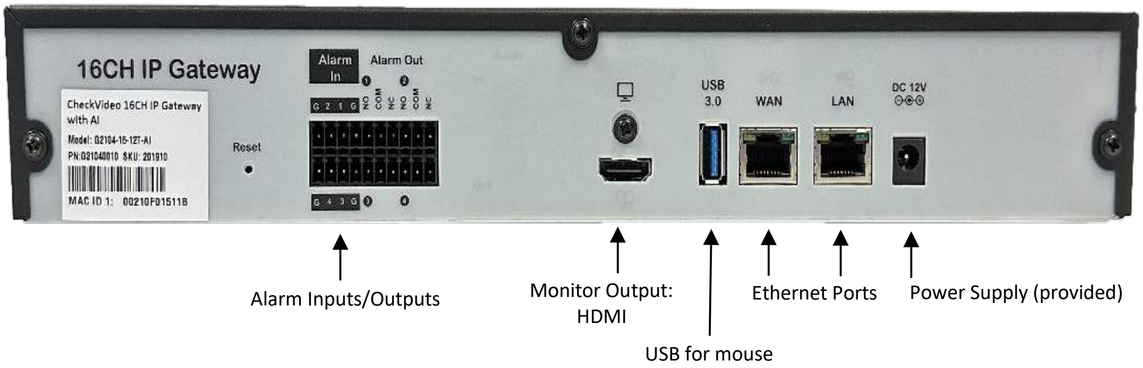
CV4IP Network Connection Guide

G1104 and G2104

The CV4IP Gateway is used to add analytics and cloud management to IP cameras. It serves as an NVR with 24x7 local recording, providing backup to event clips in the cloud.

This documentation describes the connection of the IP Gateway's network ports to third-party IP cameras.

The CV4IP has two network ports. One is designated the LAN port. The second port is the WAN port. Two separate switches are required to correctly set up the CV4IP.

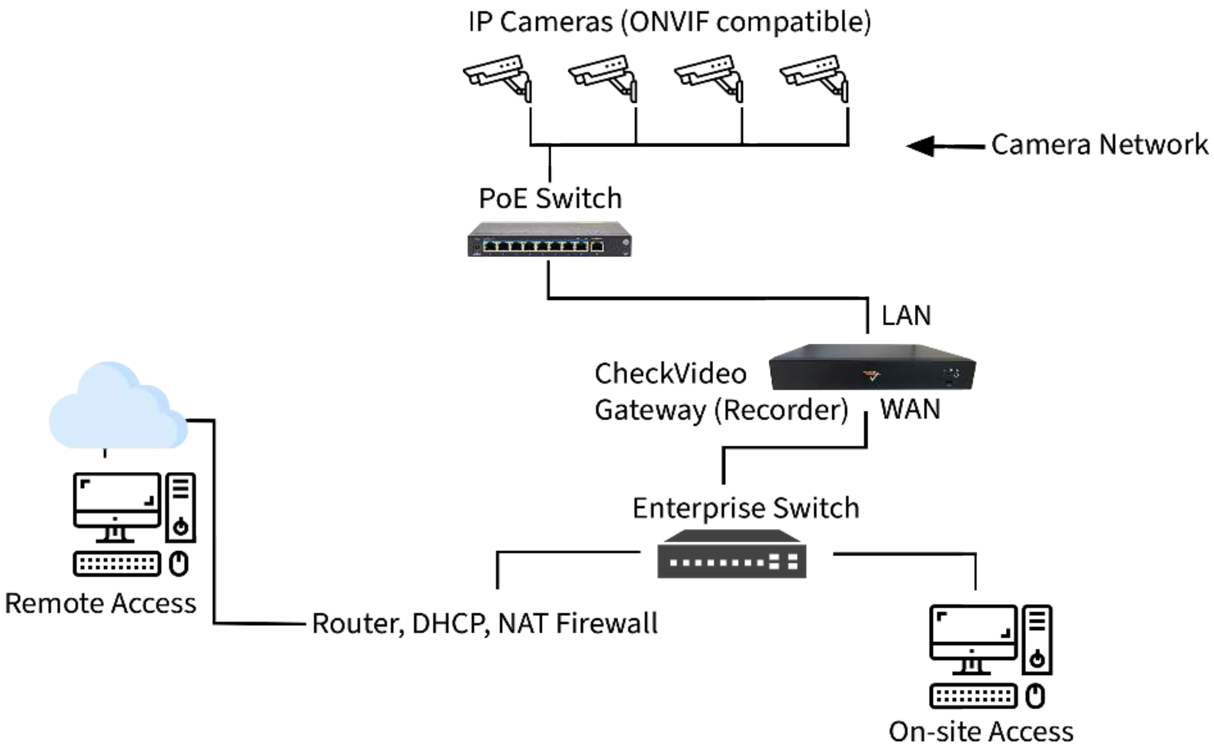


i. The main port or WAN port of the gateway is connected to a switch which uplinks to the Internet, like CheckVideo cameras. For enhanced cybersecurity, non-CheckVideo cameras must not be connected to the WAN switch. The WAN port may connect to a customer provided switch or to a new router that is installed and uplinked into an Internet modem/circuit. The router must be set up to provide DHCP addresses.

   Important: **Do not connect the LAN or WAN port of the gateway to a passive PoE port, injector or midspan as it will damage the gateway. In comparison, active PoE switches know to turn off power when not required. Passive PoE always applies power.**

ii. The second port, or LAN port, of the gateway is for the camera network controlled by the gateway and used ONLY by the gateway. Nothing other than 3rd party IP cameras must be connected to the LAN switch. This isolates cameras from the rest of the customer network. The LAN side of the gateway has no other connection to the Internet.

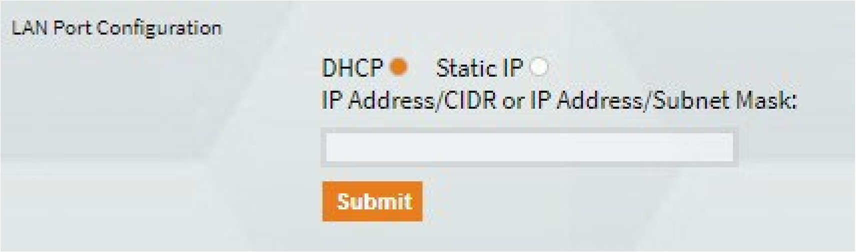
   CAUTION: DO NOT CONNECT the LAN port and WAN port to the same switch, unless they are on different VLANs. Since these are plugged into separate switches, DO NOT bridge those switches/networks/VLANs.



iii. The LAN port of the gateway can be used to keep third party, more vulnerable cameras off the Internet and off the corporate network. The gateway will see those cameras but other network routes to the camera network will be blocked by the gateway, effectively serving as a firewall.

iv. Due to the isolation of the cameras from the customer network and internet, timestamps enabled via the camera interface are not recommended. These timestamps will drift over time and will not match the time accuracy of the gateway. Please see the camera manufacturer documentation for help on how to disable the timestamp. CheckVideo servers maintain accurate time stamps for recording purposes.

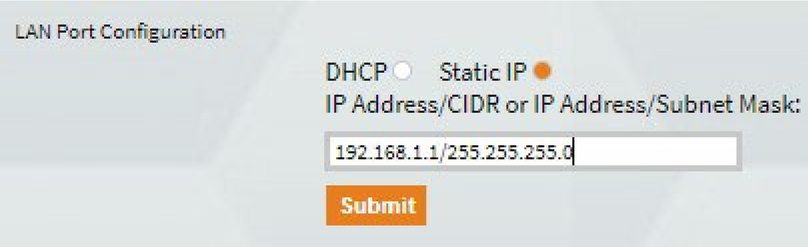
v. You can set the gateway to provide DHCP or Static IP. There are several scenarios listed below. For more advanced networking, refer to the concluding section in this document:
   a. Use DHCP when you have only 1 gateway on site providing IP addresses for all cameras on the LAN network. The Manage Device page default appears below which is the appropriate for DHCP:


LAN Port Configuration

DHCP ● Static IP ○
IP Address/CIDR or IP Address/Subnet Mask:

IMPORTANT: It is recommended that DHCP be managed by a DHCP server, while the gateway can be the DHCP server for the cameras, this should be a last resort.

b. If there are multiple gateways at the site and a router/DHCP server is providing DHCP reservations for all devices on network, no network changes are required on the Manage Device page. This is because the default is DHCP. If the gateway determines that another device is providing DHCP to the cameras, it will do nothing.
c. If there are multiple gateways at the site and the router/DHCP server is not providing DHCP reservations, use Static IP addressing on the camera network, or LAN. This is the **preferred configuration because it is the least likely to experience networking issues long term.** For example, if you have 10 cameras on the camera network, they could each have their IP address in the sequence 192.168.1.2, 192.168.1.3, 192.168.1.4, …. 192.168.1.11. In this example, the netmask used will be 255.255.255.0 and the gateway could be 192.168.1.1. The IP address for the gateway can be set through the portal under Devices->Manage Device.



LAN Port Configuration

DHCP ○ Static IP ●

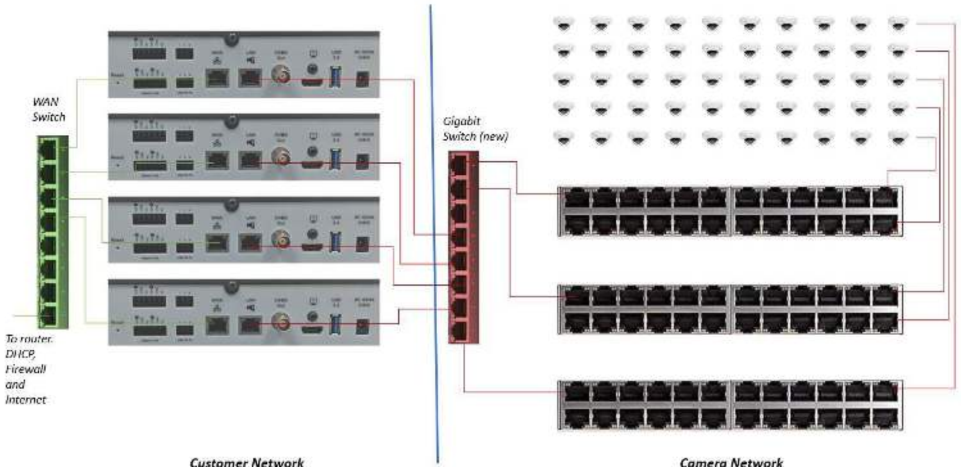
IP Address/CIDR or IP Address/Subnet Mask:

192.168.1.1/255.255.255.0

IMPORTANT: Note that the above is simply an example provided when cameras use IP addresses in the range 192.168.1.x. If cameras are already assigned IP addresses, they may not be in the range 192.168.1.x. They may use a different base address such as 10.1.2.x in which case the entry for the LAN address for the CV4IP must be in the subnet range used by the cameras. ***Make sure that the IP address used for the LAN port is unique and is NOT assigned to any camera, gateway or other device on the network***.

The Camera Validation Tool, available at www.checkvideo.com/support can be used to scan the network for existing cameras and find their IP addresses. Note this only works for ONVIF cameras. If you have other cameras, you can use an application like Advanced IP Scanner to get the IP addresses for those cameras.

If there are more than 16 cameras on the camera network, multiple gateways will be required. In that instance your network topology may look like the image below. Ensure that the gigabit switch is adequately sized to support the throughput traffic between the cameras and the gateways.



Step-by-Step Connection Instructions

Below are instructions for configuring a camera to the gateway. *For more detailed documentation, refer to Adding and Configuring the Gateway document which can be found at CheckVideo.com/Support.*

1. Starting with the gateway powered off, find or install the WAN switch that has Internet connectivity. Connect a PC to the switch and verify connectivity to your portal, e.g. portal.checkvideo.net. If ok, connect the WAN port of the gateway to the WAN switch.
2. Power on the gateway, log into your CheckVideo portal account and add it to the portal if not already added. If you have issues adding the gateway, connect a monitor to the gateway's HDMI port and a keyboard to the USB port. Use ALT-CTRL-N to view the gateway's current network status. Ensure that the gateway has received an IP address from the network. It will also display the ARP and route table between the gateway and other network devices.
3. Find the switch(es) for the camera network. Connect a PC and find IP addresses for all cameras. Use the configuration from an existing NVR or use a tool such as the CheckVideo Camera Validation Tool or Advanced IP Scanner to find the IP addresses. You may require a new Gigabit switch (shown in red) to aggregate traffic from multiple switches. This switch should have enough switching capacity for all cameras downstream of it. Connect this switch to the LAN port on each gateway.
4. On the portal, navigate to Devices > Configure IP Gateway.
5. On this page, select the IP gateway to pair to these cameras and click "Enter ONVIF Credentials".
6. Assuming that all of your cameras have the same ONVIF username and password, you will only have to fill out this area once. Once you have entered the username and password, click "Discover IP Cameras".
7. It will take a couple of minutes for this gateway to find, via ONVIF, all cameras connected to the LAN camera network. If a camera is not found, it can be added by entering the IP address via the bottom of the "Enter Onvif Credentials" area.
8. When the page populates with cameras available to be added, add up to the number of cameras supported by your gateway (ensure bitrate for cameras is under 4Mbps). In addition to channel limits, there are capacity limits as well. Consider using the IP Gateway calculator to confirm the maximum

number of channels per gateway based upon camera settings. You can get this calculator by emailing support@checkvideo.com.

9. Within Configure IP Gateway, click the thumbnail for one camera at a time, use the “Assign” button to confirm the username, password, RTSP URL, alternate resolution (choose the highest available), and alternate framerate (leave this at 10) of the camera. Once confirmed, click the “Verify” button to finish adding the camera. If Verification fails, use the Camera Validation Tool to change camera settings for compatibility and try again.
10. Once all cameras have been successfully added to the first gateway, select the next gateway (if applicable) and repeat steps 4-9.

Advanced Networking: Configure Static Routes for Cameras on Multiple Subnets

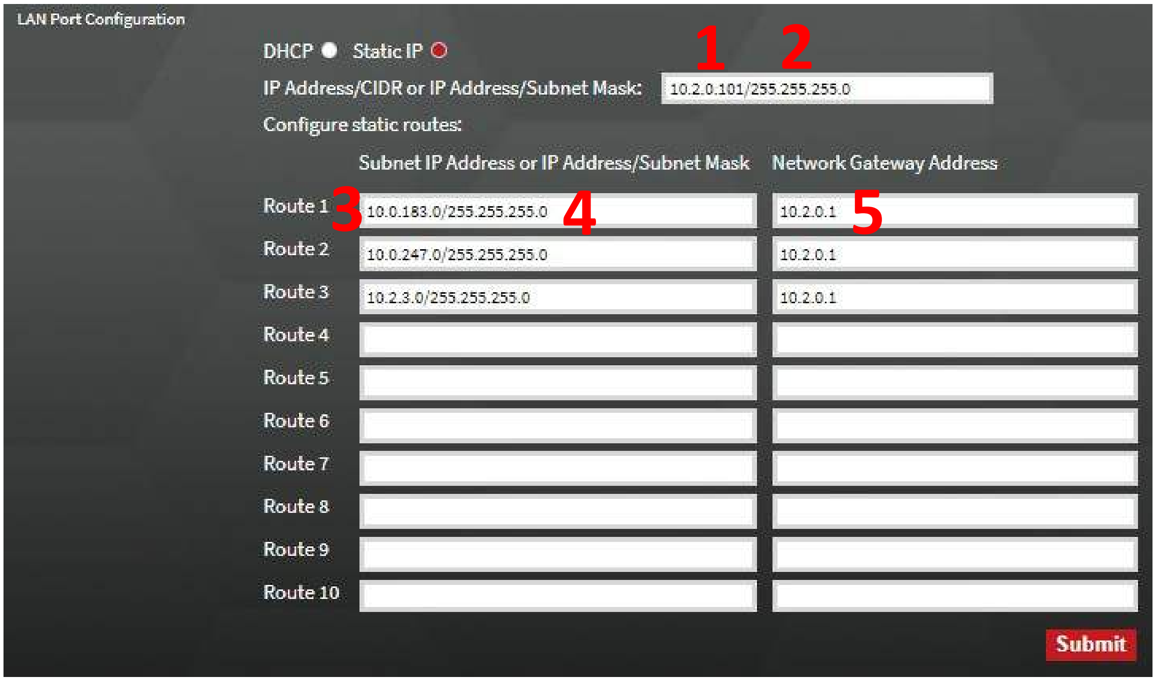
Cameras present on the same local network as the gateway but placed on different subnets can still be added to the gateway. Before proceeding, several pieces of information are required, which may require support from the client’s IT department:

1) Static IP, or DHCP, reservation information (local) for each camera
2) Static IP, or DHCP, reservation information (local) for the gateway LAN port
3) Subnet mask information for each camera and the gateway

The next two steps must be performed before attempting to assign the cameras to the gateway…

To begin, navigate to the Devices->Manage Device page and enter gateway IP/subnet Mask information as illustrated in the example within Item V on Page 2 of this document.

Next, enter route information for each camera as seen in the example below:



LAN Port Configuration

DHCP ○ Static IP ●

IP Address/CIDR or IP Address/Subnet Mask: 10.2.0.101/255.255.255.0

Configure static routes:

	Subnet IP Address or IP Address/Subnet Mask	Network Gateway Address
Route 1	10.0.183.0/255.255.255.0	10.2.0.1
Route 2	10.0.247.0/255.255.255.0	10.2.0.1
Route 3	10.2.3.0/255.255.255.0	10.2.0.1
Route 4		
Route 5		
Route 6		
Route 7		
Route 8		
Route 9		
Route 10		

1) Gateway Local IP – LAN Port
(ex. 10.2.0.101)

2) Gateway LAN Subnet Mask
(ex. 255.255.255.0)

3) Camera Local IP
(ex. 10.0.183.0)

4) Camera Subnet Mask
(ex. 255.255.255.0)

5) Gateway Local IP
(10.2.0.1)

Using Route 1 above as an example: We enter the local IP address of the camera along with its subnet mask. Note that “0” must replace the host ID component of the camera’s local IP address. **Note: The Network Gateway Addresses will be determined by the network configuration for all routes. Most times, the gateway will be either the first or the last addressable IP address in the subnet.**

Cameras can now be added to the gateway**.** ***<u>Cameras on static routes must be added via targeted onvif request, not ONVIF Discovery.</u>*** Cameras on subnets may be added via RTSP as normal – no special information is required after completing the above, but a camera added via RTSP will have limited functionality.