Typical Qorvus Qnode configuration for IP surveillance camera CCTV applications

Please note: all Qorvus equipment is licensed for installation by an experienced professional wireless field engineer only. If in doubt about any aspect of your installation, please contact Qorvus or a qualified wireless installation engineer. Poor installation practices such as incorrect antenna orientation or positioning, inadequate waterproofing, missing surge or lightning protection, or improper grounding may result in personal injury, substandard performance or equipment damage which is not covered by the warranty!
1) **Important**: if your Qorvus wireless mesh nodes have been pre-configured at the factory for installation at your facility (most have) you should NOT normally change anything on their setup other than, possibly, the ethernet port settings or camera IP host-mapping (WAN/LAN or NAT/PAT/Server pages on the GUI).

All Qorvus nodes are configured either as a **Gateway** (to be installed at your central office and attached to your internet router and / or NVR) or a **Repeater** (wireless downstream nodes that will typically have one or more IP cameras and / or portable devices such as laptops or bar-code scanners associated with them).

2) The **Gateway** node should be installed first. Once it is attached to your internet router / switch and powered up, it will request a DHCP address from the router and, upon boot-up completion (all three LEDs on), you will be able to reach the gateway node’s GUI by surfing to `http://<the_nodes_dhcp_address>:81/`. You will need to look at your router’s DHCP client list to find the node, which will be called `Qmesh` or the name that has been assigned to the node during configuration. Note – if the Gateway node does not obtain a DHCP address, it will default to a static address of 192.168.1.2

For example if your DHCP router hands out 192.168.1.100, you can reach the gateway node at that address on port 81 (on address bar type:- `http://192.168.1.100:81`).

The default user name for the GUI access is **admin**, and the default password is **wsxedc**.

Qorvus can help you with the following steps – just call **800.757.1571 Ext 105**
3) Pre-configured gateway nodes are shipped with a persistent tunnel configured back to one of our servers at the factory. This allows Qorvus service engineers to VPN into your gateway node to assist you in your installation of nodes and cameras, and to modify the firmware or radio setup if needed.

4) If required for compatibility with your internal network, you can change the LAN address on your gateway node to your choice of any static IP, Netmask, and DNS server address. However if you change to a non-functioning setup, we will lose the ability to contact your gateway remotely. To set up your ethernet port, select **LAN/WAN** tab:

This will take you to **LAN/WAN Interface Settings** page where you can make any needed changes to the nodes primary ethernet address, net-mask, gateway router, and DNS values.
5) Once the gateway node has been installed and tested for proper operation, you can begin to install the repeater nodes as indicated on the Qorvus-supplied map and attached documentation. **You should NOT need to change anything on the repeater nodes other than, possibly, the ethernet port setup.**

6) Each **repeater node** may be attached to one or more **IP cameras or IP encoders** that will use it for backhaul to your gateway and NVR. **If there is just one IP camera allocated to a given node,** this can be accomplished by plugging a **cross-over cable** between the PoE injector for the node, and the PoE injector for the camera. However, **if two or more cameras are to be attached to a given node,** you will need to use a small (e.g. Netgear 5-port) switch to attach the cams to the nodes ethernet port via its PoE injector, as in the illustration at the beginning of this document.

7) **Mobotix IP cameras are automatically detected by the repeater when they are powered up.** The repeater then sends the local camera information to the gateway node, which uses it to set up internal multi-homed NAT addresses for each camera on the gateway node’s ethernet port (see example below).

8) **Non-Mobotix IP cameras or encoders** (e.g. Axis, American Dynamics, Sony, etc) will need to be **manually set up for compatibility with the repeater nodes ethernet port.** By default, the address on the ethernet port of each repeater node is 192.168.1.2. This can be changed if needed to any private IP space but it must be on a **different subnet from the private IP space you wish to use at the gateway node.** For example, if your gateway node is operating at 192.168.1.10, the repeater (and associated cameras) could be set up at e.g. 192.168.2.2 or 192.168.0.2 and the attached cams at 192.168.2.5, .6, .7, etc.

9) At the gateway node, once you have your cameras and repeater nodes installed and working, you can begin to setup the local addresses on the gateway node’s ethernet port for the remote cameras. **This will happen automatically when you are using Mobotix cameras, a few minutes after the repeater nodes and cams have been powered on and are wirelessly associating with the gateway node.**
This setup will need to be done manually for non-Mobotix cameras. On the gateway node, surf to the GUI, and select the Advanced Settings tab, then the NAT/PAT tab.

Example setup for IP camera or encoder

Referring to the GUI snapshot below, after configuration, each wireless IP camera or encoder will be reachable via a unique Local IP Address on the left-hand column, which must be on a separate sub-net from the Remote IP Address (these are the addresses you previously assigned to the remote IP camera or encoders ethernet port). In the example below, 192.168.2.61, will map to a remote camera (for example 192.168.1.33), which is attached to that specific repeater node. Each repeater node has a unique 3-digit cell-ID which is used to identify it for this purpose (for example 134). The Cell-ID of each repeater can be obtained by looking at the gateway nodes list of active nodes on the main page of the GUI.

1. Fill out:
   (a) Local IP addresses (this can be whatever you like, but should be outside of the DHCP range of your internet router)
   (b) Remote Cell ID, (corresponding to the unique 3-digit cell-ID of each repeater node to which your cameras are attached), and
   (c) Remote IP address (the address you previously assigned to the ethernet port of each camera or IP encoder)

In the example shown below, there is one camera attached to a repeater node with the Cell-ID 134, another one attached to a separate repeater node with a Cell-ID of 228, and a third camera attached to the third node with cell-ID of 214, for a total of three cameras and three repeater nodes. It is OK to attach several cameras to one repeater node, so long as each camera has its own IP address.

Once you've completed this process and have rebooted the gateway node, each of the three cameras can then be reached separately by surfing to the respective Local IP in the left-hand column, and these local IP’s are also the ones that would be used by any NVR (network video recorder) application attached to your network.

2. Enable NAT Mapping: select Yes

3. Select Update button

4. Reboot the node (Basic Settings / General Tab)
This host-map setup process is handled automatically for Mobotix cameras - once all the cameras, repeaters, and gateway are installed and operating, the NAT/PAT page on your gateway node will automatically fill out the cameras, cell IDs, and local IPs over a period of a few minutes. The local IP will start at the starting base address specified on your LAN/WAN page. However, after all of the Mobotix cameras have automatically been set up, you can then change the local IP addresses manually, if needed for your specific requirements.

10) To set up your NVR, just assign the local IP’s in the left-hand column to the logical IP camera IP’s on your specific NVR program. If you wish to use the Mobotix MXCC NVR software application running under Windows you can download a copy of that software here:


Do not try to use automatic camera discovery function in MXCC because that will work only for IP cameras directly attached to the same layer 2 switch as the MXCC desktop computer. Instead, enter the Local IP addresses that you have set up in the left-hand column for each IP camera.

For your convenience in locating the NVR computer, it is also possible to attach your NVR to the ethernet port of one of your repeater nodes and point it to the same Local IP addresses that you have set up at your gateway. However this may require some custom route-adds depending on how your overall
system is set up. This is something that Qorvus engineers can set up for you remotely if needed; please contact us at one of the service numbers or email addresses below.

11) If your nodes are also providing network access to laptop users or portable devices such as barcode scanners, in most cases this will be accomplished via a second 2.4 GHz radio built into each repeater node. The channel, network SSID, etc are all configurable or they can be left at their default setting of Channel-3 with an SSID of QMESH2. There is a captive portal system (which can be disabled) installed on each node that will prompt users for a user name / password or provide guest access to the internet. This captive portal system includes a large number of custom setup and capabilities that are beyond the scope of this document. For more information please contact a Qorvus support technician.

12) Once you have your system completely set up and operating, you can view your IP cameras securely and remotely from anywhere in the world by using the built-in VPN functions in the QnodeJr gateway node. Unless your gateway QnodeJr is directly on a public IP address, you will need to forward one of the public addresses coming into your router, to the local private IP address that your LAN / WAN interface settings are configured for (10.10.16.35 in the earlier LAN/WAN example setup). Once that has been done, surf to the Advanced Settings / Captive Portal page:
Scroll to the bottom, and select **Edit Auto Access List**:

Add a VPN name and password of your choice, and reboot the node.
Then at the desktop computer you wish to use to remotely access your cameras, just set up a new
VPN connection using the Microsoft Connection Wizard, and establish a connection to the public IP you’ve
forwarded or configured on the LAN/WAN page of your gateway node, using the name and password you
previously set up.

Due to commonly-found network delays, you may have to re-try several times to establish a VPN
connection. If after several tries you still can’t connect, check your settings (name / password / IP) and make
sure that your internet router and ISP are set up to allow outbound Microsoft PPTP VPN (GRE47) packets. You
may have to partially disable your inbound or outbound firewall.

Once the connection is established, you will be able to see one or more of your installed cameras by
simply surfing to the Local IP Address of each cam, or http://192.168.2.61/ as in the example above.

Please feel free to contact us at any time during the installation process if you have questions. Once
your gateway is installed to a working internet connection, our engineers can readily VPN into your
system remotely and provide further assistance.

Qorvus Systems, Inc.
800.757.1571 Ext 105
360.243.7371 (direct-dial to support line)
support@qorvus.com (email)

PLEASE NOTE: All Qorvus-supplied software, equipment, services and support, as well as the information on
this and other Qorvus documents and websites is provided on a best-efforts basis with no warranty or
guarantee of availability, error-free operation, installed compliance with any local, state, or federal
regulations, or merchantability or fitness for any particular purpose. By viewing this document, availing
yourself of Qorvus products or services, or by providing Qorvus access to your network or facility, you
expressly indemnify and save harmless Qorvus Systems, Inc., and its agents, affiliates, dealers, contractors,
successors or assigns from any liability for damage of any kind or inability to use said network that may or may
not result from your actions or any actions or inactions by Qorvus, including without limitation any incidental or
consequential damages. Without limitation you further acknowledge that Qorvus products and services are not
sold or authorized for use in life-support, medical, or high-risk security applications. In any event, Qorvus' 
maximum liability is limited to your purchase price. In addition, all conditions of the Qorvus Special
Limited License apply to you. Your use of this website or purchase or use of Qorvus products and services
is your explicit acceptance of these conditions. IF YOU DO NOT AGREE TO THESE CONDITIONS YOU MAY
NOT PURCHASE QORVUS PRODUCTS OR SERVICES, OR MAKE USE OF QORVUS WEBSITES OR
INFORMATION.

This document and all text and diagrams are © 2004-2009 Qorvus Systems, Inc. All Rights Reserved