IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

REEF MOUNTAIN LLC,	§	
	§	
Plaintiff,	§	Case No:
	§	
vs.	§	PATENT CASE
	§	
NAPCO SECURITY TECHNOLOGIES, INC.,	§	
	§	
	§	
Defendant.	§	
	§	

COMPLAINT

Plaintiff Reef Mountain LLC ("Plaintiff" or "Reef Mountain") files this Complaint against Napco Security Technologies, Inc. ("Defendant" or "Napco") for infringement of United States Patent No. 8,239,481 (hereinafter "the '481 Patent").

PARTIES AND JURISDICTION

1. This is an action for patent infringement under Title 35 of the United States Code. Plaintiff is seeking injunctive relief as well as damages.

2. Jurisdiction is proper in this Court pursuant to 28 U.S.C. §§ 1331 (Federal Question) and 1338(a) (Patents) because this is a civil action for patent infringement arising under the United States patent statutes.

3. Plaintiff is a Texas limited liability company with its office address at 5570 FM 423, Suite 250-125, Frisco, TX 75034.

4. On information and belief, Defendant is a Delaware corporation with a principal address of 333 Bayview Avenue, Amityville, NY 11701.

5. On information and belief, this Court has personal jurisdiction over Defendant

because Defendant has committed, and continues to commit, acts of infringement in this District, has conducted business in this District, and/or has engaged in continuous and systematic activities in this District.

6. On information and belief, Defendant's instrumentalities that are alleged herein to infringe were and continue to be used, imported, offered for sale, and/or sold in this District.

VENUE

7. Venue is proper in this District pursuant to 28 U.S.C. § 1400(b) because Defendant is deemed to be a resident of this District.

COUNT I
(INFRINGEMENT OF UNITED STATES PATENT NO. 8,239,481)

8. Plaintiff incorporates paragraphs 1 through 7 herein by reference.

9. This cause of action arises under the patent laws of the United States and, in particular, under 35 U.S.C. §§ 271, *et seq*.

10. Plaintiff is the owner by assignment of the '481 Patent with sole rights to enforce the '011 Patent and sue infringers.

11. A copy of the '481 Patent, titled "System and method for implementing open-control remote device control," is attached hereto as Exhibit A.

12. The '481 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code.

13. On information and belief, Defendant has infringed and continues to infringe one or more claims, including at least Claims 1, 3, 9, 12, 13, 15, 17, 26, 30, 31, 32, 35, 37, 40, 44, 45, and 46 of the '481 Patent by making, using, importing, selling, and/or offering devices and methods for controlling devices in a computer system, which are covered by at least Claims 1, 3, 9, 12, 13, 15, 17, 26, 30, 31, 32, 35, 37, 40, 44, 45, and 46 of the '481 Patent. Defendant has

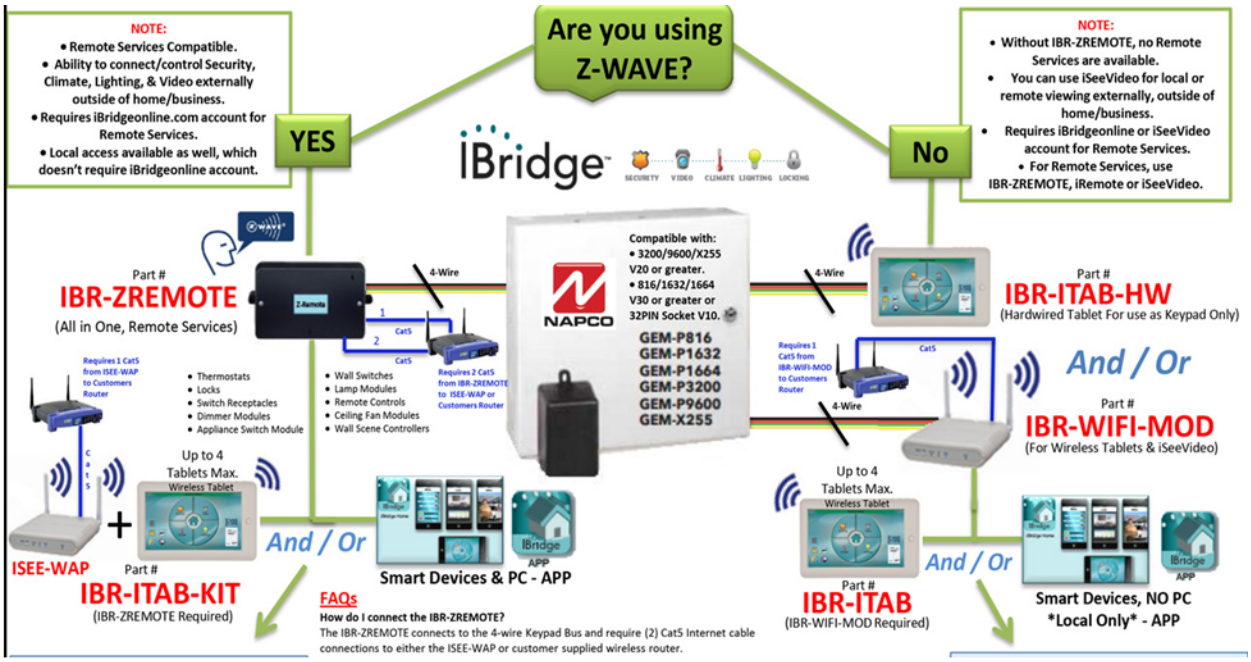
infringed and continues to infringe the '481 Patent directly in violation of 35 U.S.C. § 271.

14. Defendant sells, offers to sell, and/or uses (including by at least testing) appliance and system control devices and/or systems including, without limitation, the iBridge Connected Home system, iBridge App, and any similar products ("Product"), which infringe at least Claims 1, 3, 9, 12, 13, 15, 17, 26, 30, 31, 32, 35, 37, 40, 44, 45, and 46 of the '481 Patent. The Product enables a user to control various appliances and systems that utilize different device-specific protocol instruction through an interface by encoding selected appliance operations according to a standard communication protocol instruction.

15. In at least testing and usage, the Product implements a communication method for controlling devices in a computer system. The Product obtains a user selection (e.g., selection of smart appliances which a user wants to control. For example, the user can select a smart appliance, device or system, such as lights, door locks, thermostats, etc.) of one or more of a plurality of networked devices to be manipulated from a user interface (e.g., the iBridge App interface), wherein at least one of the plurality of networked devices requires device-specific protocol instructions (e.g., instructions pertaining to a particular device's or system's functionality; for example, a thermostat adjustment, a light being turned on or off, or a door lock being unlocked or locked) that are different from protocol instructions required by at least one of the other plurality of networked devices (e.g., different devices and systems have different instruction sets that correspond to their different functionality). The iBridge App can control, by means of a smartphone, multiple types of devices which have different functionalities, and therefore, on information and belief, must have different software operating instructions that correspond to their different (e.g., different device-specific protocol instructions). Certain aspects of these elements and limitations are illustrated in the screen shots below and/or in screen

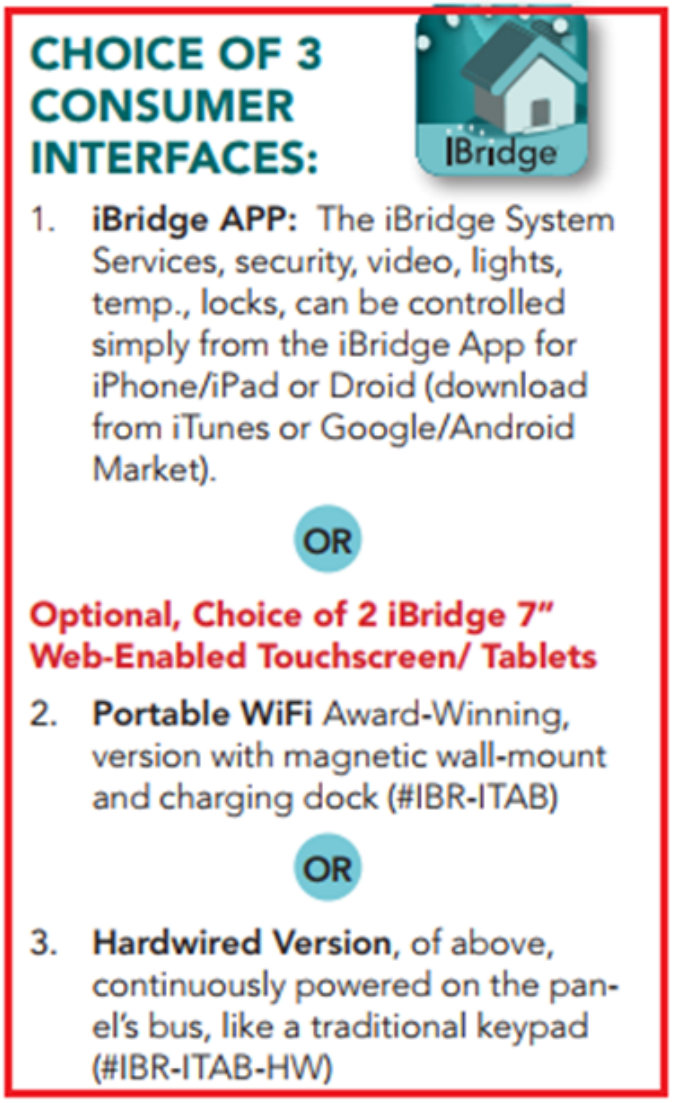
shots provided in connection with other allegations herein.

http://www.napcosecurity.com/images/web pdf/A613_iBridge_hipster_trifold_lowres.pdf

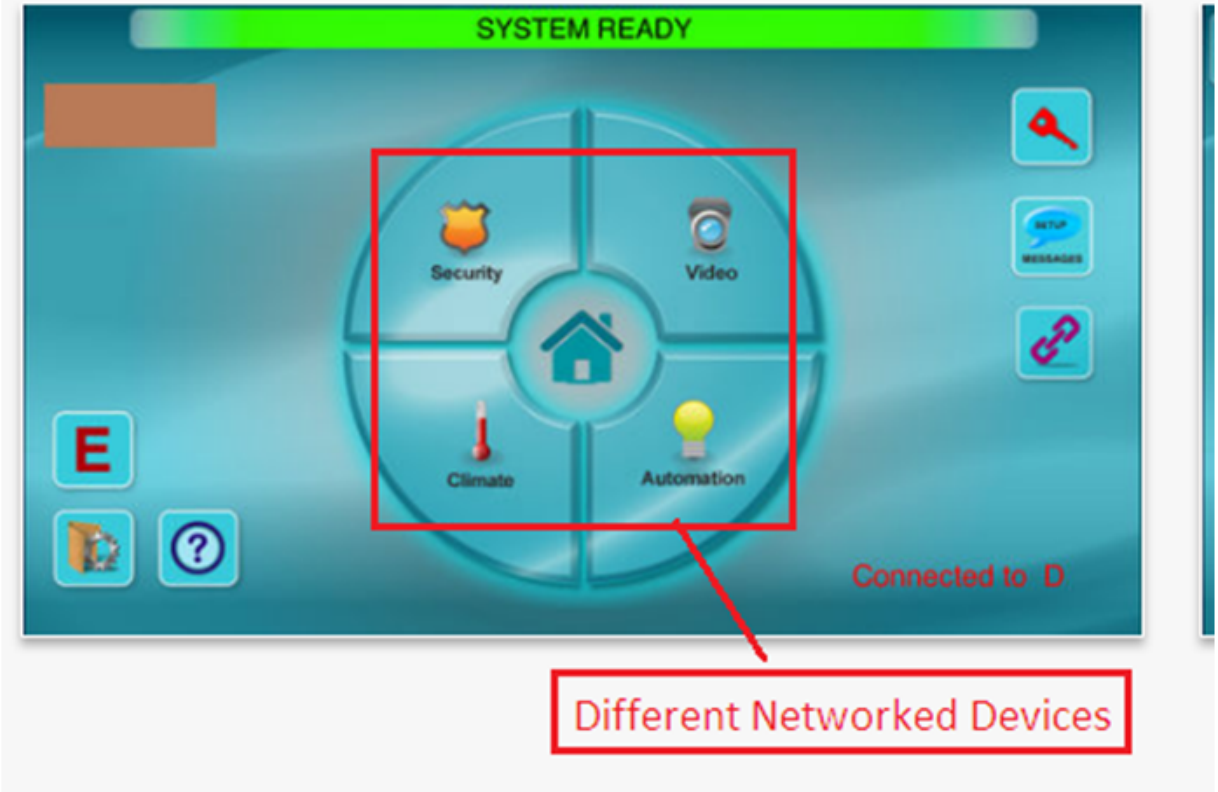


http://www.napcosecurity.com/assets/images/iBridge-Quick-Flow_large.jpg

http://www.napcosecurity.com/images/web pdf/A613_iBridge_hipster_trifold_lowres.pdf

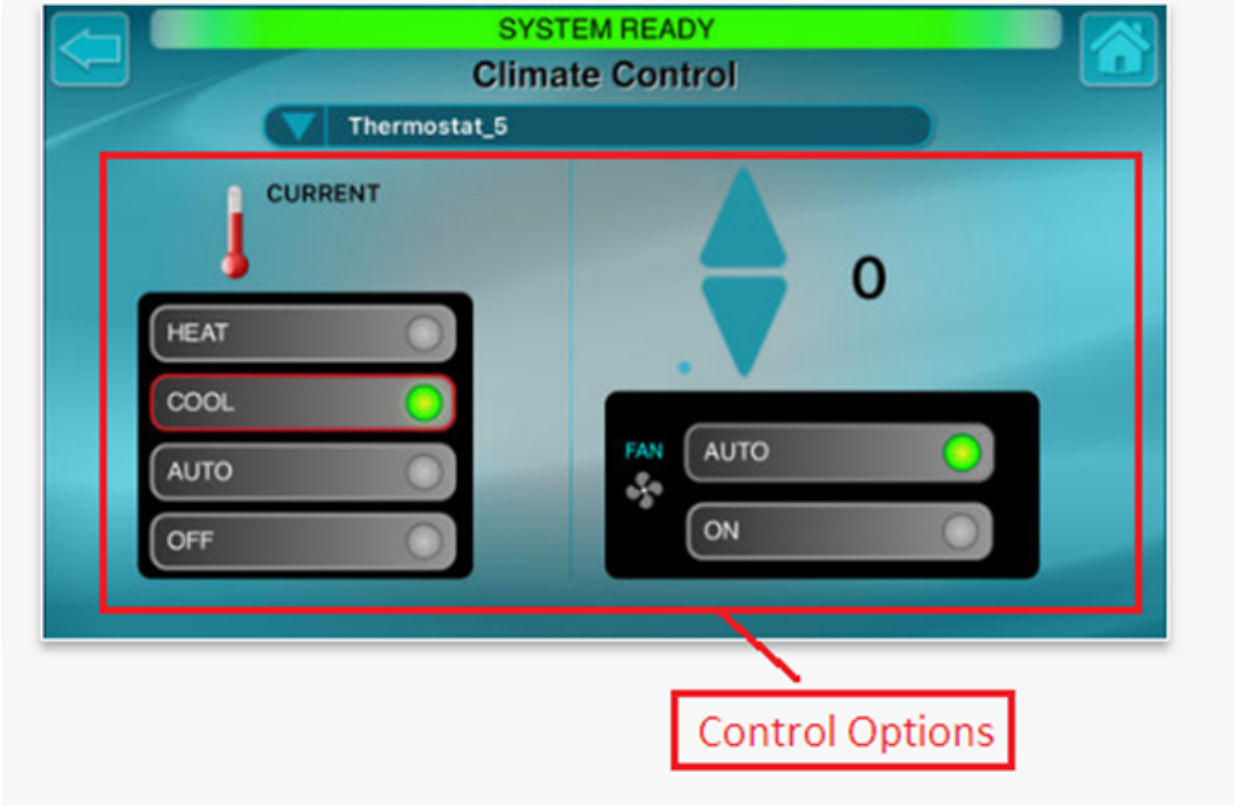


http://www.napcosecurity.com/media/pdfs/Napco_iBridge_InfoSheet.pdf

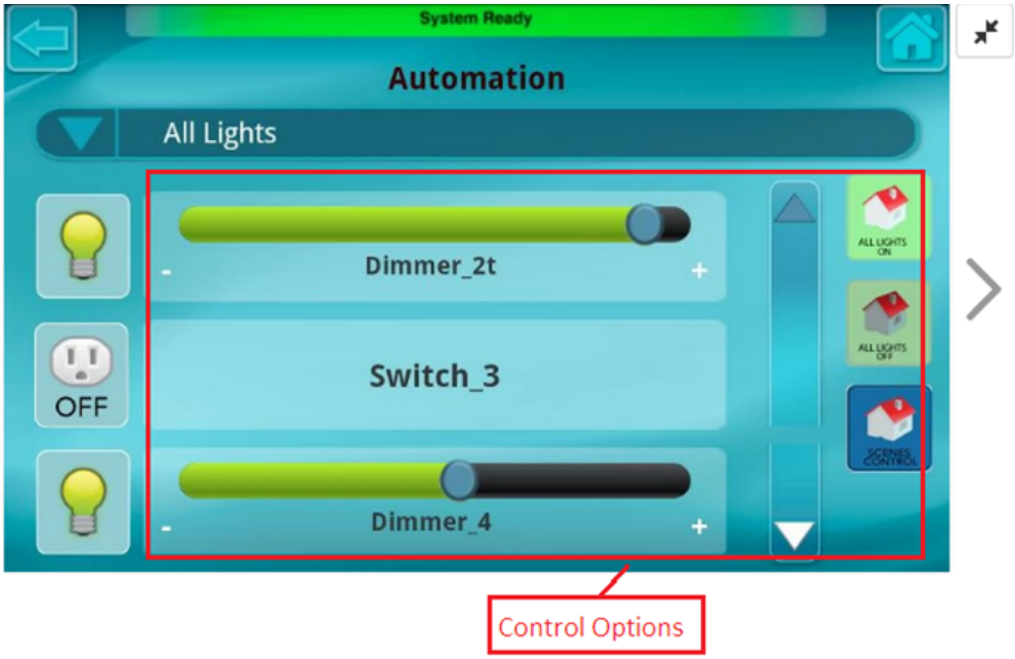


https://itunes.apple.com/us/app/ibridge/id594495700?mt=8

https://itunes.apple.com/us/app/ibridge/id594495700?mt=8



https://itunes.apple.com/us/app/ibridge/id594495700?mt=8



https://play.google.com/store/apps/details?id=com.napcosecurity.android.rcm.ui&hl=en

http://www.napcosecurity.com/images/web pdf/A613_iBridge_hipster_trifold_lowres.pdf

16. In at least testing and usage, the Product obtains a user interface application (e.g., the iBridge smartphone app) corresponding to the selected one or more networked devices (e.g., smart appliances such as lights, door locks, etc.). Certain aspects of these elements are illustrated in the screen shots provided in connection with other allegations herein.

17. In at least testing and usage, the Product transmits, to at least one user interface selection device, the user interface application (e.g., a smartphone with the iBridge application installed), the user interface application (e.g., the iBridge smartphone app) corresponding to the selected one or more networked devices (e.g., the iBridge application will display a user interface that can be used to control corresponding smart appliances) so that the user interface (e.g., the iBridge smartphone app) can be displayed on the at least one user interface selection device (e.g., a smartphone with the iBridge application installed). Certain aspects of these elements are illustrated in the screen shots provided in connection with other allegations herein.

18. In at least testing and usage, the Product obtains a user selection of an operation

(e.g., a user can control and/or set a particular device using the iBridge App) corresponding to at least one selected networked device (e.g., smart appliances). Certain aspects of these elements are illustrated in the screen shots provided in connection with other allegations herein.

19. On information and belief, in at least testing and usage, the Product encodes the selected operation (e.g., a user's selection of a particular setting or control pertaining to a particular device) according to a standard communication protocol instruction (e.g., a standard protocol utilized by the iBridge system to encode all user instructions to a format appropriate for transmittal to the Napco server and/or Bridge over the Internet). Because the iBridge system utilizes a single application interface to control a multitude of devices, it follows that the application utilizes a common communication protocol to encode all user instructions originating from the iBridge App for the sake of efficiency. Because a Napco server and/or bridge device parses all of the said instructions or settings, it follows that a single communication protocol is utilized by the iBridge App to transmit settings and/or settings. The standard communication protocol could be any Internet protocol appropriate for the transmittal of controls/settings from the mobile application to the Napco server/bridge via the Internet. Certain aspects of these elements are illustrated in the screen shots below and/or in screen shots provided in connection with other allegations herein.

iBridge® Connected Home/Businesses Services App, Connect Hub, Touchscreen & Cameras

Control Security, Video & Smart Automation from any smart device or new iBridge Touchscreen, including SMS/MMS Notifications. For smart home or business, interface video cameras and your choice of Z-Wave IoT devices with StarLink Connect Communicator's built in hub with multi-brand panel support or use iBridge Modules for Gemini panels. Three all-new iBridge Cameras™ offer hi-res, onboard storage, super easy enrollment, WAP-free convenience and two-way voice or the exterior dome cam also has POE option. Also ask about new iBridge Video Door Bell.

Z-Wave Device Control is universally provided by StarLink Connect® Cell/IP Communicator/Hub, or for Gemini Systems with iBridge Z-Remote (hardwire or wireless)

http://www.napcosecurity.com/products/ibridge/

The Protocol

IP is a protocol. Simply said, a protocol is a set of rules governing how things work in a certain technology so that there is some kind of standardization. When put into a network communication context, an internet protocol describes how data packets move through a network.

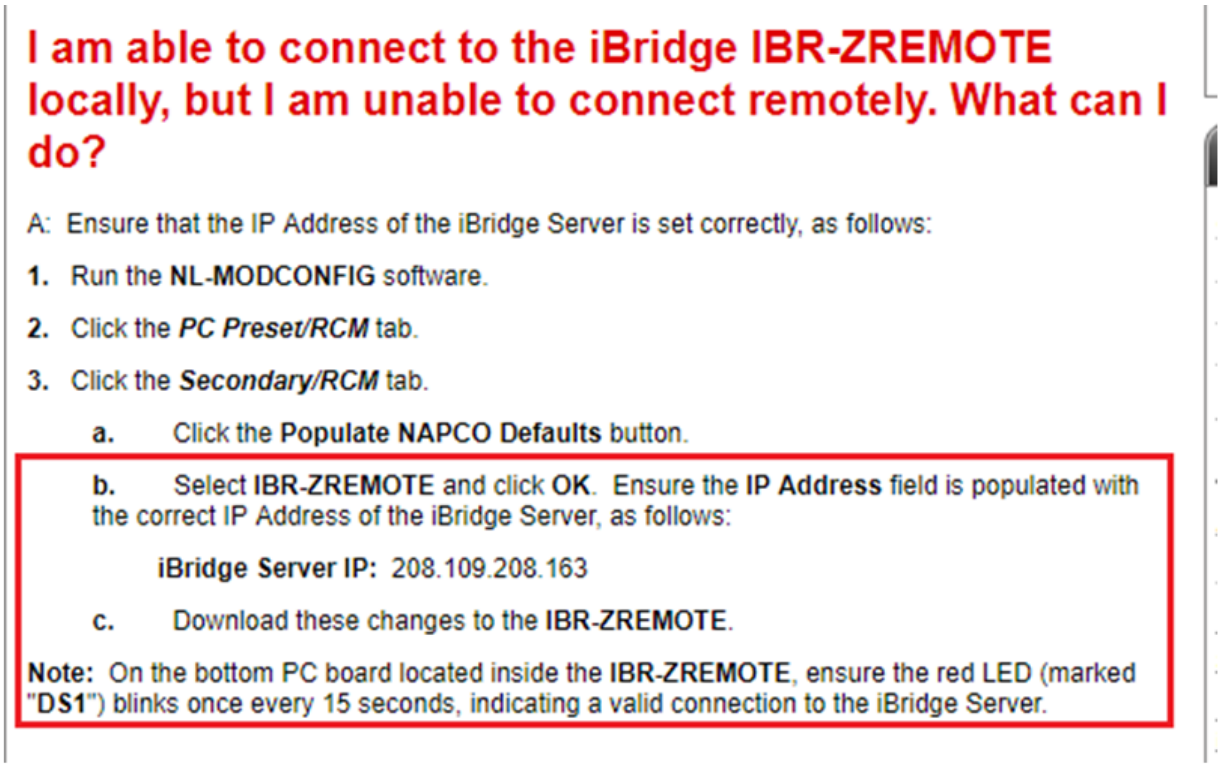
When you have a protocol, you are sure that all machines on a network (or in the world, when it comes to the internet), however different they might be, speak the same "language" and can integrate into the whole framework.

The IP protocol standardizes the way machines over the Internet or any IP network forward or route their packets based on their IP addresses.

https://www.lifewire.com/internet-protocol-explained-3426713

20. The Product transmits the selected standard protocol instruction (e.g., user input settings or controls that have been encoded utilizing a standard Internet protocol) to a server

(e.g., Napco's server and/or bridge device) corresponding to the selected networked device (e.g., smart appliances connected to a Napco server and/or bridge.). Certain aspects of these elements are illustrated in the screen shot below and/or in screen shots provided in connection with other allegations herein.



I am able to connect to the iBridge IBR-ZREMOTE locally, but I am unable to connect remotely. What can I do?

A: Ensure that the IP Address of the iBridge Server is set correctly, as follows:

1. Run the **NL-MODCONFIG** software.
2. Click the ***PC Preset/RCM*** tab.
3. Click the ***Secondary/RCM*** tab.
   - **a.** Click the **Populate NAPCO Defaults** button.
   - **b.** Select **IBR-ZREMOTE** and click **OK**. Ensure the **IP Address** field is populated with the correct IP Address of the iBridge Server, as follows:

     iBridge Server IP: 208.109.208.163
   - **c.** Download these changes to the **IBR-ZREMOTE**.

Note: On the bottom PC board located inside the **IBR-ZREMOTE**, ensure the red LED (marked "**DS1**") blinks once every 15 seconds, indicating a valid connection to the iBridge Server.

http://tech.napcosecurity.com/index.php/faq/details/id/250/

21. On information and belief, the Product obtains an output (e.g., the actual carrying out of controls or settings by a particular device; for example, the retrieval of status data from a device such as the current temperature settings of a thermostat, the operation of a device such as turning on/off a light, or the locking/unlocking of a lock) corresponding to the selected operation (e.g., the user input control and/or setting) of the selected networked device (e.g., smart appliances or other connected devices or systems). On information and belief, the Napco server and/or bridge will receive commands and or settings originating from a mobile device that have been encoded utilizing a standard internet protocol that is appropriate for data transmission over

the Internet. The Napco server and/or bridge will than parse said data to determine the appropriate commands/instructions to send to a particular device so that the desired setting/control can be carried out (e.g. the appropriate Zwave protocol command). Certain aspects of these elements are illustrated in the screen shots provided in connection with other allegations herein.

22. Regarding Claim 3, the Product contains a selection option wherein the selected networked device is a monitoring device (e.g., a smart appliance such as a thermostat that monitors temperature). Certain aspects of these elements are illustrated in the screen shots provided in connection with other allegations herein.

23. Regarding Claim 9, the output includes data indicative of the network device status (e.g., device settings or status such as the current temperature settings of a thermostat).

24. Regarding Claim 12, the standard communication protocol is device independent (e.g., the Internet protocol utilized for data transmission to the Napco server and/or bridge is independent of any protocols used for direct communication with actual devices and is universally used to transmit controls and settings across all of the different devices).

25. Regarding Claim 13, the user interface is a web-based graphical user interface (e.g., a smartphone app interface which controls through a network such as the Internet).

26. Regarding Claim 15, obtaining a user selection of an operation (e.g., settings of the device being controlled) corresponding to at least one selected networked device (e.g., smart appliances, lights, thermostat, etc.) includes obtaining a user manipulation of a graphical icon.

27. Regarding Claim 17, the Product includes a computer-readable medium having a computer executable program therein for performing the method of controlling devices in a computer system. The method steps are as described in connection with Claim 1 and as

illustrated in the screen shots provided in connection with other allegations herein.

28. Regarding Claim 26, the output includes data indicative of a networked device status. This is described in connection with Claim 9 and as illustrated in the screen shots provided in connection with other allegations herein.

29. Regarding Claim 30, the standard communication protocol is device independent. This is described in connection with Claim 12 and as illustrated in the screen shots provided in connection with other allegations herein.

30. Regarding Claim 31, the user interface is a Web-based graphical user interface. This is described in connection with Claim 13 and as illustrated in the screen shots provided in connection with other allegations herein.

31. Regarding Claim 32, obtaining a user selection of an operation corresponding to at least one selected networked device includes obtaining a user manipulation of a graphical icon. This is described in connection with Claim 15 and as illustrated in the screen shots provided in connection with other allegations herein.

32. Regarding Claim 35, the Product provides a method of controlling devices in a computer system. The method steps are as described in connection with Claim 1 and as illustrated in the screen shots provided in connection with other allegations herein.

33. Regarding Claim 37, the selected networked device is a monitoring device. This is described in connection with Claim 3 and as illustrated in the screen shots provided in connection with other allegations herein.

34. Regarding Claim 40, the output includes data indicative of a networked device status. This is described in connection with Claim 9 and as illustrated in the screen shots provided in connection with other allegations herein.

35. Regarding Claim 44, the standard communication protocol is device independent. This is described in connection with Claim 12 and as illustrated in the screen shots provided in connection with other allegations herein.

36. Regarding Claim 45, the user interface is a Web-based graphical user interface. This is described in connection with Claim 13 and as illustrated in the screen shots provided in connection with other allegations herein.

37. Regarding Claim 46, obtaining a user selection of an operation corresponding to at least one selected networked device includes obtaining a user manipulation of a graphical icon. This is described in connection with Claim 15 and as illustrated in the screen shots provided in connection with other allegations herein.

38. Defendant's actions complained of herein will continue unless Defendant is enjoined by this court.

39. Defendant's actions complained of herein are causing irreparable harm and monetary damage to Plaintiff and will continue to do so unless and until Defendant is enjoined and restrained by this Court.

40. Plaintiff is in compliance with 35 U.S.C. § 287.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff asks the Court to:

(a) Enter judgment for Plaintiff on this Complaint on all causes of action asserted herein;

(b) Enter an Order enjoining Defendant, its agents, officers, servants, employees, attorneys, and all persons in active concert or participation with Defendant who receive notice of the order from further infringement of United States Patent No. 7,797,011 (or, in the alternative,

awarding Plaintiff a running royalty from the time of judgment going forward);

(c) Award Plaintiff damages resulting from Defendant's infringement in accordance with 35 U.S.C. § 284;

(d) Award Plaintiff pre-judgment and post-judgment interest and costs; and

(e) Award Plaintiff such further relief to which the Court finds Plaintiff entitled under law or equity.

Dated: August 16, 2018

Respectfully submitted,

/s/ Stamatios Stamoulis

STAMATIOS STAMOULIS (#4606)
STAMOULIS & WEINBLATT LLC
Two Fox Point Centre
6 Denny Rd.
Suite 307
Wilmington, DE 19809
(302) 999-1540
stamoulis@swdelaw.com

ATTORNEYS FOR PLAINTIFF