Using the Matrox Capture Assistant

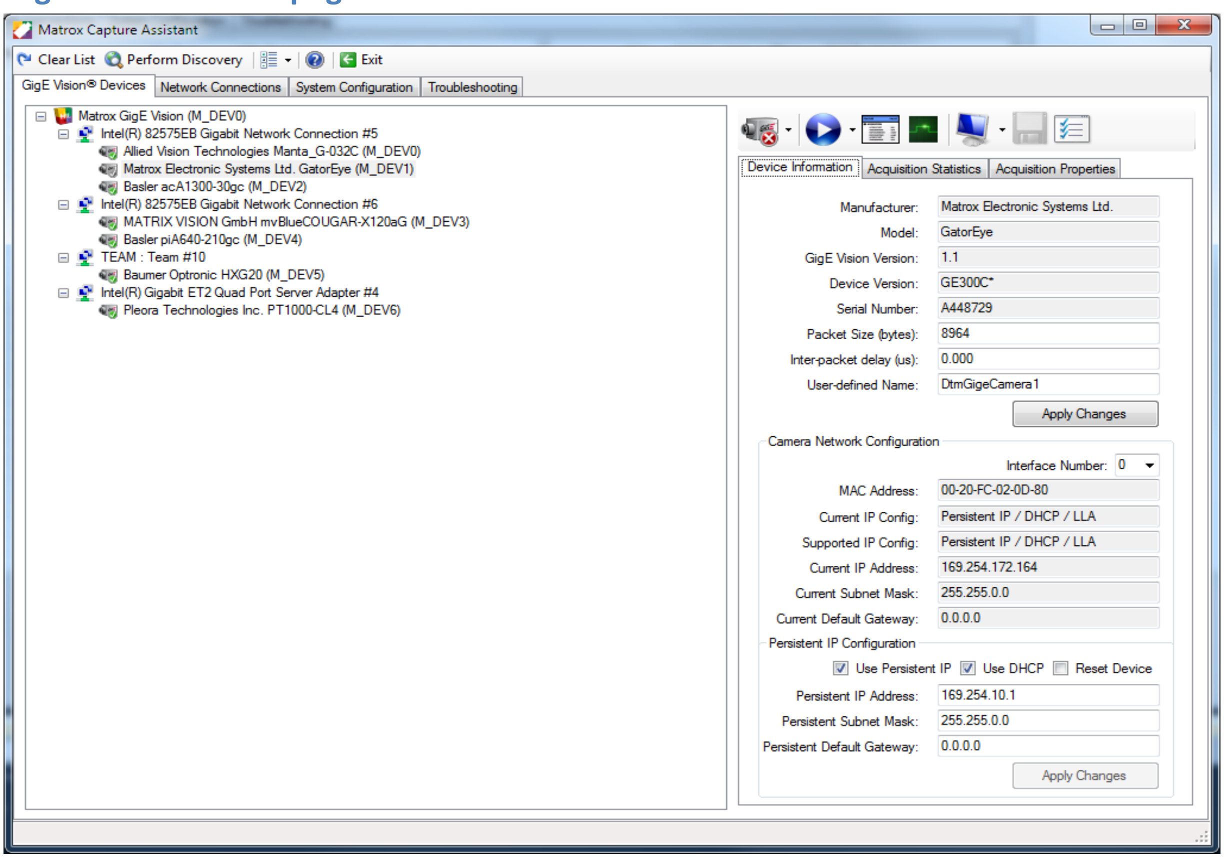
(Using MIL with GigE Vision®)

Matrox Capture Assistant

Matrox Capture Assistant is a tool that allows you to rapidly test and evaluate the performance of virtually any GigE Vision device using the Matrox Imaging Library (MIL)'s GigE Vision driver. It can also be used to configure network adapter settings and specific MIL GigE Vision configuration parameters. The tool has three main sections, each occupying a specific tab.

> ***GigE Vision Devices*** - Lists all detected GigE Vision devices and allows you to directly control setup and acquisition parameters for each device. Note that you must first select a listed GigE Vision device to do so.
>
> ***Network Connections*** - Lists all functioning network adapters installed in the system and allows you to specify the IP settings for each adapter.
>
> ***System Configuration*** - Allows you to control specific connection parameters for a MIL GigE Vision system.

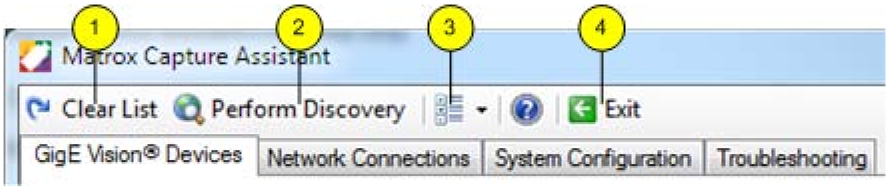
GigE Vision Devices page



1 - Matrox Capture Assistant's ***GigE Vision Devices*** tab.

The ***GigE Vision Devices*** page lists all GigE Vision devices that have been detected with all Ethernet network adapters installed in your computer. It also provides the starting point for you to select each of these devices.

Main tool strip

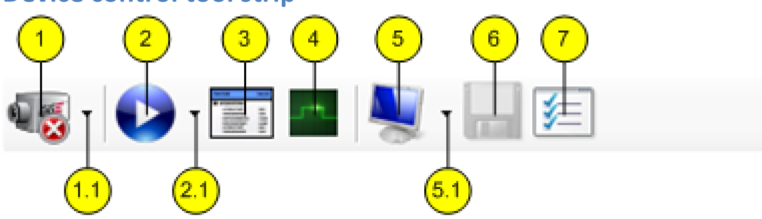


Matrox Capture Assistant's main tool strip

The command bar at the top of Matrox Capture Assistant allows you to detect GigE Vision devices and specify how they should be displayed. It consists of the following buttons.

1. The ***Clear List*** button allows you to flush the camera cache and perform a GigE Vision device discovery.
2. The ***Perform Discovery*** button allows you to perform a GigE Vision device discovery without flushing the camera cache.
3. The ***Change View*** button allows you to control how devices are listed in the GigE Vision Devices page. You can select from among a ***Tree*** view, a ***Details*** view, or a ***Tile*** view.
4. The ***Exit*** button allows you to close the application.

Device control tool strip



Matrox Capture Assistant's device control tool strip

The right side of the ***GigE Vision Devices*** tab contains a set of icons whose functionality allows you to control a selected GigE Vision device.

1. You can use the ***Allocate Device*** button to allocate/free the currently selected GigE Vision device. Note that an allocated device cannot be reallocated or freed (even from a remote computer within a shared corporate network, for example) until it is first freed on the PC on which it has already been allocated.
   1.1 Clicking on the ***Allocate Device*** button's downward-pointing triangle allows you to select from amont the following allocation options:

- The ***Default*** command allows you to allocate the GigE Vision device in standard mode.
- The ***Multicast master*** command allows you to allocate the GigE Vision device in multicast master mode.
- The ***Multicast slave*** command allows you to allocate the GigE Vision device in multicast slave mode.

2. You can use the ***Capture*** button to start or stop capturing images from your GigE Vision device. Note that it is implemented as a split button.

   2.1 Clicking on the ***Capture*** button's downward-pointing triangle allows you to select from among the following acquisition options:

   - The ***Continuous*** and ***Snapshot*** commands allow you to perform a continuous or a single-image grab, respectively, when you press the ***Capture*** button.
   - The ***Buffering*** command allows you to specify the number of image buffers into which the allocated GigE Vision device will capture data when you press the ***Capture*** button. Specifying a larger number of buffers reduces the likelihood of missing frames during acquisition as a result of high system loads.
   - The ***Calculate inter-packet delay*** command opens the inter-packet delay calculator dialog box.

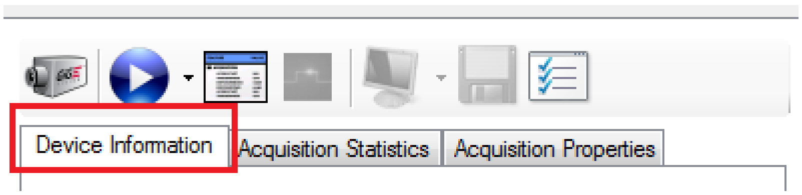
3. You can use the ***Device Features*** button to browse the selected GigE Vision device's features. Note that clicking this button opens a separate dialog box from which you can view and control your GigE Vision device's features. The state of some of your GigE Vision device features might change while an acquisition is in progress; some features might become read-only. Grayed out features indicate that their current state is read-only. These features cannot be written to.
4. If your GigE Vision device is in software triggered mode, you can use the ***Software Trigger*** button to send a software trigger signal to your GigE Vision device . See the Acquisition properties section later in this document to configure your device to operate in triggered mode.
5. You can use the ***Display*** button to show or hide the display window. Note that this is a split button and provides several possibilities.

   5.1 Clicking on the ***Display*** button's downward-pointing triangle allows you to select from among the following display options.

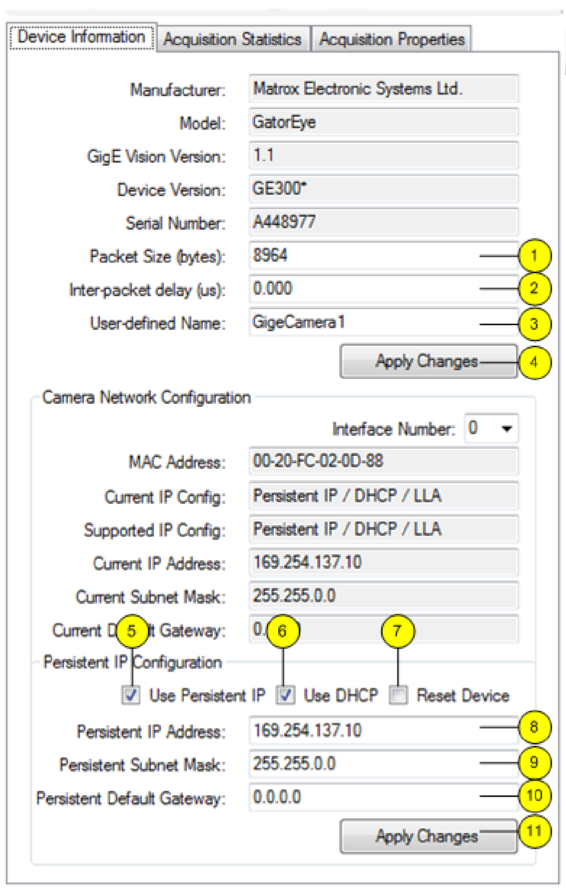
   - The ***Enable*** and ***Disable*** commands allow you to enable or disable the display of acquired images, respectively.
   - The ***Display Mode*** command can be used to convert acquired images to a more appropriate display setting if the displayed image appears incorrectly.
   - The ***Frame Counter*** command displays a running count of the number of grabbed frames in the display window.

6. You can use the ***Save As*** button to save the last acquired image to a file. Note that you can specify one of several file formats.
7. The ***Device Capabilities*** button allows you to open the selected GigE device's GigE Vision device capabilities window.

Device Information



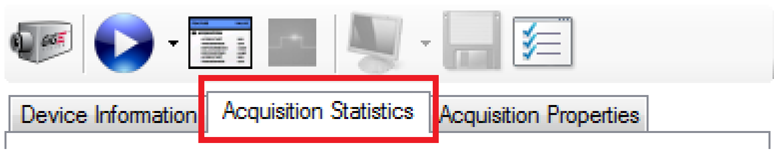
The ***Device Information*** tab on the right pane displays and allows you to specify basic information about the selected GigE Vision device.



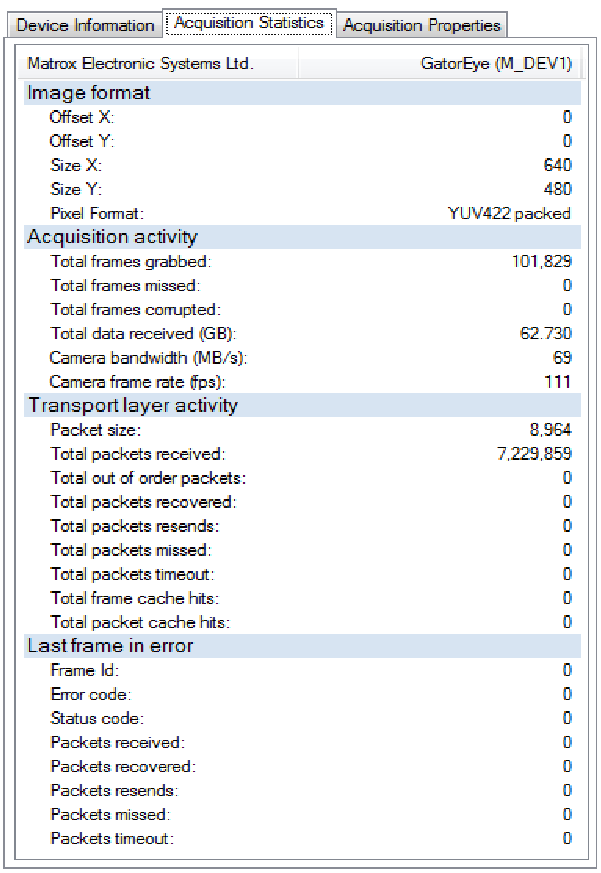
1. Display and specify the size of data packets that the selected GigE Vision will transmit.
2. Display and specify the inter-packet delay that the selected GigE Vision device will use.
3. Display and specify the persistent User-defined Name of the selected GigE Vision device.
4. Writes the packet size, inter-packet delay, and user-defined name to the selected GigE Vision device.
5. Put the selected GigE Vision device in Persistent IP mode.
6. Put the GigE Vision device in DHCP mode.
7. Resets the GigE Vision device (forces device to use the newly updated persistent IP settings.
8. Display and control the persistent IP Address of the selected GigE Vision device.
9. Display and control the persistent subnet mask of the selected GigE Vision device.
10. Display and control the persistent default gateway of the selected GigE Vision device.
11. Write Persistent IP data to the selected GigE

Vision device.

Acquisition Statistics page



The ***Acquisition Statistics*** page displays information about the data being grabbed using the selected GigE Vision device. Note that statistics are displayed not only for GigE Vision devices controlled using Matrox Capture Assistant, but also for GigE Vision devices that are allocated and controlled using other applications running on the same computer. The ***Acquisition Statistics*** page is useful for quickly identifying acquisition problems, which are typically caused by incorrect or non-optimal network settings. See the [Settings for optimal performance] section later in this document for details.

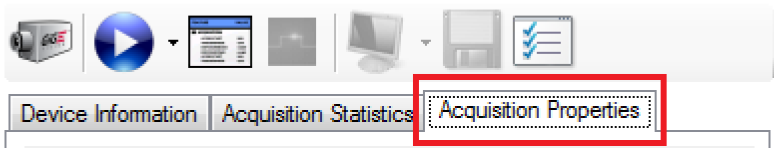


Statistics are divided into three sections.

- The ***Image format*** section describes the pixel format, image size, and offset (if any) of the series of images currently being grabbed.
- The ***Acquisition Activity*** section provides various reliability metrics (such as the number of frames grabbed, missed, or corrupt) in addition to bandwidth and frame rate.
- The ***Transport layer activity*** section displays information about the network data packets that make up the GigE Vision image data being captured. In addition to counting the number of packets received and missed, it also provides information such as the number of packets that have been received out of order, recovered, and re-sent.
- The **Last frame in error** section displays information about the last frame acquired with errors.

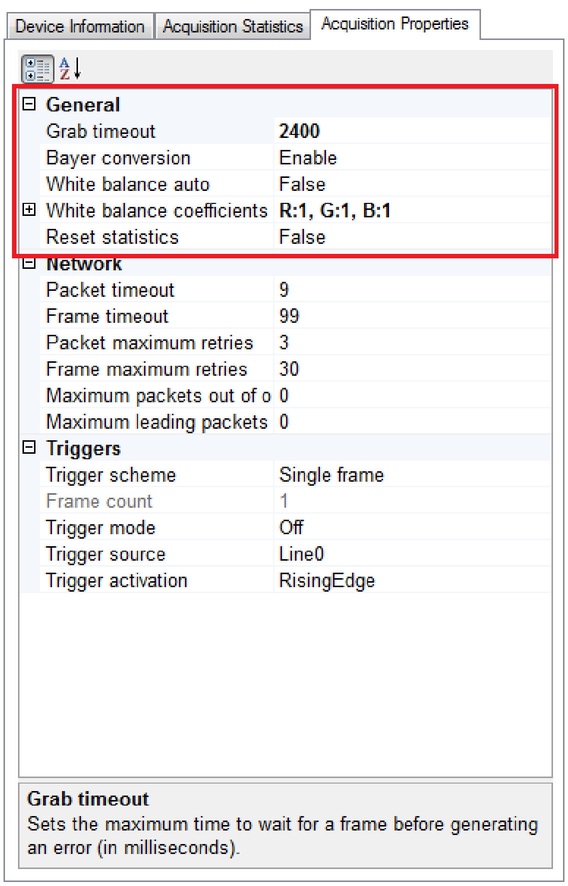
Note that each metric is also described as a tooltip.

Acquisition Properties page



The ***Acquisition Properties*** page allows you to control a number of parameters that govern how a GigE Vision device's general, network, and trigger category properties are managed. Note that the presence and availability of several properties listed depends on the capabilities and current settings of the GigE Vision device selected.

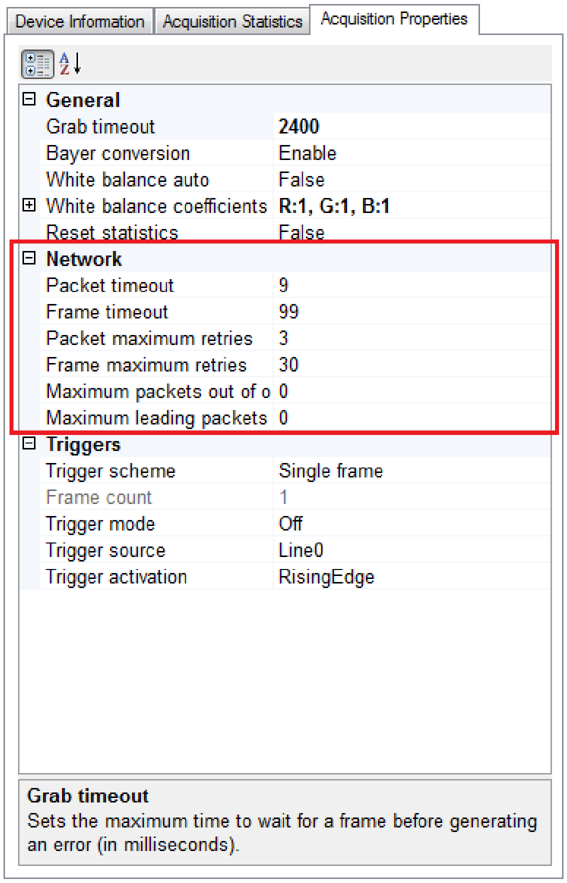
General properties



Properties in this category perform various operations such as Bayer color conversions and color balancing.

1. ***Grab timeout*** – Specifies the maximum time to wait for a frame (in milliseconds) before generating an error.
2. ***Bayer conversion*** – For Bayer-encoded images, specifies whether a color conversion is performed by MIL's GigE Vision driver.
3. ***White balance auto*** – For Bayer-encoded images, specifies whether an automatic white balance (color balance) calculation is performed.
4. ***White balance coefficients*** – For Bayer-encoded images, specifies the white balance coefficients applied to the color-converted image. Automatically computed white balance coefficients are displayed when the White balance auto property is enabled.
5. ***Reset statistics*** – Resets the ***Acquisition Statistics*** page's statistics counters.

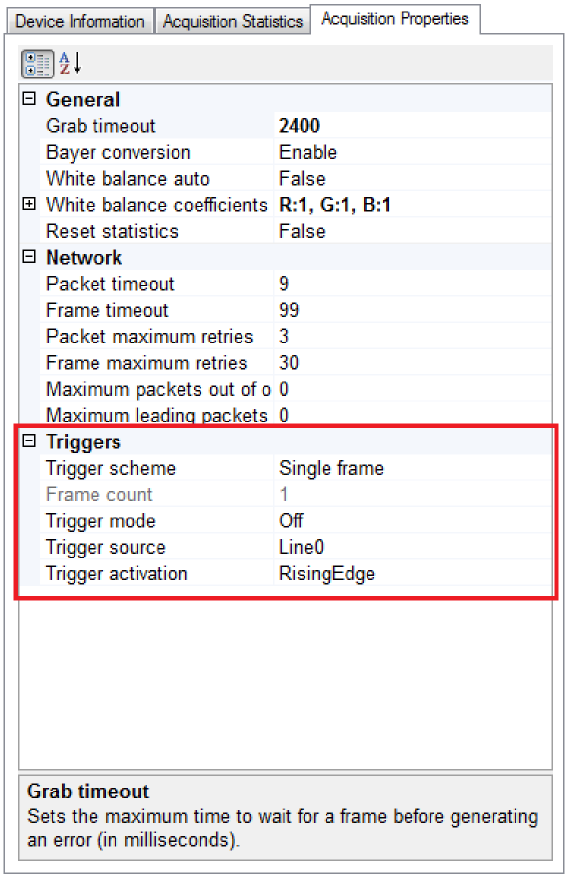
Network properties



Properties in this category allow you to control MIL's GigE Vision driver's packet resend engine. Note that these rarely need to be adjusted manually.

1. ***Packet timeout*** – Specifies the maximum amount of time to wait (in milliseconds) before flagging a packet as dropped.
2. ***Frame timeout*** – Specifies the maximum amount of time to wait (in milliseconds) for the remaining packets of a frame after the trailer packet has been received. If packets are missing, the frame is flagged as corrupted.
3. ***Packet maximum retries*** – Specifies the maximum number of times that MIL's GigE Vision driver should request that the GigE Vision device resend a packet that has not been received by the driver. If this value is reached, the frame is considered corrupted.
4. ***Frame maximum retries*** – Specifies the maximum number of times per frame that MIL's GigE Vision driver should request that the GigE Vision device resend a packet that has not been received by the driver. If this value is reached, the frame is corrupted.
5. ***Maximum packets out of order*** – Specifies the number of packets to wait before asking for a retransmission. This is useful with link-aggregated cameras whose packets could be received out of order.
6. ***Maximum leading packets missed*** – Specifies the number of leading packets that MIL's GigE Vision driver can fail to grab but still consider to have successfully acquired a frame. Missed leading packets will be flagged for retransmission.

Triggers



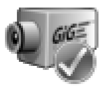
Properties in this category can configure your GigE Vision device for triggered acquisition. Note that different properties will be enumerated depending on your device's capabilities. (These include, but are not limited to, trigger schemes for single or multiple frames, software triggers, and hardware triggers.)

1. ***Trigger scheme*** – Configures your GigE Vision device for triggered operation using one of the following trigger schemes:
   a. ***Single frame*** – A single frame will be sent when a trigger signal is received.
   b. ***Multi frame*** – Multiple frames will be sent when a trigger signal is received.
   c. ***Continuous*** – Frames will be sent continuously when a trigger signal is received.
2. ***Frame count*** – Specifies the number of frames sent per trigger signal. Note that this property can be used only when ***Trigger scheme*** is set to ***Multi frame***
3. ***Trigger mode*** – Specifies whether the GigE Vision device should operate in triggered mode (***On***) or in continuous mode (***Off***).
4. ***Trigger source*** – Specifies whether to use an internal signal or physical input line as the selected GigE Vision device's trigger source.
5. ***Trigger activation*** – Specifies the trigger's activation mode.

GigE Vision Device icon overlays

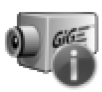
Once MIL detects a GigE Vision device, that device will appear in the ***GigE Vision Devices*** tab using Matrox Capture Assistant's ***Tree***, ***Details***, or ***Tile*** view. Note that each device icon is represented by a camera icon overlaid with the following set of symbols to indicate the device's status.

1  The device is ready to be used. Its resources have not yet been allocated.

2  The device's resources have been allocated by Matrox Capture Assistant or another process which could be running either on your Host PC or on a remote computer. When you hover your mouse over this device icon, Matrox Capture Assistant will display a tooltip that can help you determine which local Windows® process or remote computer has already allocated this device.

3  The device's resources have been allocated by Matrox Capture Assistant or another process in Multicast mode. The owner process could be running either on your Host PC or on a remote computer.

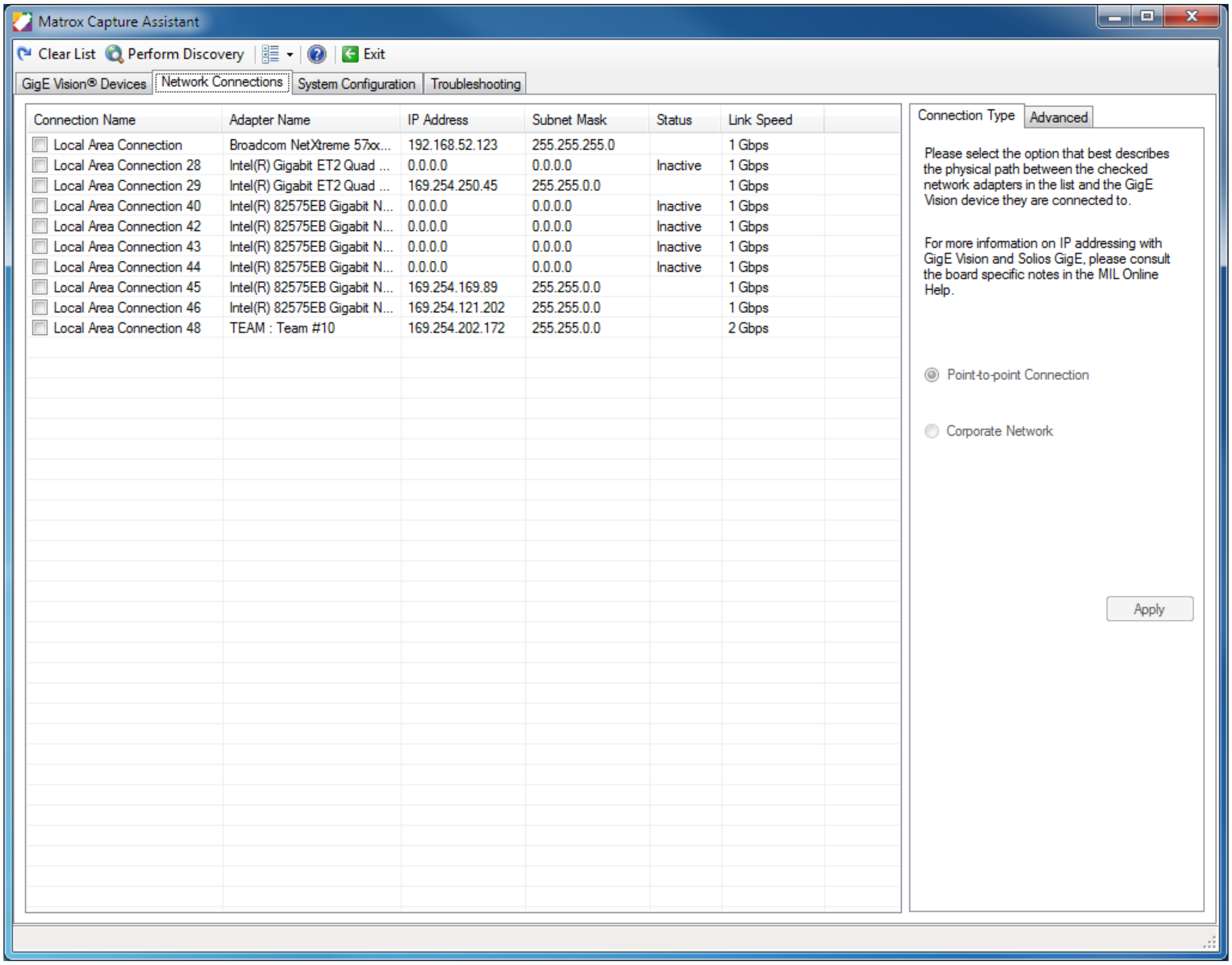
4  The device is available but its currently specified packet size is not optimal. This could happen if the device has just been turned on and its default packet size is less than 1500 bytes. You can click on the ***Allocate device*** button and wait for the packet size to be negotiated automatically.

5  The device's resources have been allocated (as in item 2 above). The exclamation point indicates that automatic packet size negotiation failed and that the device's current packet size is not large enough. Attempting to grab with an insufficiently large packet size will lead to acquisition problems. See packet size negotiation and firewalls for more information about resolving this problem.

6  Your computer lacks the proper MIL license privilege to use this device.

Network Connections page

The ***Network Connections*** page lists all Ethernet network adapters installed in the system. Its ***Connection Type*** tab also allows you to configure the multiple network adapters in your computer to static IP mode (or ***Point-to-point Connection***) or DHCP mode (or ***Corporate Network***). Note that if your GigE Vision devices are connected to a network with a DHCP server, you must set your network adapters connected to these devices to ***Corporate network***. On the other hand, if your GigE Vision devices do not obtain their IP addresses from a DHCP server, you must set your network adapters to ***Point-to-point connection***.



2 - Matrox Capture Assistant's ***Network Connections*** page.

To change your network adapter's settings, simply check the boxes corresponding to the connection(s) to specify and select either the ***Point-to-point Connection*** or ***Corporate network*** radio button. Matrox

Capture Assistant will change the network settings of the selected network adapters when you click ***Apply***.

A GigE Vision device automatically assigns itself an IP address in the link-local addressing (LLA) range (i.e. 169.254.*x*.*x*) by default if no DHCP server is present. Matrox Capture Assistant will also set the connections in the LLA range when ***Point-to-point Connection*** is selected.

You can also let the Windows® operating system automatically assign an IP address to your GigE Vision network adapters. This is done in cases where no DHCP servers are present. Microsoft® Windows® will assign an IP address in the LLA range however this procedure takes time (one to two minutes) to complete. During this time your GigE Vision devices will not be visible. Your GigE Vision devices will become available once the operating system has completed this procedure.

GigE Vision devices can also boot with a pre-programmed IP address in any address range. Such an IP configuration is called ***Persistent IP***. In this case, you must manually assign a compatible IP address to the network connections using the interface provided by Microsoft® Windows®.

Your GigE Vision device can be set to use Persistent IP by using Matrox Capture Assistant's Device Information page. To do so, you will need to manually select:

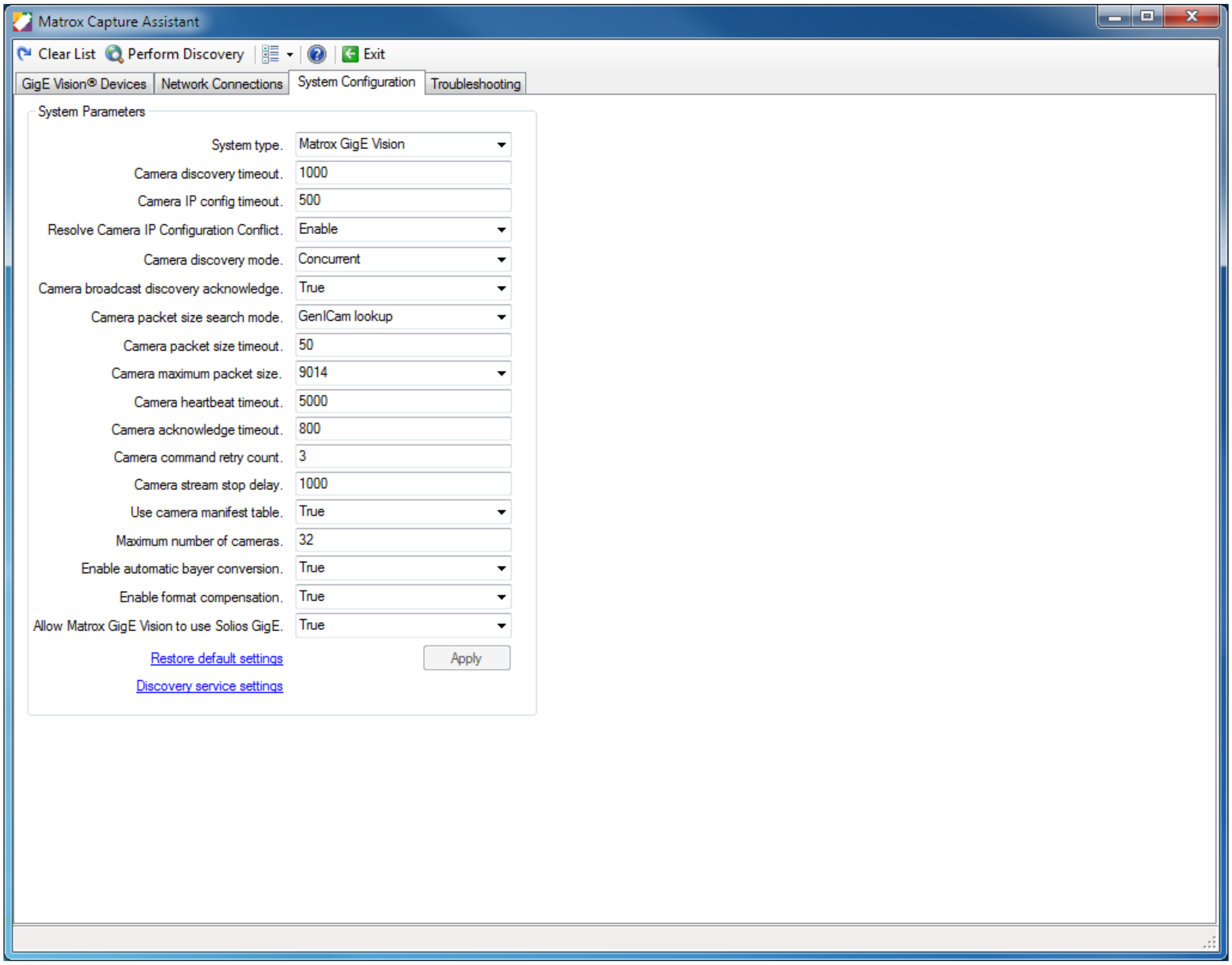
1. a valid IP address;
2. a valid subnet mask; and
3. optionally, a default gateway.

If your GigE Vision device supports the *DeviceReset* feature you can select the ***Reset Device*** option. When the ***Apply*** button is pressed, the Persistent IP settings will be written to the device's non-volatile memory and the device will reset itself. This forces the device to reboot using the newly assigned Persistent IP settings.

If your device does not support the DeviceReset feature, it will need to be power-cycled for the newly assigned Persistent IP settings to take effect.

System Configuration page

The ***System Configuration*** page allows you to specify persistent values for global parameters used by MIL's GigE Vision driver. These parameters are the following.



3 - Matrox Capture Assistant's ***System Configuration*** page.

1. ***System type*** – Specifies the Matrox GigE Vision system type to control. This value can either be set to ***Solios GigE*** (if using a Matrox Solios GigE frame grabber) or ***Matrox GigE Vision*** (for Matrox Concord and third-party Ethernet network adapters).
2. ***Camera discovery timeout*** – Specifies the amount of time to wait (in milliseconds) for a GigE Vision device's response to a discovery request.
3. ***Camera IP configuration timeout*** – Specifies the amount of time to wait (in milliseconds) for a response from a GigE Vision device to an IP configuration change event.
4. ***Resolve IP Configuration Conflict*** – Allows MIL's GigE Vision driver to resolve IP configuration conflicts between the GigE Vision device and the Ethernet network adapter to which it is connected.
5. ***Camera discovery mode*** – Specifies whether a GigE Vision device's discovery should be concurrent (per NIC) or serialized.

6. ***Camera broadcast discovery acknowledge*** – Allows the GigE Vision device to broadcast its response to a discovery command issued by the driver.
7. ***Camera packet size search mode*** – Specifies which method to use to negotiate a packet size with the GigE Vision device.
8. ***Camera packet size timeout*** – Specifies the timeout value (in milliseconds) to use when negotiating packet size with the GigE Vision device.
9. ***Camera maximum packet size*** – Allows the driver to limit the negotiated packet size to the specified value. This parameter is useful in cases where smaller packet sizes are desirable to avoid packet collisions. This situation might occur more frequently when multiple cameras are connected to a single Ethernet port (usually through an Ethernet switch).
10. ***Camera heartbeat timeout*** – Specifies the period (in milliseconds) used to keep the connection with the GigE Vision device alive.
11. ***Camera acknowledge timeout*** – Specifies the time (in milliseconds) during which the driver should wait for an acknowledgement from the GigE Vision device after issuing a command.
12. ***Camera command retries count*** – Specifies the number of times MIL's GigE Vision driver should resend a command if the GigE Vision device fails to acknowledge a command issued by the driver.
13. ***Camera stream stop delay*** – Specifies the time delay (in milliseconds) applied before stopping the GigE Vision device's video stream.
14. ***Use camera manifest table*** – Allows MIL's GigE Vision driver to use the GigE Vision device's manifest table (if one is available) when the device's description file is downloaded.
15. ***Maximum number of cameras*** – Limits the number of GigE Vision devices that can be discovered and controlled. Note that you must reboot your computer for a change to this parameter to take effect.
16. ***Enable automatic Bayer conversion*** – Specifies whether or not to automatically convert the raw Bayer data to the MIL destination buffer's format. Doing so results in a color-converted image.
17. ***Enable format compensation*** – Specifies whether or not to allow the driver to compensate the camera's pixel format (if available) to the format of the MIL acquisition buffer.
18. ***Allow Matrox GigE Vision to use Solios GigE*** – Specifies whether or not to treat any Matrox Solios GigE frame grabbers in the computer like a generic four-port Ethernet adapter. Setting this parameter to ***False*** prevents the Matrox GigE Vision system type from allocating any cameras connected to the Solios GigE frame grabber.

Using MIL with GigE Vision

For reliable acquisition performance, you must configure both your network adapter's settings and your GigE Vision device's settings.

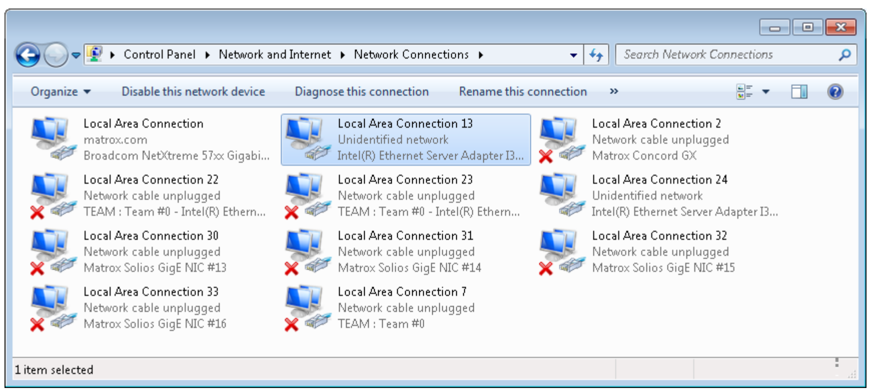
Network adapter settings

The following settings must be adjusted on your network adapter for reliable acquisition performance:

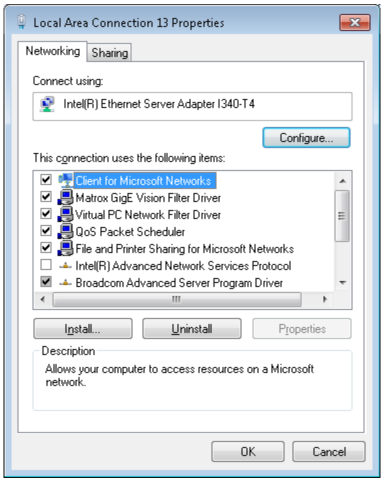
- receive buffers;
- packet size;
- flow control;
- interrupt moderation; and
- Receive side scaling.

Adjusting Intel® network adapter settings on Windows®

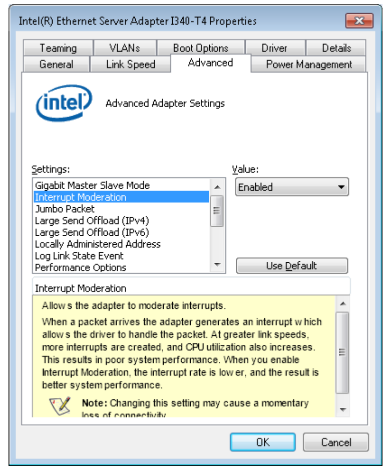
1. You can access your network adapter's configuration window from the ***Control Panel***'s ***Network Connections*** window. Right-click on the connection to configure and select ***Properties***.



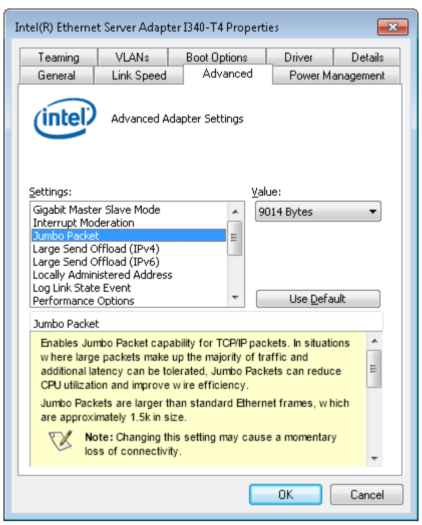
2. From the ***Properties*** window, click ***Configure***.



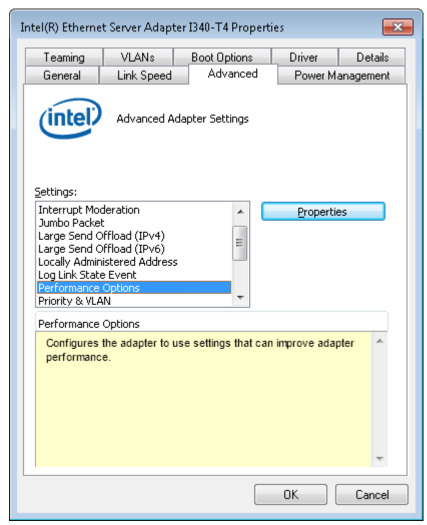
3. In the window that appears, navigate to the ***Advanced*** tab and ensure that the adapter's interrupt moderation is set to ***Enabled***.



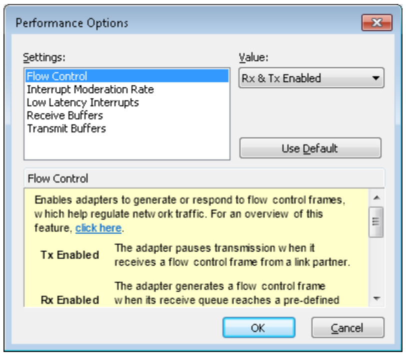
4. Ensure that the Jumbo Packet setting has a value of 9014 bytes.



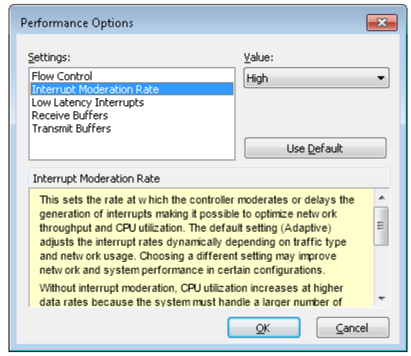
5. Select the ***Performance Options*** setting and click the ***Properties*** button.



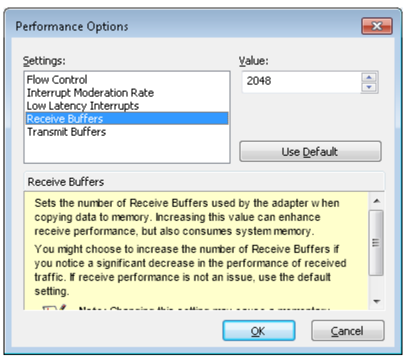
6. In the ***Performance Options*** window that appears, ensure that Flow Control is set to ***Enabled***.



7. Specify an ***Interrupt Moderation Rate*** setting that is appropriate for your application.



8. Ensure that the ***Receive Buffers*** setting has the highest possible value.



Receive buffers

Receive buffers, also known as *receive descriptors*, are used by Ethernet controllers to store received packets. Your network adapter's driver allocates a pool of receive buffers in Host non-paged memory. Data packets sent by the GigE Vision device arrive through your network adapter's Ethernet port. The packets' contents are then temporarily stored inside your adapters receive FIFO. Eventually a DMA transaction is performed and the packet's content is copied into one of the host receive buffers. The arrival of packets is signaled to the operating system's network stack, which then routes the receive buffers' contents to the appropriate Host software (in this case, MIL's GigE Vision driver). Once a packet has been handled by the network stack, its corresponding receive buffer returns to the pool of receive buffers available for use by the Ethernet controller. If the number of packets sent by the GigE Vision device exceeds the number of available receive buffers, those additional packets will be lost.

The number of receive buffers assigned to your Ethernet controller therefore impacts the reliability of your GigE Vision image acquisition. Typical bandwidth usage of GigE Vision devices requires that a large number of receive buffers be assigned to your network adapter. Matrox recommends setting this parameter to its maximum value (typically 2048 for Intel® Gigabit network adapters).

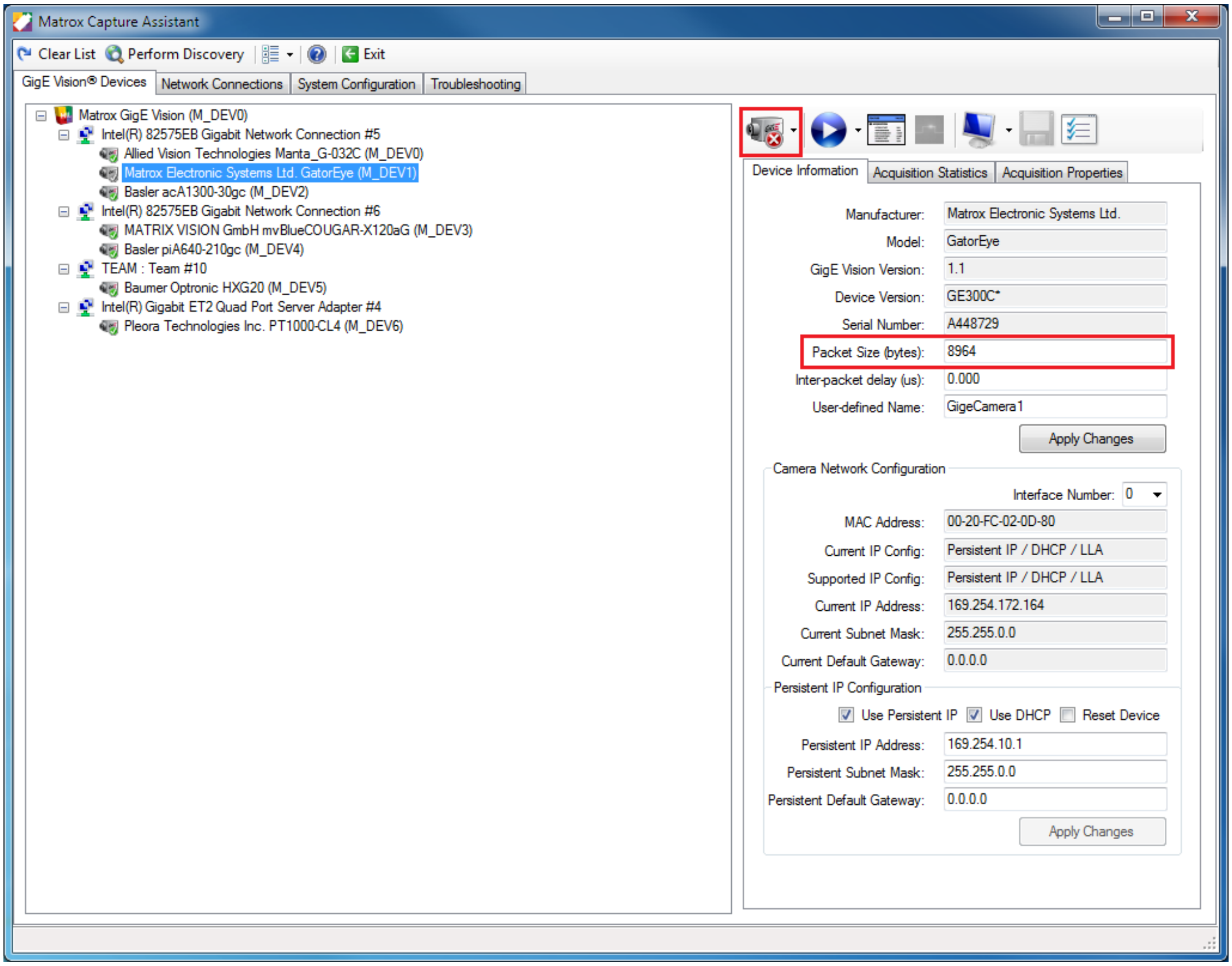
Choosing a packet size

In situations where large packets make up the majority of traffic, which is the case for GigE Vision image streams, jumbo packets can reduce CPU utilization and improve wire efficiency. Jumbo packets are larger than standard Ethernet frames, which are approximately 1.5k in size.

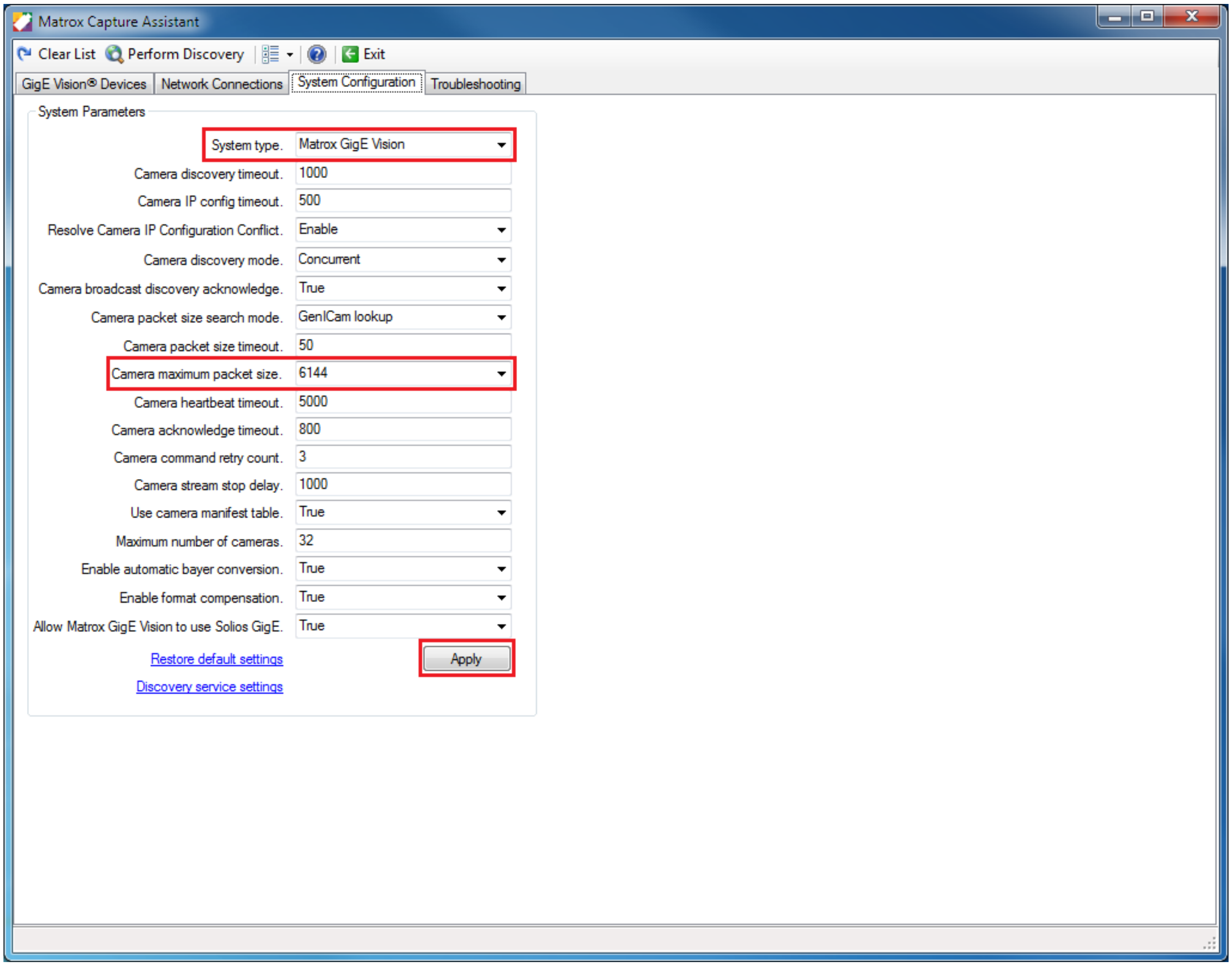
Enabling jumbo packets of 9014 bytes is recommended to reduce CPU utilization and increase efficiency.

Note that most gigabit Ethernet switches ship with jumbo packet support disabled. If you wish to use jumbo packets and require the use of an Ethernet switch, jumbo packets must be enabled in your switch.

MIL's GigE Vision driver will attempt to negotiate an optimal packet size during device allocation. This is done in order to validate that the data path between your GigE Vision device and your system is able to handle the negotiated packet size. You can validate the negotiated packet size with the Matrox Capture Assistant's ***GigE Vision Devices*** page. Simply select the GigE Vision device you wish to inspect; the ***Packet Size*** will be displayed in the right pane. Note that the device must have been allocated at lease once; otherwise the packet size shown will be the device's default packet size. To allocate the device your can simply click on the ***Allocate Device*** button.



By default, MIL's GigE Vision driver will attempt to negotiate the largest possible packet size with the GigE Vision device. On some networking environments this might not be optimal. This setting can be changed through Matrox Capture Assistant's System Configuration page. Simply select the GigE Vision system type you are using and then set the maximum negotiated packet size and click ***Apply***. At the next device allocation, the new packet size will be used.



In some cases, automatic packet size negotiation could fail. This might occur for the following reasons.

- Jumbo packets are not enabled in your network adapter's settings.
- Your Ethernet switch does not support jumbo packets.
- You are using an Ethernet switch on which jumbo packets are not enabled.
- A firewall is preventing packet size negotiation[1].

When packet size negotiation fails, MIL's GigE Vision driver selects the default packet size of the target GigE Vision device. In this case, the packet size used might not be optimal. This could lead to acquisition problems including image corruption.

[1] A device that is compliant to GigE Vision specification version 1.1 or higher and which supports firewall traversal can negotiate an optimal packet size even with a firewall enabled. See the ***GigE Vision device capabilities*** section of this document for details.

The packet size used can also be changed in code using **MdigControl()** with **M_GC_PACKET_SIZE**. This will force your device to use the packet size value specified. Forcing the packet size to a value that is not supported by your networking environment (i.e., your computer's network adapter, if present, your switch) will result in an unusable GigE Vision device.

Ethernet flow control

The IEEE 802.3 working group defining wired Ethernet has introduced the concept of Ethernet flow control in order to reduce packet loss.

Typical Gigabit Ethernet controllers have very little on-board memory. This local memory is used for temporary storage of received packets before they are transferred by DMA transaction to the host networking stack. System conditions exist that can temporarily prevent the Ethernet controller from transferring packets from on-board memory to the networking stack. If these conditions persist, then local memory becomes insufficient and packet loss occurs. This can take place even if the overall utilized Ethernet bandwidth is low, especially if your device has a tendency to burst its stream packets.

For this reason standard Ethernet flow control can be used in many cases to prevent packet loss. Before local memory runs out, the MAC sub layer of the Ethernet controller can issue a MAC Control PAUSE request. The PAUSE request is sent to inhibit data transmission for a period of time. During the PAUSE period, the Ethernet controller should have enough time to transfer the remaining packets from on-board memory to the networking stack thus avoiding packet loss.

A number of GigE Vision devices support Ethernet flow control. Enabling Ethernet flow control in your network adapter's settings is recommended.

Note that most Gigabit Ethernet switches ship with Ethernet flow disabled. If you wish to take advantage of flow control and require the use of an Ethernet switch then you must enable flow control in your Ethernet switch.

Interrupt moderation settings

Your network adapter generates an interrupt when it receives a data packet. This allows the network adapter's driver to handle the packet. A greater number of interrupts is typical with higher link speeds. Handling more interrupts increases CPU utilization and your computer's performance suffers as a result.

You can lower the interrupt rate and improve system performance by enabling *Interrupt moderation*. The rate at which the Ethernet controller *moderates* or delays the generation of interrupts allows you to optimize network throughput and CPU utilization.

Interrupt moderation causes the network adapter to accumulate interrupts and send a single interrupt rather than a series of interrupts. This lowers CPU utilization associated with higher data rates and can improve system performance. However, a lower interrupt moderation setting is preferred at low data rates, since delaying the rate at which the CPU handles interrupts also introduces latency.

A high moderation rate therefore reduces CPU utilization at the expense of increased latency. You should determine the best tradeoff between these to meet your application's specific needs.

The moderation of interrupts directly impacts how quickly an image is delivered to your application. For example, the delivery of an image can be delayed up to 921 microseconds with interrupt moderation rate set to ***Extreme***. The following table lists the maximum delay using various interrupt moderation settings:

Interrupt Moderation Setting[2]	**Delay (µs)**
Minimal	51
Low	102
Medium	243
High	512
Extreme	921

4 - Intel® PRO 1000 and Matrox Concord GE/GX interrupt moderation settings.

Finally, specifying a larger packet size also reduces the number of interrupts generated, since fewer packets are needed to constitute an image.

Receive-Side Scaling

Receive-Side Scaling (RSS) resolves the network processing bottleneck on a single processor by allowing the traffic through the receiver-side network adaptor to be handled by multiple processors. When enabled on your network adapter, RSS allows the Windows Networking subsystem to take advantage of multi-core processor architectures.

RSS is a result of Microsoft's Scalable Networking Initiative which was introduced in the Network Driver Interface Specification (NDIS) version 6.0. Windows Vista was the first version of Windows with NDIS 6.0 support. Earlier versions of Windows (e.g., Windows XP) do not support RSS.

To enable RSS, you need to enable it in the operating system and in the properties for each network adapter. RSS is enabled by default in Windows Server 2008 and more recent versions of Windows (including Windows 7 and Windows 8).

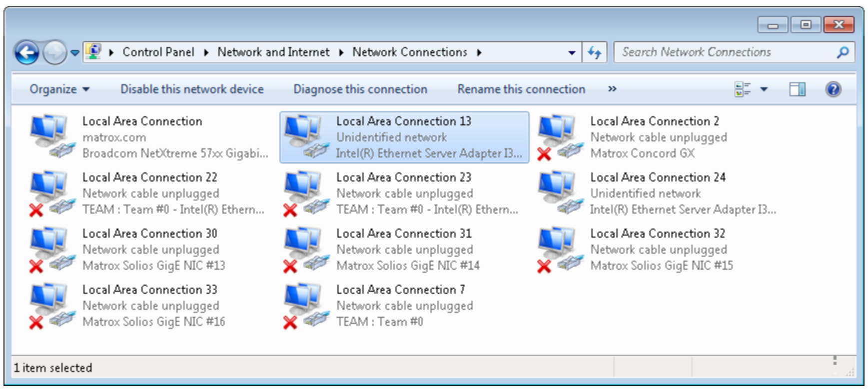
[2] Based on the Intel® Pro 1000 family of network adapters.

To enable receive side scaling in the operating system:

1. open an elevated command prompt;
2. type **netsh interface tcp set global rss=enabled** and press ENTER; and
3. close the command prompt window.

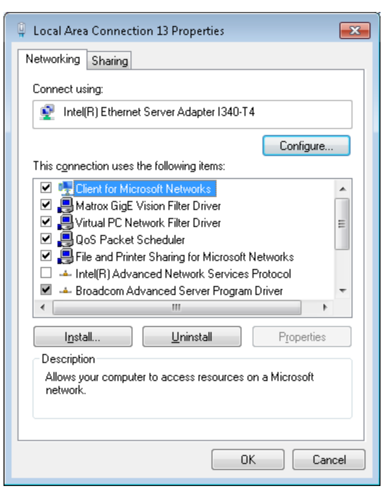
To enable receive side scaling in your network adapter:

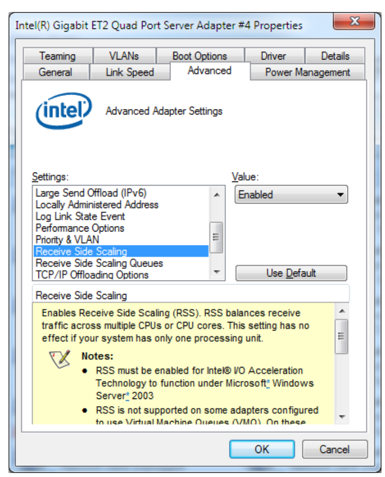
1. access your network adapter's configuration window from the ***Control Panel***'s ***Network Connections*** window, right-click on the connection to configure and select ***Properties***;



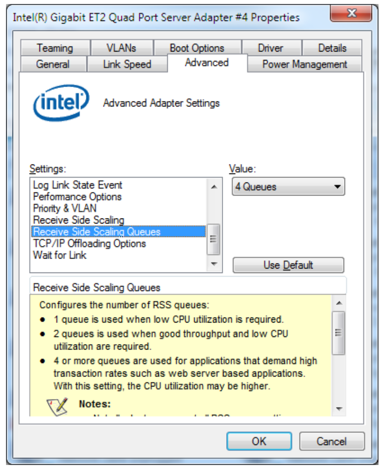
2. from the ***Properties*** window, click ***Configure***;

3. in the window that appears, navigate to the ***Advanced*** tab and ensure that the adapter's **Receive Side Scaling** is set to ***Enabled***;





4. Each RSS queue is associated to a specific CPU (core). Ensure that the Receive Side Scaling Queues is set to the number of queues appropriate for your application. This will spread received packet processing across multiple CPUs (cores).



GigE Vision device settings

Your GigE Vision device might require further optimization if its performance is not adequate using the network adapter settings explained above.

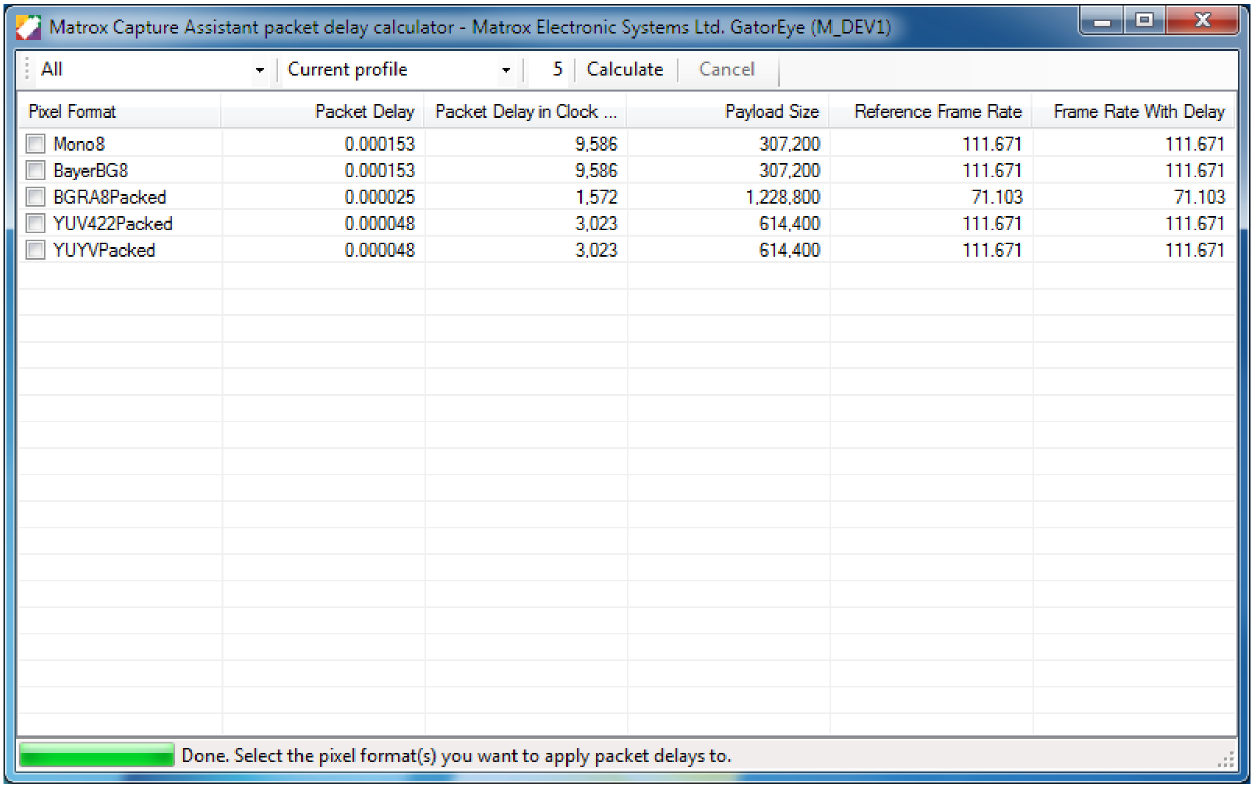
Inter-packet delay

Gigabit network adapters have very limited on-board memory for storing received packets. Intel® PRO 1000 Gigabit Ethernet controllers only have 48 KB of receive memory. With 48 KB of on-board memory thirty two (32) 1500 byte packets or five (5) 9014 byte packets can be stored before memory runs out. It is therefore imperative for the Ethernet controller to quickly transfer received packets to one of the host receive buffers. System conditions exist that can delay the transfer of received packets to the networking stack. If these conditions persist packets will accumulate in the 48 KB receive memory of the Ethernet controller until memory runs out and packet loss occurs. This is where programming an inter packet delay in your GigE Vision device can help. Inter packet delays help by spreading packet transmission in time. This gives the receiving Ethernet controller enough time in between packets to evacuate received packets to the host networking stack.

You can program your GigE Vision device's inter-packet delay from Matrox Capture Assistant's GigE Vision Devices page.

Inter-packet delay calculator

Matrox Capture Assistant includes an inter-packet delay calculator to determine the optimal inter-packet delay to use for your GigE Vision device. The inter-packet delay calculator begins by taking the theoretical inter-packet delay and iteratively fine-tunes this value, validating results against the initially sampled data.



Pixel Format	Packet Delay	Packet Delay in Clock ...	Payload Size	Reference Frame Rate	Frame Rate With Delay
Mono8	0.000153	9,586	307,200	111.671	111.671
BayerBG8	0.000153	9,586	307,200	111.671	111.671
BGRA8Packed	0.000025	1,572	1,228,800	71.103	71.103
YUV422Packed	0.000048	3,023	614,400	111.671	111.671
YUYVPacked	0.000048	3,023	614,400	111.671	111.671

5 - Matrox Capture Assistant's ***packet delay calculator*.**

The packet delay calculator's algorithm begins by sampling the GigE Vision device's frame rate and bandwidth by starting live data acquisition. Then a theoretical inter-packet delay is mathematically calculated using the device's current profile and sampled information. The device's profile consists of parameters susceptible of changing the bandwidth on the wire; these include but are not limited to:

- packet size;
- device payload size (e.g., the size of an image);
- Ethernet link speed; and
- acquisition frame rate (which can be influenced by other parameters such as exposure time).

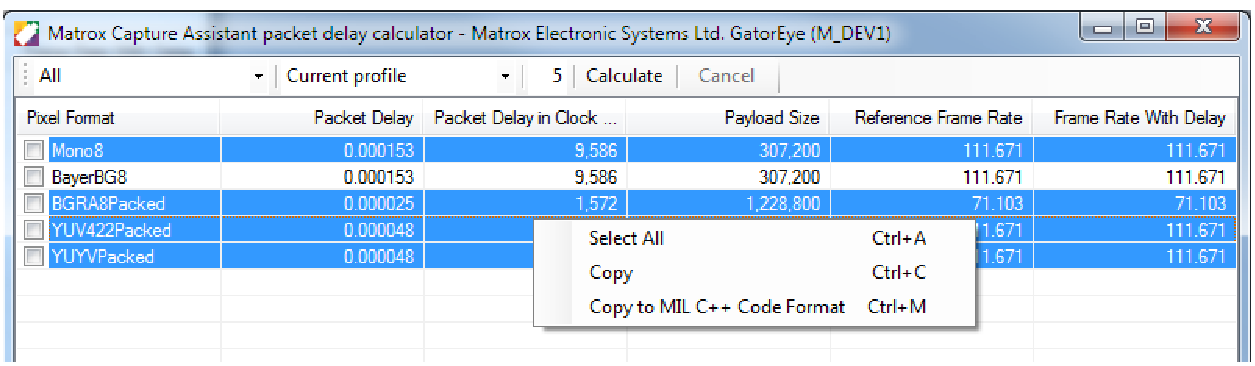
Using a mathematically calculated theoretical inter-packet delay as a starting point, the algorithm iteratively fine-tunes this delay validating results against the initially sampled data.

The empirical method was chosen because it takes into account unforeseeable factors that make up the device's current profile. These cannot be accounted for by strictly using a theoretical mathematical calculation.

By selecting results of interest and clicking on the Apply button, the user can tell Matrox Capture Assistant which results to use for subsequent data acquisition. These results can also be copy-pasted in text form or in C++ code form for use in code by selecting the results of interest and doing a right click operation.

Selecting ***Copy to MIL C++ Code Format*** will copy to the Windows® clipboard a C++ class containing the MIL code required to program the inter-packet delay of the selected device. The generated class name will be of the form ***PacketDelay_Model_Version*** where ***Model*** is the GigE Vision device's model name and ***Version*** is the GigE Vision device's version. In the example below, the class generated will be named ***PacketDelay_GatorEye_GE300C***. To use the class, simply declare it and call its SetPacketDelay() method passing the MilDigitizer identifier corresponding to the device you wish to control. SetPacketDelay() will program the device's packet delay to the value corresponding to the device's current pixel format.

Note that in the example below, BayerBG8 was not selected; the C++ class generated will not contain the code handling the BayerBG8 pixel format.



6 - Matrox Capture Assistant's *packet delay calculator* menu.

GigE Vision device numbers

GigE Vision devices are ranked by the MIL driver according to the device's MAC address. For example, the device having the lowest MAC address is ranked as device zero (**M_DEV0**); the rank increments by one for each device having a subsequently greater MAC address value. Note that adding a GigE Vision device to an existing system will shift the rank of all devices with a higher MAC address than the newly-added device.

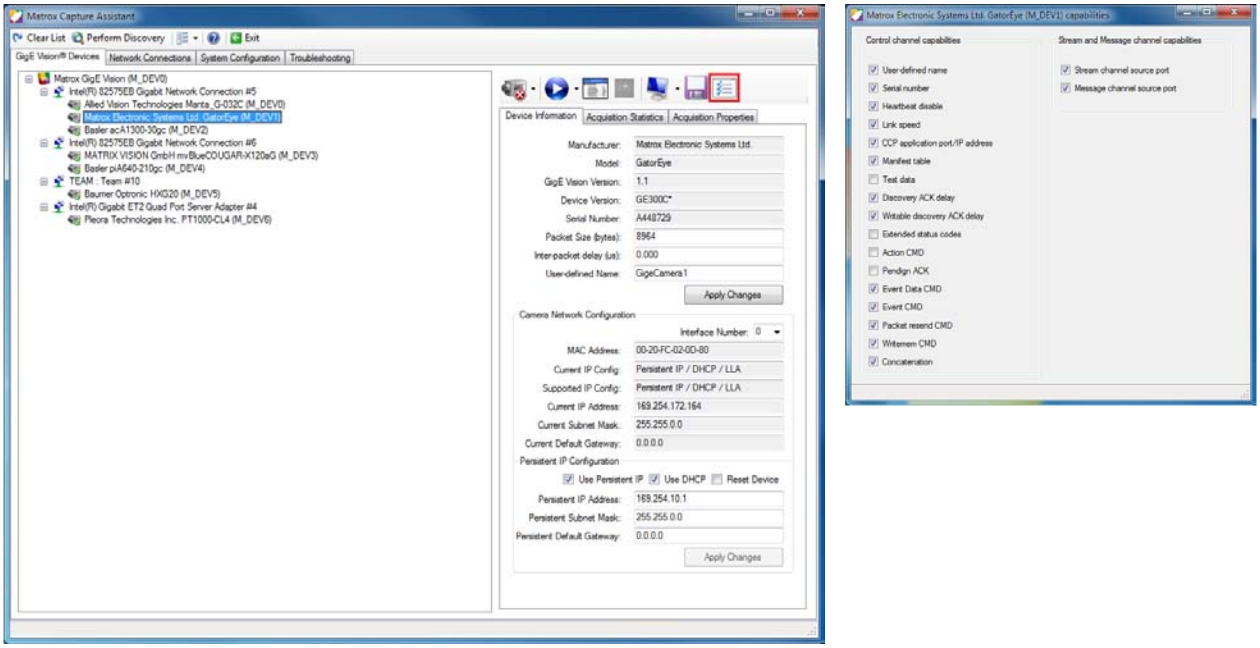
You can allocate a GigE Vision device using ***MdigAlloc()*** with the device number (e.g. **M_DEV0**, **M_DEV1**, etc.). However, this could be problematic in some applications where device rank is important or is likely to change. This is particularly likely if a device needs to be replaced. As a result of its different MAC address, the new device's rank could differ from the one it has replaced, resulting in potential problems.

GigE Vision devices can also be assigned a text string or *user-defined name* to store in the device's non-volatile memory. Once a name has been programmed in a device, you can use it to allocate that device. You can program your device's user-defined name in Matrox Capture Assistant's device information section. You can then use **MdigAlloc()** with **M_GC_DEVICE_USER_NAME**, which allows you to specify a device's user-defined name rather than its device number when allocating it. Consult MIL Help for additional information.

If a device needs to be replaced, you can simply program the user-defined name of the new device to match the name of the device that it replaces. This would allow your application to work with the new device without modifying either your application or your application's configuration.

GigE Vision device capabilities

Matrox Capture Assistant can be used to inquire your GigE Vision device's capabilities. To do so, specify your device and click the ***Capabilities*** button. A dialog box with a series of read-only checkboxes will appear. A checked box indicates that a specific capability is supported.



GigE Vision ***Device Capabilities*** button and dialog box

GigE Vision device capability description

Below is a list of capabilities and descriptions that you are likely to encounter in various GigE Vision devices.

Capability	**Description**
User-defined name	The device supports a user-defined name that can be written to the device's non-volatile memory.
Serial number	The device supports the serial number register.
Heartbeat disable	This device supports disabling the heartbeat mechanism. The device will continue streaming images even if the application that controls it stops abruptly.
Link speed	This device supports the link speed register. This register specifies of the speed of the Ethernet link that the device is connected to. Note that depending on network topology, this speed can be

	different than the link speed of the Host NIC.
CCP application port / IP address	This device can report the IP address and UDP port number of the application that controls it.
Manifest table	This device supports multiple versions of the GenICam™ GenApi schema. It might therefore support multiple XML files.
Test data	This device can send test packets initialized with test data.
Discovery acknowledge (ACK) delay	This device supports a discovery acknowledge delay register. This register reports the randomized delay that the device will wait (in milliseconds) following its reception of a discovery command before it will send out a discovery acknowledge command.
Writable discovery acknowledge (ACK) delay	This device supports writing to the discovery acknowledge delay register.
Extended status codes	This device supports extended status codes.
Action command (CMD)	This device supports the action command, which can be used to trigger an action on multiple devices at roughly the same time.
Pending acknowledge (ACK)	This device can respond to a command with a pending acknowledge if the command execution time is unusually long.
Event data command (CMD)	This device supports sending asynchronous events with device specific data.
Event command (CMD)	This device supports sending asynchronous events.
Packet resend command (CMD)	This device supports the packet resend command. Useful when stream packets are lost.
Writemem command (CMD)	This device supports the writemem command.
Concatenation	This device supports concatenating multiple commands into a single command.
Stream channel source port	This device supports firewall traversal features for all of its stream channels. Used during automatic packet size negotiation.
Message channel source port	This device supports firewall traversal features for its message channel.

GigE Vision device capabilities defined

Link aggregation

Some GigE Vision devices require more than one network interface because the total bandwidth generated exceeds 1 Gbps. They employ link aggregation, a method of combining multiple network connections in parallel, to increase the throughput beyond what a single connection can sustain.

Link aggregation and GigE Vision devices

Some adopters of link aggregation technology released their GigE Vision devices before link aggregation was even included in the GigE Vision specification. As a result, there is no standard way for the vast majority of link-aggregated GigE Vision devices to indicate whether they support this capability to MIL's GigE Vision driver. Instead, the driver deduces that a GigE Vision device is link-aggregated if the reported link speed of its parent network adapter is greater than 1 Gb/s but less than 10 Gb/s.

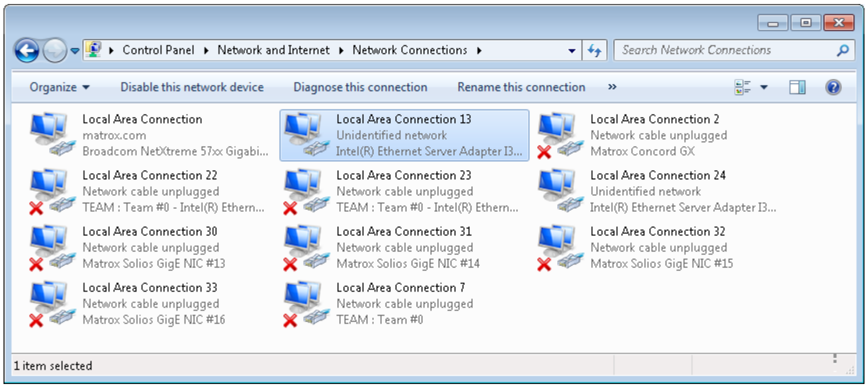
Detecting that a device is link-aggregated allows the Matrox GigE Vision driver to automatically adjust its packet resend engine to fit the requirements of these devices as they tend to send stream packets in a more or less out of order fashion.

Link aggregation has been incorporated into version 2.0 of the GigE Vision specification which has formalized its use with GigE Vision devices.

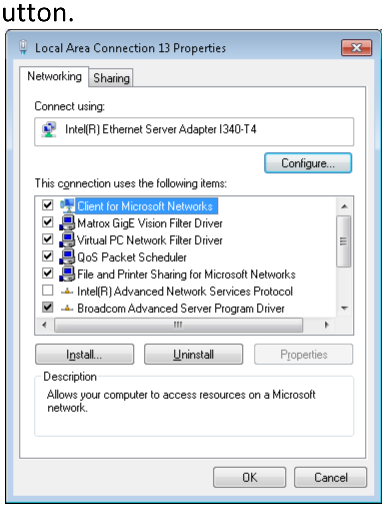
Teaming Ethernet controllers

Link-aggregated GigE Vision devices require that the Ethernet controllers in the system be *teamed*. You can use, for example, the Intel® network adapter's software to team Ethernet controllers together:

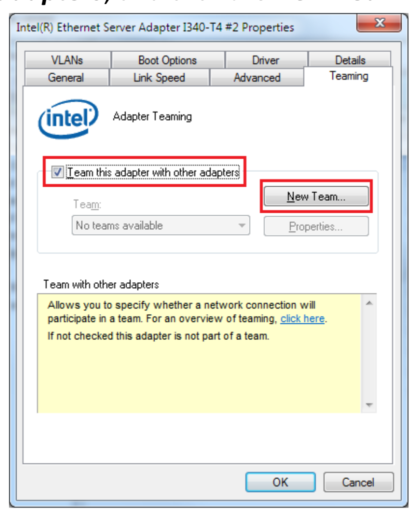
1. Right-click on the first connection you wish to team and select the ***Properties*** menu command.



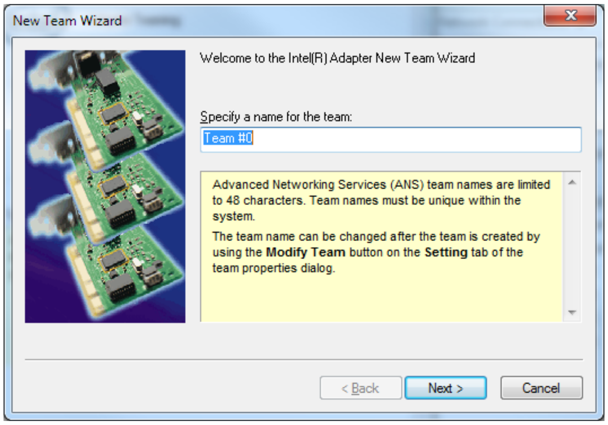
2. From the ***Local Area Connection Properties*** window, click the ***Configure*** button.



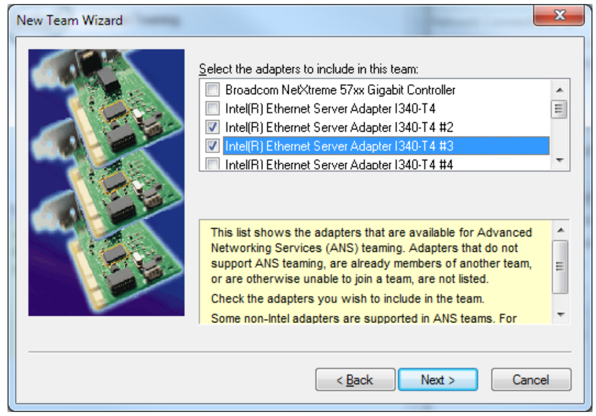
3. In the adapter properties window that appears, navigate to the ***Teaming*** tab, select ***Team this adapter with other adapters***, and click the ***New Team*** button.



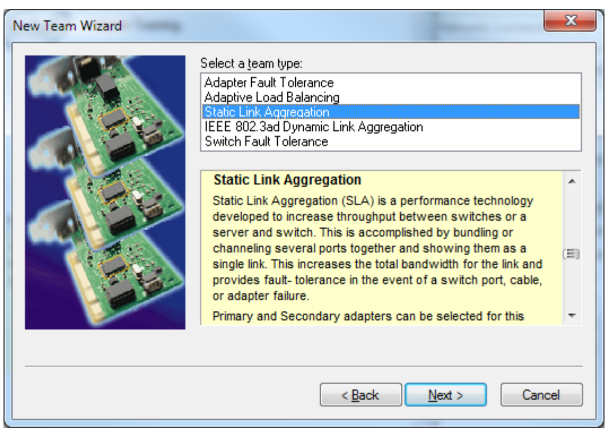
4. From the ***New Team*** wizard, specify a name for the team you are creating and the click the ***Next*** button.



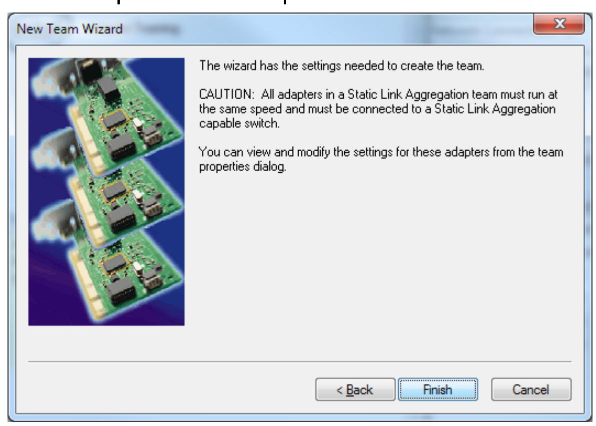
5. Specify the adapter(s) to include in the team and click the ***Next*** button.



6. Select ***Static Link Aggregation*** and click the ***Next*** button.



7. Click the ***Finish*** button. A new network connection will appear with the name you specified in step 4.



Firewall settings

Firewalls can affect your experience with GigE Vision devices in the following ways:

- preventing GigE Vision device discovery;
- preventing automatic packet size negotiation from taking place; or
- preventing GigE Vision message channel events from being received.

Device discovery problems and firewalls

The GigE Vision device discovery mechanism uses broadcasted UDP packets to find GigE Vision devices[3]. Firewalls can block broadcasted packets, preventing MIL's GigE Vision driver from discovering GigE Vision devices.

To work around this problem, MIL's GigE Vision module uses a dedicated software component: the *Matrox GigE Vision Discovery Assistant service* to perform GigE Vision device discovery. It is registered as an exception to the Windows® firewall. This allows the Matrox GigE Vision Assistant service to work around the Windows® firewall for GigE Vision device discovery.

Third-party firewalls

Although the Matrox GigE Vision Discovery Assistant service can work around the Windows® Firewall, it cannot work around other software firewalls. If you are using a third-party firewall product and experience GigE Vision device discovery issues, you can try the following.

- Register the Matrox GigE Vision Discovery Assistant service (MtxGigeService.exe) as an exception to your third-party firewall software.
- Open a port in your third-party firewall product allowing broadcasted UDP packets on destination port 3956.
- Disable your third-party firewall product on the network interface(s) used for GigE Vision acquisition and leave the firewall active only on your main network interface(s).

Packet size negotiation and firewalls

Firewalls can also prevent packet size negotiation from taking place. Both third-party firewalls and Windows® Firewall can prevent your GigE Vision device's packet size from being properly optimized.

When your GigE Vision device is allocated, MIL's GigE Vision driver will perform packet size negotiation to determine the largest possible packet size to use across all network components involved. These are, namely:

1. your GigE Vision device;
2. any networking components, such as an Ethernet switch, between your GigE Vision device and your system; and
3. your Ethernet controller.

If packet size negotiation fails, your GigE Vision device will use its default packet size. This can leave your device improperly optimized and lead to increased CPU usage. In some cases, an inadequate packet size could lead to corrupt images and acquisition reliability issues.

[3] Discovery packets are UDP packets using a dynamic source port and the fixed destination port 3956.

Auto-negotiated packet size and the GigE Vision firewall traversal capability

Version 1.1 of the GigE Vision specification introduced the firewall traversal capability for the stream channel. If firewall traversal is supported by your GigE Vision device, MIL's GigE Vision driver can negotiate an optimal packet size with your GigE Vision device regardless of the firewall used.

You can check whether your device supports firewall traversal for its stream channel by referring to the GigE Vision device capabilities section in this document.

If your GigE Vision device does not support the firewall traversal capability for its stream channel, MIL's GigE Vision driver will not be able to negotiate an optimal packet size. In this case, you can disable the firewall on the network interface(s) used for GigE Vision and leave the firewall enabled only on the network interface(s) used to access internal or external networks.

GigE Vision message channel events and firewalls

GigE Vision devices can optionally support a message channel. The message channel is used by the device to send asynchronous events to the application that controls it. Events supported are device-specific and can include exposure events, input line events, and error events.

Firewalls will block these events, since they appear to be unrequested packets. GigE Vision specification version 1.1 introduced the firewall traversal capability for the message channel. If GigE Vision message channel events are supported by your GigE Vision device, MIL's GigE Vision driver will be able to receive asynchronous events from your device's message channel.

You can check whether your device supports firewall traversal for its message channel, by referring to the GigE Vision device capabilities section in this document.

If your GigE Vision device does not support the firewall traversal capability for its message channel, MIL's GigE Vision driver will not be able to receive message channel events. In this case, you can disable the firewall on the network interface(s) used for GigE Vision and leave the firewall enabled on the network interface(s) used to access internal or external networks.

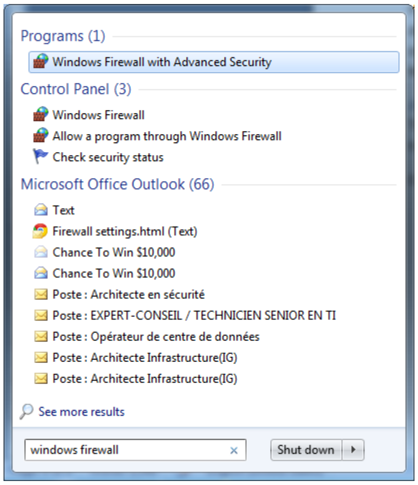
Disabling the Windows® Firewall

If your GigE Vision device does not support the firewall traversal capability, you can disable the firewall on the network interface to which it is connected. This will allow you to use MIL's GigE Vision driver to:

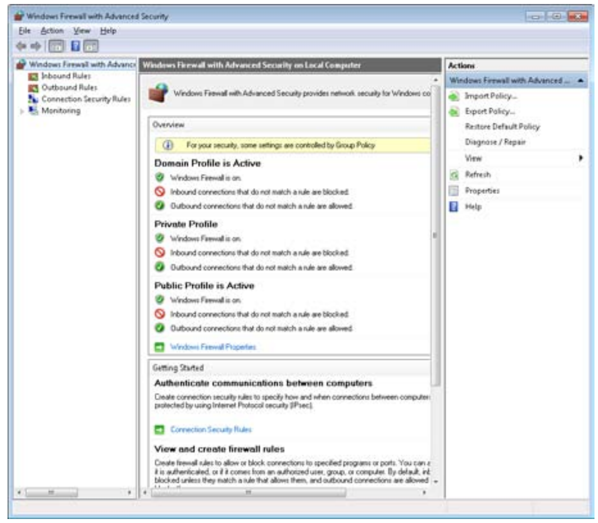
1. automatically negotiate the device's packet size; and
2. receive GigE Vision message channel events on the device.

To disable the Windows® firewall on a network interface, perform the following steps.

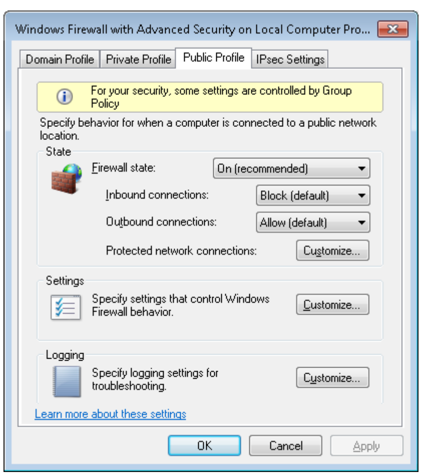
1. Open the Windows Firewall with Advanced Security dialog by typing ***Windows firewall*** in the Start menu search box.



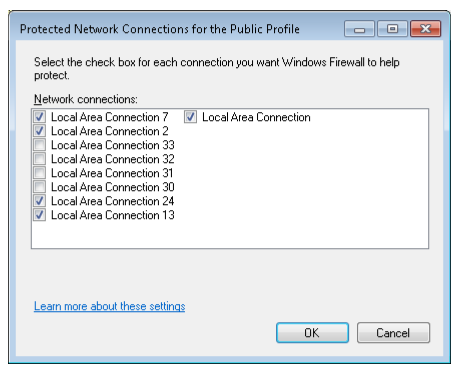
2. From the Windows Firewall with Advanced Security dialog, select the ***Windows Firewall Properties*** hyperlink.



3. From the ***Windows Firewall Properties*** window that appears, navigate to the ***Public Profile*** tab and click the ***Protected network connections Customize*** button.



4. Uncheck the network interface(s) used for GigE Vision acquisition, leaving checked only the network interfaces used to access internal and external networks. Click ***OK*** once the selection is complete.



Disabling the Windows® firewall instructions

IP multicast

IP multicast is a method of sending IP datagrams to a group of interested receivers in a single transmission. It is often employed by streaming media applications on the Internet and on private networks. With IP, multicast a GigE Vision device can stream data to multiple destinations without having to send multiple copies of the image data; the data replication is performed by network routers and switches. On a local network, multicast delivery is controlled by the Internet Group Management Protocol (IGMP) for IPv4 networks and Multicast Listener Discovery (MLD) for IPv6 networks. The following discussion will focus on IGMP only because GigE Vision devices currently only support IPv4.

Multicast address range

A multicast address is associated with a group of interested receivers. In IPv4, multicast addresses are defined by the leading bits of 1110. The multicast address group therefore includes addresses from 224.0.0.0 to 239.255.255.255. Address segments within this range are specified in RFC 5771, an Internet Engineering Task Force (IETF) Best Current Practice document. As such, some address ranges are reserved and should not be used.

Administratively scoped multicast addresses

The administratively scoped IP multicast address range 239.0.0.0 to 239.255.255.255 is assigned by RFC 2365 for private use within an organization. Packets destined to administratively scoped IPv4 multicast addresses do not cross administratively-defined organizational boundaries. These addresses are locally assigned and do not have to be globally unique. By default MIL's GigE Vision driver will select a multicast address in this range when allocating a GigE Vision device in multicast mode.

IP multicast with MIL and GigE Vision devices

To use IP multicast with your GigE Vision devices you must allocate the device with the MIL MdigAlloc() function using one of the following InitFlags:

1. M_GC_MULTICAST_MASTER; or
2. M_GC_SLAVE.

Two MIL examples illustrate how to use IP multicast with MIL and GigE Vision devices:

- MulticastMaster.cpp; and
- MulticastSlave.cpp.

A MIL digitizer allocated with the M_GC_MULTICAST_MASTER InitFlag behaves just like a normal MIL digitizer. You can read and write to a GigE Vision device with MdigInquireFeature() and MdigControlFeature(), receive events from the device using MdigHookFunction() (provided your GigE Vision device supports the GigE Vision message channel) and you can acquire images from the device using MdigGrab(), MdigGrabContinuous() or MdigProcess(). A multicast master digitizer will program the device's destination stream and message channels (if supported) with an administratively scoped IP multicast address.

A MIL digitizer allocated with the M_GC_SLAVE InitFlag is restricted in what it can do. A slave digitizer can read from a GigE Vision device with MdigInquireFeature() but it cannot write to the device. This is because GigE Vision devices impose that only one application has control. For this reason, the slave digitizer's DCF parameter passed to MdigAlloc() is not used because the parameters contained in the DCF cannot be written to the device by a slave digitizer. A slave digitizer can however read, receive events and acquire images from the device. Image acquisition will be performed only if the master digitizer on another PC has initiated a grab and the GigE Vision device is streaming data. If the master has not initiated image acquisition, then the slave digitizer will not receive any images when MdigGrab(), MdigGrabContinuous() or MdigProcess() is called; because of this, a slave digitizer's M_GRAB_TIMEOUT is set to M_INFINITE by default.

It is also important to note that a slave digitizer is allowed to issue packet resend requests (if supported by your GigE Vision device). Packet resend requests are issued by MIL when missing packets are detected. Because of the nature of multicast, resent packets will be forwarded to all members of the multicast group (the master and slave digitizer). A slave digitizer is typically used to view images on a secondary station and as such data integrity is not critical. If this is your use-case it is recommended that you disable packet resend on the slave digitizer; this will eliminate the possibility that packet resend requests issued by the slave affects acquisition reliability on the master. To prevent a slave digitizer from issuing packet resend requests, you can use MdigControl on the salve digitizer with M_GC_PACKET_RESEND as control type and M_DISABLE as control value. This control must be executed before calling MdigGrab(), MdigGrabContinuous() or MdigProcess(). Disabling packet resends on the slave digitizer does not prevent packet resends on the master digitizer.

The administratively scoped IP multicast address chosen by the MIL multicast master digitizer uses the digitizer's device number plus 1 and applies this to the base multicast IP address of 239.255.0.0. For example if you allocate a multicast master digitizer on M_DEV0 the multicast addresses used will be:

- 239.255.0.1 for the stream channel; and
- 239.255.1.1 for the message channel.

For a multicast digitizer allocated on M_DEV15 (provided you have 16 or more GigE Vision devices connected to your PCs) the addresses used will be:

- 239.255.0.16 for the stream channel; and
- 239.255.16.1 for the message channel.

The multicast master digitizer has no way of detecting if the automatically chosen IP multicast address and UDP host port numbers are conflicting with other multicast addresses and ports that might be in use. However, the default IP multicast addresses and port numbers can be inquired and changed with MdigControl/Inquire using the following Control/Inquire types:

- M_GC_STREAM_CHANNEL_MULTICAST_ADDRESS;
- M_GC_MESSAGE_CHANNEL_MULTICAST_ADDRESS;
- M_GC_STREAM_PORT; and
- M_GC_MESSAGE_PORT.

A multicast slave digitizer will simply use the multicast address programmed by the multicast master digitizer.

IP multicast requires the use of other network components such as Ethernet switches and routers; these devices must support network protocols regulating IP multicast traffic.

Ethernet switches, routers, IGMP and IP multicast

A network designed to deliver a multicast service might use the following basic components:

- A multicast transmitter (i.e., your GigE Vision device);
- Ethernet routers;
- Ethernet switches; and
- Host multicast receivers (i.e. your MIL GigE Vision applications allocated with a master or slave multicast digitizer).

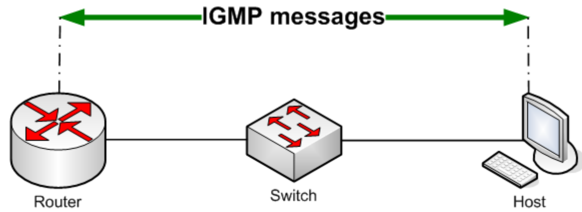
Each component has a defined role to play which we will expose below. In order to deliver a multicast service the Internet Group Management Protocol (IGMP) is used.

Internet Group Management Protocol (IGMP)

IGMP is a standard that specifies how a host can register with a router in order to receive specific multicast traffic. IGMP operates between the client computer (i.e. the computers running your MIL GigE Vision applications with a slave or master multicast digitizer) and a local multicast router.

A MIL digitizer allocated with M_GC_MULTICAST_MASTER or M_GC_SLAVE will automatically send IGMP requests to a network router asking for membership to a multicast group. The network router will then issue periodic membership queries to the registered members of a multicast group. Upon reception of these queries, MIL will respond with IGMP report messages. IGMP allows a router to correctly forward multicast traffic.

The diagram below illustrates IGMP messages exchanged between a host, requesting membership to a specific multicast group, and a router.

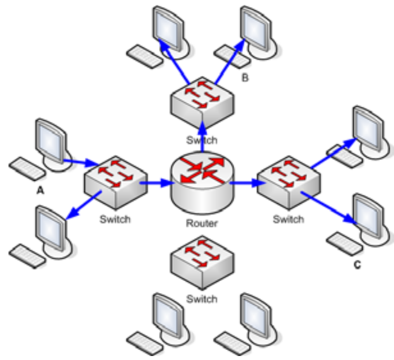


Ethernet switches and multicast

In order to correctly establish packet forwarding, an Ethernet switch uses and maintains an address table. Each packet that enters an Ethetnet switch is added to this table; the incoming packet's source MAC address is put in the address table along with the port on which the packet came from. To know on which port to output the packet, the switch will lookup the packet's destination MAC address in the address table. If the address is found, the packet will be output on the appropriate port. If the destination MAC address is not found, the packet is flooded on all ports. Eventually the address table will allow the switch to avoid flooding packets because almost every packet received can be looked up in the table.

By default Ethernet switches floods multicast traffic within the broadcast domain. This consumes a lot of bandwidth as all multicast packets received on one port of the switch are ouput to all other ports of the switch. In essence the default behavior of an Ethernet switch is to "broadcast" multicast packets on all ports. Multicast traffic becomes flooded because a switch usually learns MAC addresses by looking into the source address field of all the Ethernet frames it receives. A multicast MAC address is never used as source address for a packet. Such addresses do not appear in the MAC address table, and the switch has no method for learning them.

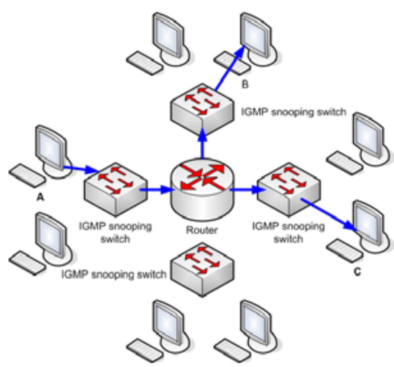
The diagram below illustrates multicast datagrams transmitted over a network. Server A is sending multicast IP data to clients B and C. As you can see the router correctly forwards the data to the client's networks because of the IGMP messages gathered. The LAN switches however flood the data to all PCs connected to them resulting in wasted bandwidth as PCs not members of the multicast group also receive this data.



IGMP Snooping and Ethernet switches

Typical Ethernet switches are Layer 2 devices and as such are not aware of Layer 3 protocols such as IGMP. In order to eliminate the flooding problem just exposed, some Ethernet switches support IGMP snooping. IGMP snooping allows an Ethernet switch to snoop IGMP messages exchanged between a host and a router. The switch will intercept IGMP packets and populate its Layer 2 forwarding table based on the content of the intercepted packets. By snooping IGMP messages, a switch can establish appropriate forwarding of multicast traffic avoiding the flooding scenario exposed previously.

The diagram below illustrates this. Again server A is sending multicast IP data to clients B and C. In this case both the router and swithches correctly forwards the data to the relavent clients.



IGMP snooping is disabled by default in LAN switches. To avoid IP multicast flooding problems you must enable IGMP snooping in your Ethernet switch using the managed (or other) interface of your switch.

IGMP Snooping Querier - IP multicast without a router

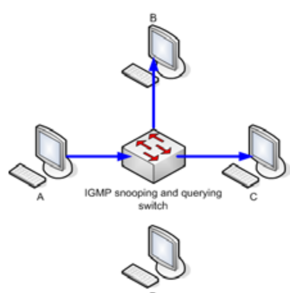
As explained previously IGMP operates between a client computer and a local router. If your network does not have a multicast router, IGMP will fail as there is no originator for IGMP queries. In such a case, you must configure an IGMP snooping querier to send membership queries to client computers. When an IGMP snooping querier is enabled, it sends out periodic IGMP queries that trigger IGMP report messages from hosts that want to receive multicast traffic. IGMP snooping in your switch listens to these IGMP reports to establish appropriate forwarding.

Without an IGMP querier present (which is typically done by a multicast router), your Ethernet switch will eventually flush snooped IGMP information and your application will stop receiving multicast traffic because of the following. When allocating a multicast master or slave digitizer with MdigAlloc(), the MIL driver will issue IGMP messages requesting membership to a multicast group. These messages get snooped by the Ethernet switch (provided IGMP snooping is enabled in the switch). The Ethernet switch will then be able to establish appropriate forwarding of multicast traffic. After some time has elapsed (depending on the switch settings) the switch will flush IGMP information because no IGMP queries were performed. Once IGMP settings have been flushed by the switch, your application will stop receiving multicast traffic. It is typically the routers responsibility to perform periodic IGMP queries that, when snooped by your Ethernet switch, will prevent flushing of the switch's multicast forwarding information.

Some Ethernet switches support IGMP querying. If you do not have a multicast router in your network then you must use an Ethernet switch that support IGMP querying. IGMP querying is typically disabled by default and must be enabled using the managed (or other) interface of your Ethernet switch.

If both IGMP snooping and IGMP querying are supported by your Ethernet switch then IP multicast becomes possible without the need of a router. Make sure both IGMP snooping and IGMP querying are enabled in your switch as these features are typically disabled by default.

The diagram below illustrates a network with a switch that supports IGMP snooping and querying. Again server A is sending multicast IP data to clients B and C.

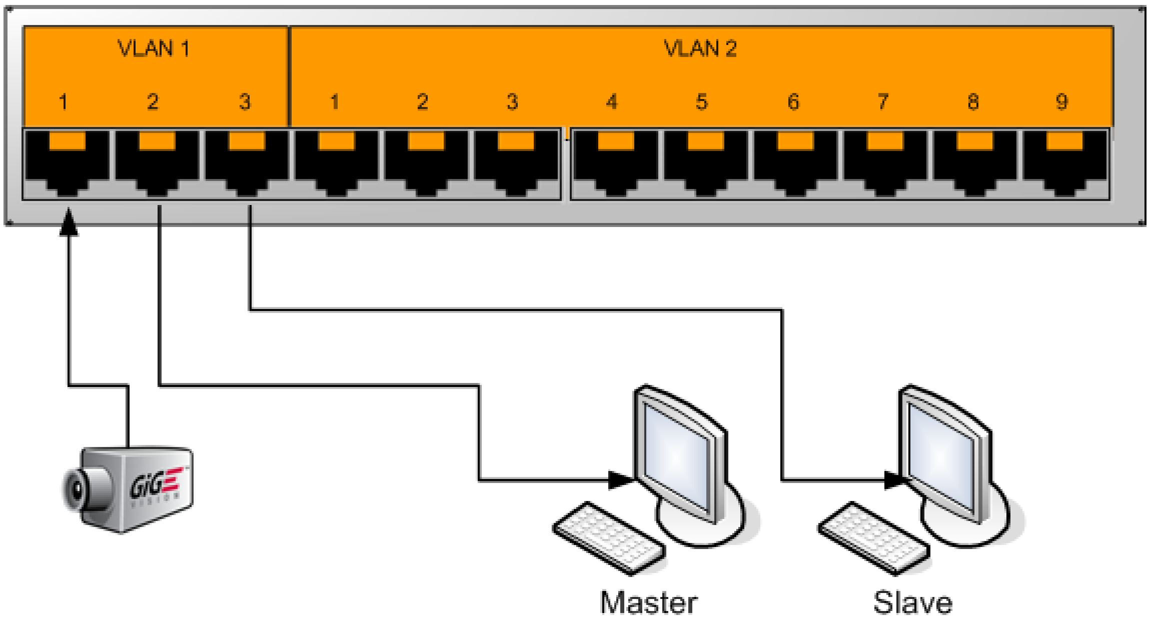


Routing multicast packets with a VLAN

As explained in the Ethernet switches and multicast section, Ethernet switches flood the broadcast domain with multicast traffic. This causes problems because multicast packets will end up where they shouldn't. IGMP can be used to correctly steer multicast packets to their intended destination. However, in cases where IGMP cannot be used, VLANs can be a good alternative.

A VLAN or Virtual Local Area Network is a way of partitioning a network into multiple distinct broadcast domains. These domains are mutually isolated. A VLAN will therefore isolate multicast packets and prevent them from crossing over to other VLANs.

For example, imagine a case where you have a single GigE Vision device sending multicast data to two destinations. A tree port VLAN can be created in your Ethernet switch which will prevent the multicast packets from crossing over to other VLANs.



This VLAN partitioning scheme can be used to create other VLANs in order to support additional multicast sources (e.g., GigE Vision devices). It can also be modified by adding ports in order to support more than two destinations per multicast source.

Using an Ethernet switch with GigE Vision devices

When multiple GigE Vision devices are used, you might need to use a gigabit Ethernet switch. In this configuration, multiple GigE Vision devices might stream image data to the same host network adapter simultaneously. You should ensure that your gigabit switch's performance metrics are adapted to your application's needs, particularly with regard to how many GigE Vision devices are connected and their respective bandwidth. Pay particular attention to:

- switching capacity; and
- packets per second capacity.

In addition, your Gigabit Ethernet switch should support the following:

- jumbo packets;
- IEEE 802.3x flow control; and
- port grouping (if interfacing link-aggregated GigE Vision devices through a switch).

Jumbo packets and flow control are typically disabled by default and must be enabled if needed. If port grouping is required, it must be manually configured using the switch's configuration utility.

Finally, if you wish to use IP multicast, make sure your switch supports the following:

- IGMP Snooping; and
- IGMP queriying (unless your network has a multicast router to handle IGMP).

IGMP Snooping and IGMP queriying are typically disabled by default and must be enabled if needed.

Troubleshooting acquisition reliability issues

A number of factors can cause acquisition reliability issues. You can determine if you are having reliability issues using the Matrox Capture Assistant's ***Acquisition Statistics*** page. This page will show whether any acquired frames (images) are corrupt as a result of missing packets. You can produce statistics either by starting a grab using your GigE Vision application or with Matrox Capture Assistant's built-in acquisition interface. From Matrox Capture Assistant, select the GigE Vision device from which to gather statistics and click on the Acquisition Statistics page, which will display acquisition statistics for the device. If you notice any corrupt frames or a large number of packet resend requests being issued by MIL's GigE Vision driver, you might need to adjust your network settings. Corrupt frames could occur for the following reasons.

Common causes of corrupt frames

- Your gigabit network adapter is not well-suited to your GigE Vision device's bandwidth requirements. Matrox recommends using a Matrox Concord GE/GX or an Intel® Gigabit Ethernet network adapter.
- Your network adapter settings have not been adjusted for GigE Vision acquisition. You need to adjust your adapter with recommended settings.
- Your Firewall is preventing automatic packet size negotiation between MIL's GigE Vision driver and your GigE Vision device. Improper packet size can result in poor acquisition performance as well as corrupt frames. You should adjust your firewall settings for optimal GigE Vision performance.
- A network device between your GigE Vision device and your network adapter, such as an Ethernet switch, is dropping packets. See the Using an Ethernet switch with GigE Vision devices section.

- The total bandwidth of all GigE Vision devices streaming image data to the same network adapter exceeds its link speed.
- An insufficient inter-packet delay value is specified in your GigE Vision device.
- Your camera does not have the Packet Resend capability.
- Your Ethernet cables are not rated Category 5e (Cat 5e) or better.