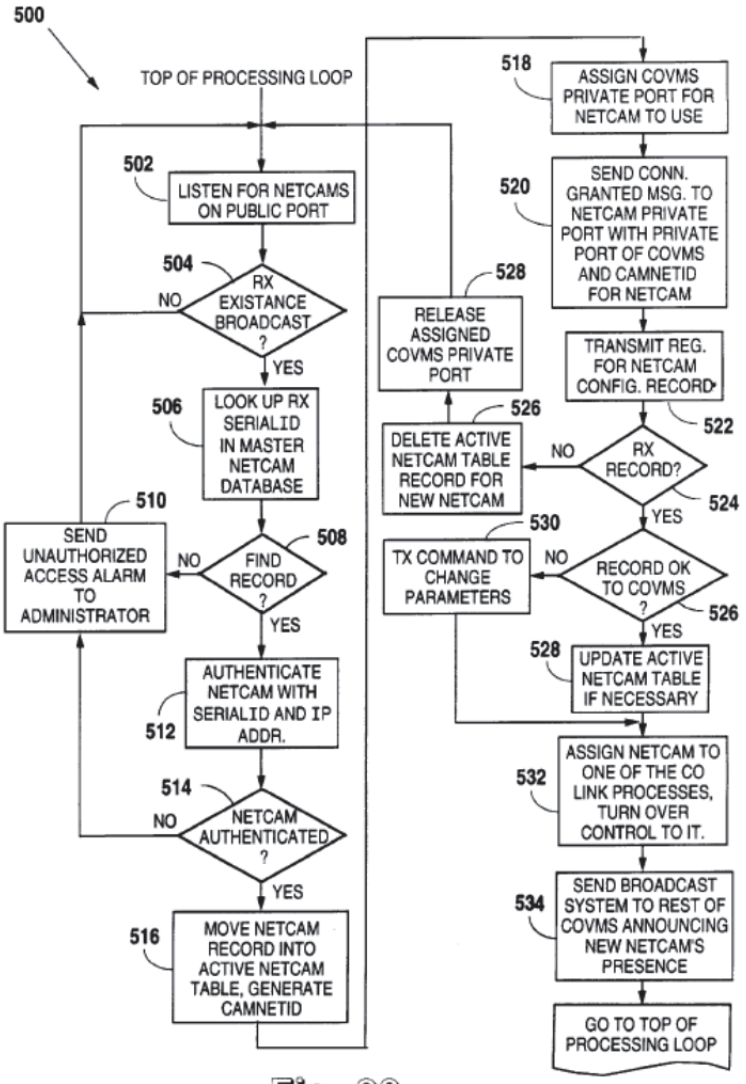


Fig. 20

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

81. 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.

82. 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).). 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).) 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).)

83. It would have been obvious to modify Acosta's COVMS 16 to send a request for the MAC address of the Axis 200 camera. 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. 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.

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

84. 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. 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.

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.**

85. 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. 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.

86. Accordingly, based on my analysis and applying the legal principles discussed above, claim 4 would have been in obvious to one of ordinary skill in the art in light of Acosta, Axis 200, and Nelson.

## VI. CONCLUSION

87. I understand and have been warned that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. § 1001). I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under § 1001 of title 18 of the United States Code.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on February 4, 2016 in Livermore, CA.

Greg Thompson