IMAX CAM PRO

NETWORKING TUTORIALS

WORLD EYECAM

Networking

Remotely accessing video recorders and cameras on the internet (WAN) is an important feature to most clients and it should be considered when installing and implementing a video surveillance system. Discussed on this page are three critical aspects of networking a video recorder or camera system:

- Port forwarding video recorder(s) and camera(s)
- Managing an network IP camera system
- Bandwidth and throughput limitations

Port Forwarding

Port forwarding is required to view a device across the internet (WAN) remotely. The most basic of implementations requires knowledge of the network layout and the log in information of all applicable routing devices. Here is a step by step process on how to network a video recorder:

1. Get a basic understanding of how the network is laid out. If the video recorder is behind multiple routers, ports must forwarded through all routers.

2. Find the gateway IP address of the routing device that the video recorder is attached to. If there is a Windows PC connected to the same network tier (router) as the video recorder, running a CMD from the start menu and typing the command **ipconfig** at the prompt will display the gateway information. On a Apple Mac computer, pull down the apple menu in the top left corner and click on System Preferences. Next click on Network under Internet and Network. The address will appear next to the Router heading. Also note the subnet mask.

3. Take note of the video recorder's IP address found in Main Menu > Setting > Network or by using the ConfigTool (Windows only). If the video recorder is set to DHCP, disable DHCP to allow the video recorder to keep a static (non-changing) IP address. By default most video recorders are set statically at 192.168.1.108. If the gateway noted in the previous step is different (i.e. 10.1.10.1), change the gateway IP address in the video recorder to match the current network gateway and also change the IP address to match the gateway (i.e. 10.1.10.108). When changing the IP address of the video recorder, make sure that IP address is available by using the **ping** command in a CMD prompt (Windows) or Terminal (Mac). Also in more uncommon situations, the subnet mask may also be different and may need to be changed to match the network.

4. Take note of the video recorder's HTTP and TCP ports (Main Menu > Setting > Network). The HTTP port is the web port used to view the video recorder (or camera) on web browsers and the TCP port is the port used for mobile devices (DMSS) and VMS software (PSS). By default the HTTP port is 80 and the TCP port is 37777. If there is more than one video recorder to be forwarded through the same network, the IP address, HTTP and TCP ports must be different on each unit to differentiate them (i.e. 192.168.1.108 – 81 - 40001, 192.168.1.109 – 82 - 40002, etc.). Some ISPs do not allow for port 80 to be forwarded; in this case, the HTTP port should be changed on the video recorder and forwarded instead.
5. Access the router by inputting the gateway IP address noted in step 2, into a web browser. The router will usually ask for a username and password; if the log in information was changed from

default, find out the credentials from the network administrator or internet service provider. Some of the more common default router log in combos are admin:admin and admin:password. Default router log in information can also be found on http://www.routerpasswords.com.

6. Once logged into the router, navigate to the Internet or Status section and find the IP address of the router. If the WAN IP address appears to look like a LAN IP (i.e. 192.168.x.x or 10.x.x.x), then another router is assigning this router an IP and the ports will need to be forwarded through both (see Multiple Router Port Forwarding section below for more details). Navigate to the Advanced section of the router and look for a Gaming/Applications, Port Forwarding, Pinholes or Virtual Servers menu. Sometimes the Port Forwarding menu can be located in the Firewall section of the router as well. Every router brand and model is different, however there are two basic setups:
    1. The router allows for a set number of rules; in this case, select Custom Ports (rather than a preset port) if the option is available. For each rule, the router will usually ask for a private (internal) and public (external) port range. Use the same port for all entries. The rule will also have a protocol setting; set it to TCP. Enter in the local (LAN) IP address of the video recorder that corresponds to the port being forwarded. Make sure to save the port forwarding rules before navigating away from the menu.
    2. The router allows for port groups; in this case, a port group will have to be created and then assigned to an IP. When creating the group, name it something like "DVR_http" or "DVR_tcp". On some routers, multiple port ranges can be added to the same group. After creating (and saving) the group, assign the group to the IP address of the video recorder. Save the port forwarding rules before navigating away from the menu.

7. After setting up the port forwarding rules, go to a website such as www.canyouseeme.org or www.yougetsignal.com/tools/open-ports/ to check and make sure that the ports are open. If the TCP port is open, but not the HTTP port, try changing the HTTP port to a number other than 80 or 8080 (i.e. 2000). If both HTTP and TCP are not open, try the following steps:
    1. Check the router for any firewall settings that could be blocking remote access. Every router make and model is different when it comes to firewall settings.
    2. Try setting up a DMZ host. To do so, navigate to the Advanced (or Firewall) section of the router and look for a DMZ submenu. From here, enter in the local (LAN) IP address of the video recorder and save the settings. Sometimes the router will report that there are duplicate port forwarding rules, but this can be ignored. Test to see if the ports are open again. NOTE: The DMZ host only works for one device. The DMZ essentially opens all ports for that one device. Opening a DMZ presents a security vulnerability and the user may opt not to utilize this feature.
    3. If a DMZ host does not open up the ports, then double check to make sure that the router is not behind another router(s). If it is, check the Multiple Router Port Forwarding section below.
    4. If the previous step does not apply, the ISP may be blocking all port forwarding. Call the ISP to find out more information on why port forwarding is not working properly on the routing device. If the client is using a satellite internet service, port forwarding may not work unless additional static IP addresses are purchased.

8. Once the correct ports are confirmed open, take note of the external IP address. The external IP address of the network can be found on www.ipcow.com (or on any of the port checking sites

linked previously). The external IP address can be used to view the device remotely or a DDNS can be setup (more information on remote viewing provided below).

Multiple Router Port Forwarding

After reviewing the previous section, and it is discovered that there are multiple routing devices, take the following steps:

1. Note the routing device that the video recorder is currently attached to. Make sure that the computer used for network configuration is getting it's network connection (IP address) from the same router. As in the previous section (Steps 2-5), access to the router should be done by inputting the router's gateway IP address into a web browser.

2. Log in to the router using the proper log-in credentials (see previous section step 5) and go to the Status or Internet menu of the router. Note the Internet IP address and Default gateway of the router. The IP address will be the dynamic IP address being issued by the router located above the current router in the network structure. The gateway address will be used to access the higher tier router.

3. Forward the HTTP and TCP ports for the video recorder(s) IP address as described in the previous section.

4. Log in to the higher tier router using the Internet gateway address previously noted from Step 2.

5. Navigate to the Status or Internet menu of the higher tier router and inspect the Internet IP address and default gateway. Ensure that it has an address that is being assigned by the ISP either dynamically or statically. If it is another local IP address (i.e. 192.168.x.x or 10.x.x.x), then there may be a third router; this process will have to be repeated for each additional router.

6. Repeat the port forwarding steps 6 and 7 from the previous section, however the ports must be forwarded for the Internet IP of the lower tier router (rather than the local IP address of the video recorder)

7. Repeat step 7 from the previous section to check to see if the ports are open.

8. Repeat all steps from this section if there is any additional routers that the ports need to be forwarded through.

Managing an network IP camera system

Besides port forwarding, managing a network IP camera system requires changing device IP addresses to prevent conflicts, plotting out power over Ethernet (PoE) switches and cable distances. This next section will give some basic information on how to organize and maintain an network camera setup. iMaxCamPro recommends using a Windows PC so that the installer can use the ConfigTool to configure a new network IP camera system. If a Mac is used, a custom network must be created and each camera must be attached and configured one at a time.

Configuring using the ConfigTool (Windows)

1. Download the ConfigTool here. Uncompress the ConfigTool.zip file and run the ConfigTool.exe application file. Allow the ConfigTool through any firewall alerts.

2. In the lower left hand corner of the software, in the IP Version dropdown, select IPv4.

3. Click the Refresh button. The ConfigTool should now list all attached devices IP addresses.

4. With the latest firmware, the network IP cameras will be set to DHCP. If all the devices listed on the ConfigTool have different IP addresses, then the installer can move on to adding the cameras into the network video recorder(s) or VMS software.

5. If the cameras are all set to the default static 192.168.1.108, then they must be changed to different IP addresses that match the current network segment Using the ConfigTool, double click a device listed in the program and log in. If the device is on a different segment than 192.168.1.1, then the program will request an IP address and default gateway change, otherwise it will log in. In either case, change the IP address to an available one on the LAN and also make sure that the gateway and subnet mask is correct (matches the LAN settings).

6. Repeat step 5 on all cameras, ensuring each one has a different IP address. iMaxCamPro suggests ordering the IP address to keep things organized. For example, 192.168.1.201, 192.168.1.202, 192.168.1.203 and so on.

7. If the client wants to access the cameras remotely, independently from a video recorder, then each camera must have differing HTTP and TCP ports. iMaxCamPro suggests using 2xxx for the HTTP port and 40xxx for the TCP port (i.e. 2001 / 40001, 2002 / 40002, etc.)

Configuring using a Mac computer

1. First check to see if the cameras are set to DHCP by default. To do so, connect all cameras to the network and log in to the router using the default gateway. Most routers have a connected devices menu that will show all devices connected to the router and what IP addresses are being assigned. Check if the cameras are listed in the connected devices and try to log in to a few of the IP addresses using Safari. If the cameras are confirmed as set to DHCP, then no further camera configuration is needed.

2. If the cameras are not on DHCP, then a new network location must be created. Choose Apple menu > System Preferences, and then click Network. Choose Edit Locations from the Location pop-up menu, and then click Add (+). Enter settings for that match the network segment the cameras are on by default which is gateway 192.168.1.1, subnet 255.255.255.0 and the local IP of the Mac computer can be set to 192.168.1.2.

3. After setting up the new network location, connect one camera to the Mac. Usually this is done by connecting a PoE switch to the Mac's Ethernet port.

4. Using Safari, connect to the default static IP address of the camera – 192.168.1.108. Log in to the Web Service using the default credentials – admin : admin. Click the Setup tab and navigate to the Network menu on the left. Change the IP address, default gateway and subnet mask of

the target network segment in the TCP/IP submenu. Be aware that after changing the information, the installer will not be able to access the camera on the custom network location, so make sure the information is correct.

5. Repeat step 4 for each camera, making sure that each IP address is unique and available on the target network segment.

Bandwidth and throughput limitations

When setting up a security camera system, the most frequent bottleneck to viewing performance is low bandwidth both on the LAN and WAN. This is especially true when working with network IP cameras. Low bandwidth can cause live video streams to appear staggered or laggy, jumping between frames and missing seconds of footage. Here are some steps you can take to improve or troubleshoot bandwidth related issues:

LAN (Local Area Network)

- Lowering main stream encode settings over all cameras can improve recordings if lag is experienced, however this can adversely affect image quality in both live streams and recorded footage. It is also suggested to change the bitrate to CBR (constant bitrate) if there is lag on recorded footage.

- All iMaxCamPro video recorder units have 10/100/1000M (gigabit) uplink ports, however our network IP cameras do not. This means that when using multiple (8+) network cameras, it is suggested to use gigabit networking devices (switches and routers) when viewing them through a network video recorder. Using quality networking devices can drastically improve LAN performance.

- Many times it is preferred to use a separate dedicated router for the camera system which can improve network load balancing and throughput management.

- Using Cat6 cabling may improve throughput, albeit minimally. Also gigabit network devices (switches and routers) will be necessary to see any improvement from using higher quality network cabling.

WAN (Wide Area Network)

- When viewing remotely either through the Web Service, PSS or DMSS it is advised to use the extra stream. Extra stream is set to a low encode settings (resolution and bitrate) specifically for viewing remotely. Be aware, that extra stream does not have as good video quality as main stream, so if higher quality is required for remote live viewing then lowering main stream encode settings may be required.

- Generally, bandwidth and throughput is highly dependent on the internet service package the client is receives from their ISP. An improvement to remote viewing is made by increasing upload speeds, which means upgrading the whole package. iMaxCamPro suggests at least 2MB upload speed per network camera, or around 25MB for a large camera system.

Other considerations

Here is a quick list of other factors that need to considered when networking a security camera system:

- Specifications may require not recording at the location of the cameras. Remote recording can be accomplished with iMaxCamPro video recorders. iMaxCamPro suggests placing a video recorder at both the recording and the camera location to ensure network stability. To add the cameras remotely from the camera location's video recorder, it is as simple as using the external IP address and TCP port of the remote locations recorder and add it to the recording network video recorder as a remote device using the correct remote channel. For more information refer to this article.

- Certain iMaxCamPro cameras are wireless (Wi-Fi) capable. Wi-Fi capability can be enabled by logging into the camera via the Web Service and setting up connectivity with the appropriate Wi-Fi routing device. For more information on Wi-Fi setup, refer to this article.