

CV4IP Network Connection Guide

The CV4IP Gateway is used to add analytics and cloud management to IP cameras. It serves as a NVR doing 24x7 recording on the Gateway, and also provides backup video in the cloud.

This documentation describes connection of the network ports of the IP Gateway 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.

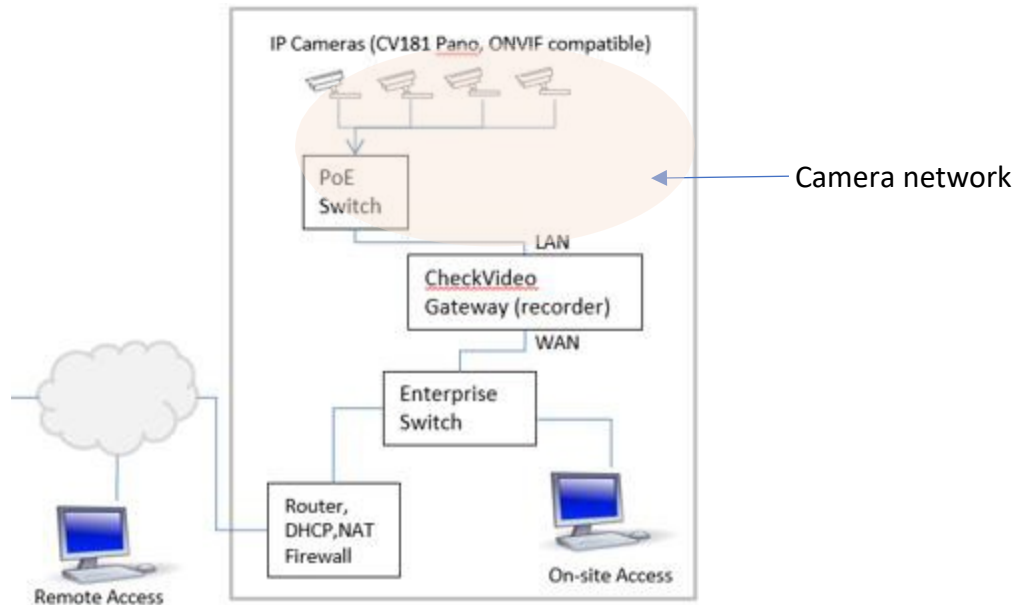


- i. The main port or WAN port of the gateway is connected to a switch which uplinks to the Internet, similar to other CheckVideo cameras. For enhanced cybersecurity, non-CheckVideo cameras must not be connected to the WAN switch. This port may connect to a customer provided switch or to a new router 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, it will damage the gateway. Active PoE switches know to turn off power when not required, passive PoE keeps power on at all times.

- 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 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. Since these are plugged into separate switches DO NOT connect those switches.



- iii. The LAN port of the gateway can be used to keep third party, possibly 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, camera embedded timestamps are not recommended. These timestamps will drift over time and will not be accurate. Please see the camera manufacturer documentation for help on how to disable the timestamp. This will require logging into the camera and disabling the timestamp. CheckVideo servers maintain accurate time stamps for recording purposes.
- v. Static IP addressing of cameras on the camera network, or LAN, is the preferred configuration. 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 will 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

Submit

IMPORTANT: Note that the above is simply an example provided 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 on the network.**

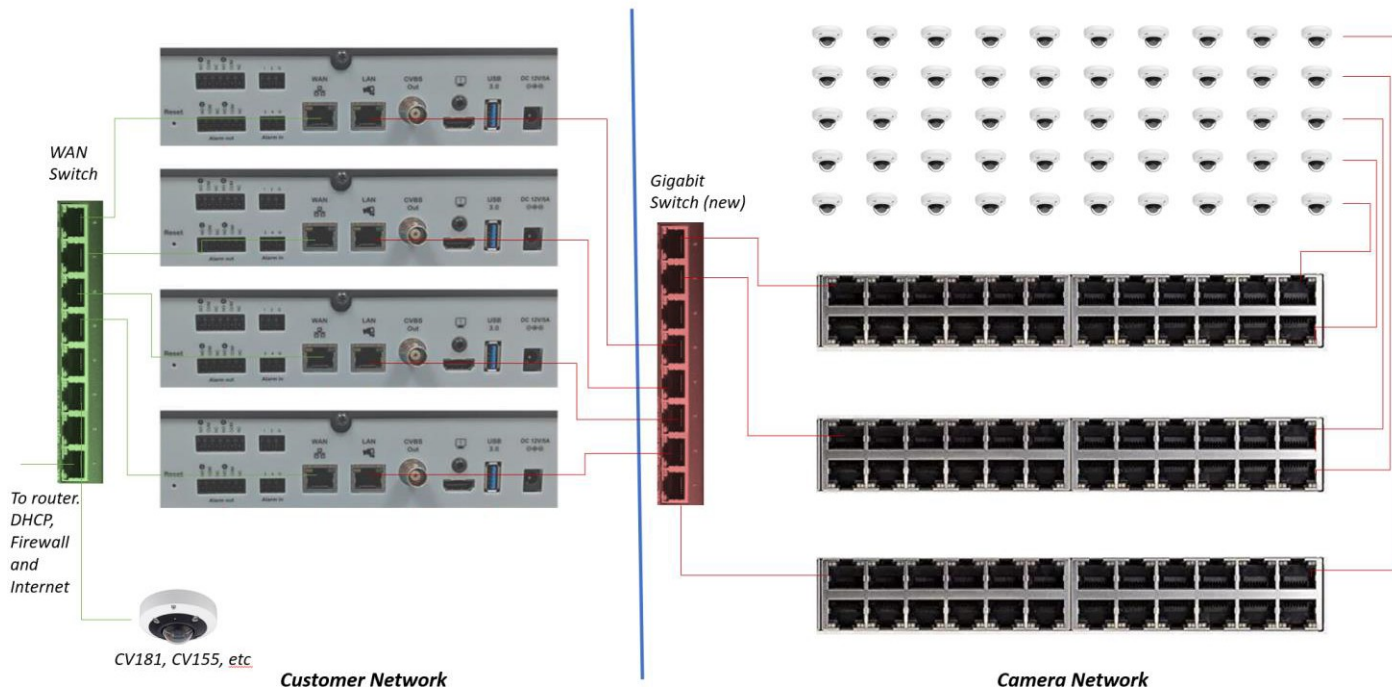
The Camera Validation Tool, available at www.checkvideo.com/support can be used to scan the network for existing cameras and find their IP addresses. Note this only works for ONVIF cameras, if you have other cameras, you will have to consult the existing NVR to get IP addresses for cameras.

Special Note: CV181 cameras require a gateway and must be connected to the WAN switch, same as the gateway WAN port. Similarly, any other CV cameras such as the CV155 must be connected to the WAN switch.

- vi. If the camera network is set for DHCP, you do not have to set up the Static IP in Step v above. Instead, change the gateway configuration to DHCP and leave the IP address blank. **IMPORTANT: If you use this configuration, power up at least one gateway before powering up cameras.**



- vii. If there are more than 16 cameras on the camera network, multiple gateways will be required. The LAN port for each gateway can be connected to a new gigabit switch, which is in turn connected to switches that are connected to the IP cameras.



Step-by-Step Connection Instructions

1. Starting with the gateway powered off, find or install the WAN switch that has Internet connectivity. Connect a PC this 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 portal account and add it to the portal if not already added.
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 Camera Validation Tool 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 sufficient 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 you are unable to find all cameras using ONVIF, the other option is to connect directly to the camera IP address, log into the camera and find its RTSP URL, which can be manually entered on the web portal.
8. When the page populates with cameras available to be added, add up to 16 cameras to this gateway (ensure bitrate for cameras is under 4Mbps). 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.
9. Once all cameras have been successfully added to the first gateway, select the next gateway (if applicable) and repeat steps 4-8.